POLITIET
KRIPOS

Politidirektoratet

NCIS Norway

pr. e-post

Deres referanse:	Vår referanse:	Sted, dato
201504848	201502604	Oslo, 01.03.2016

HØRINGSSVAR – NOU 2015:13 DIGITAL SÅRBARHET – SIKKERT SAMFUNN

Det vises til brev fra Justis- og beredskapsdepartementet av 9. desember 2015 med tilhørende e-post fra Politidirektoratet av 5. januar 2016, hvor Kripos er anmodet om å bidra med innspill til NOU 2015:13.

Innledning

Kripos har i brev av 11. januar og 8. februar 2016 (vedlagt) gitt innspill til Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet tiltak 14 og 15. Det vises til det vi der har anført innledningsvis om økningen i bruk av teknologi, samfunnets sårbarhet og hvordan utviklingen stiller både samfunnet og politiet overfor nye utfordringer.

Arbeidet med IKT-sikkerhet og kampen mot IKT-kriminalitet blir stadig viktigere. Det digitale inntoget i vår hverdag har medført at tradisjonell kriminalitet har endret gjennomføringsmåte (modus) og utføres nå også på internett eller ved bruk av internett-tjenester. Dette betyr at omfanget av den digitale sikkerhet har konsekvenser ut over det som skjer på selve nettet. Kripos jobber daglig, både direkte og indirekte, med forebygging, avverging og etterforsking av IKT-kriminalitet.

Som påpekt av utvalget ligger Norge helt i verdenstoppen når det gjelder bruk av IKT. Det norske samfunnet er derfor utsatt for andre typer risiko enn for bare få år tilbake. Dette gir igjen nye utfordringer i politiets arbeid, herunder mulighetene for å sikre nødvendige bevis i straffesaker. Kripos har i stadig større grad erfart at bevisbildet og tilgang til informasjon som er lagret utenfor Norges grenser krever internasjonalt samarbeid. Kripos er derfor enig med utvalget når det innledningsvis påpeker at dette medfører nye sikkerhetsutfordringer, og at det i mange tilfeller faktisk blir vanskeligere å sikre verdikjedene. Dette gjelder særlig når tjenester helt eller delvis blir levert av utenlandske aktører og informasjon lagres utenfor Norges grenser.

Kripos

Post: Pb. 8163 Dep., 0034 Oslo
Besøk: Brynsalléen 6, 0667 Oslo
www.politi.no/kripos

Telefon: (+47) 23 20 80 00
Telefaks: (+47) 23 20 88 80
E-post: kripos@politiet.no

Org. nr: 974 760 827

Det er ikke tvilsomt at dette også har betydning for hvordan samfunnet bør forberede seg i forhold til både tilsiktede og utilsiktede hendelser. Erfaring viser at en digital hendelse kan få svært utfordrende konsekvenser innen andre sektorer enn der hendelsen startet. Kripos mener at utvalget undervurderer politiets rolle når det gjelder krisehåndtering. Krisehåndtering ved IKT hendelser bør følge de samme prinsipper som annen krisehåndtering i samfunnet. Det bidrar til uklar rolleforståelse samt manglende helhetstenkning og effektivitet, når det over tid er skapt relativt skarpe skiller mellom "den fysiske verden" og "den digitale verden". Kripos mener utvalget, gjennom sin beskrivelse av aktører, roller og ansvar bidrar til et slikt uhensiktsmessig skille.

Roller og ansvar

I likhet med utvalget har Kripos registrert at det stadig dukker opp nye trender som påvirker sårbarhetsbildet i samfunnet, og vi kan i det vesentlige slutte oss til utvalgets vurderinger om dette i kapittel 6. Stadig flere samfunnsfunksjoner som tidligere var basert på menneskelig arbeidskraft blir nå automatisert, og vesentlige deler av arbeid vil i fremtiden ha innslag av digitale funksjoner. Så og si alle digitale teknologiske nyvinninger har også i seg et potensiale til å bli benyttet av kriminelle. Det er derfor viktig at politiet holder seg orientert om trender og drivkrefter som påvirker denne utviklingen, særlig for å være forberedt på nye digitale sårbarheter. Vi mener det er behov for nært samarbeid med de ulike sikkerhetsaktørene nasjonalt, og mellom politimyndigheter på tvers av landegrenser. Selv om internasjonalt samarbeid byr på en del utfordringer, er det et tankekors at politiet til tider kan oppleve det nasjonale samarbeidet med andre sikkerhetsaktører som mer krevende enn samarbeidet med utenlandske aktører.

Særlig hva gjelder bekjempelse av IKT-kriminalitet som ligger utenfor CKG[1] sitt ansvarsområde, erfarer politiet unødige hindringer for effektivt samarbeid og informasjonsdeling. Disse synes ofte knyttet til uklarhet rundt roller og ansvar, samt mangel på samarbeids- og delingskultur. Kripos er for øvrig enig med utvalget i at mangel på anvendelige metoder og verktøy for utveksling av sensitiv og gradert informasjon er en faktor som i mange situasjoner hindrer et mer effektivt samarbeid.

Politiets rolle og ansvar etter politiloven ved digitale kriser synes ikke å være vurdert av utvalget i tilstrekkelig grad. Utvalget har, i kapittel 8 om "Roller og ansvar" nøyd seg med å henvise til at CKG i denne sammenheng utveksler informasjon med sektororganer, herunder politiet. Dette utgangspunktet synes også å prege utvalgets vurderinger i kapittel 20 når det gjelder «Styring og kriseledelse», hvor politiet i liten grad er omtalt. I tilknytting til punktet om "Sivilt–militært samarbeid i kriser" (20.1.5) har utvalget kort vist til at politiet har en sentral lederrolle i krisesituasjoner, og at politiet gjennom bistandsinstruksen kan be Forsvaret om assistanse. Når utvalget samtidig viser til at eventuell bistand på IKT-sikkerhetsområdet reguleres på samme måte, fremstår det som en mangel at utvalget ikke går nærmere inn på hvilke

[1] Cyberkoordineringsgruppen CKG - Fellesforum for NSM, E-tjenesten og PST i arbeidet med å koordinere de mest alvorlige datahendelsene.

situasjoner de anser at politiet har en leder rolle i, samt hvilken bistand utvalget ser for seg at Forsvaret bør yte. Utvalget uttaler at politiet har en sentral lederrolle i krisesituasjoner, men har i svært liten grad drøftet konsekvensen av dette i sine øvrige analyser og vurderinger. Dette er en beklagelig mangel, og kan illustrere en realitet som preger samarbeidet på dette området i praksis.

Det er viktig at det øves innenfor "digitalsikkerhet". Gjennom øvelser kan man trene på å bli stilt overfor ukjente situasjoner og problemstillinger, og sikkerhetsaktørenes evne til å løse problemene i fellesskap blir satt på prøve. Kripos kan på flere punkter slutte seg til utvalgets observasjon om at mangelfull gjennomføring og evaluering av øvelser er et hinder for effektiv samhandling. Til dette vil Kripos bemerke at det for politiet først og fremst er et problem at sentrale sikkerhetsaktører gjennomfører øvelser uten tilstrekkelig involvering fra politiet. Dette medfører stor fare for at sentrale politifaglige vurderinger og oppgaver blir glemt i håndteringen av virkelige hendelser, og at en eventuell etterforsking vil kunne bli forsinket eller hindret ved at bevis går tapt.

Kripos er enig med utvalget i behovet for å avstemme beredskapssystemene, og at det er behov for å oppdatere PBS-systemet[2]. Dette er også påpekt i "Datakrimstrategien"[3] og er særlig knyttet til hvordan politiet skal opptre når det er snakk om IKT-relaterte situasjoner. PBS inneholder ingen beskrivelser av scenarioer knyttet til digitale kriser, uavhengig av om krisen har fysisk skade som følge eller ikke. Verken Nasjonal sikkerhetsmyndighet (NSM) eller Nasjonal kommunikasjons-myndighet (Nkom) er beskrevet som sikkerhetsaktører. Dette er klare mangler som bør rettes opp. Etter Kripos' oppfatning er det behov for en totalgjennomgang av beredskapssystemene for digital krisehåndtering i Norge. Det er viktig at alle sikkerhetsaktører blir tatt med, også politiet. Det er særlig starten på en krisesituasjon som kan være uklar og uoversiktlig, og det er ofte i denne fasen det kan oppstå usikkerhet om hvilke sikkerhetsaktører som har ansvar for hva. Det er derfor viktig at de aktuelle aktørene avklarer ansvarsforholdene for å sikre at håndteringen kommer hurtig og riktig i gang. Samhandling er nødvendig for å sikre en god helhetlig innsats.

Kapittel 21 omhandler problemstillinger knyttet til avdekking og håndtering av digitale angrep. Våre merknader til dette kapitlet begrenser seg til politiets kjerneoppgaver – i hovedsak forebygging, avverging og etterforsking.

NSM har en sentral og svært viktig rolle når det gjelder forebygging og avverging av digitale kriser. Samtidig vil Kripos understreke at også politiet kan iverksette krisehåndtering på eget tiltak og med egne hjemler. Ved mistanke om pågående eller kommende straffbare handlinger, kan forebyggende og avvergende tiltak etter

[2] PBS - Politiets Beredskapssystem https://www.politi.no/vedlegg/rapport/Vedlegg_1690.pdf
[3] Datakrimstrategien: https://www.regjeringen.no/contentassets/4d2ba37bf2ae4cc9ac39afdf20a2f41b/datakrimstrategi_2015-pdf

politiloven være aktuelle i tillegg til etterforskning. Erfaring viser at NSM i svært beskjeden grad bistår politiet når det gjelder bevissikring, analyse og rådgiving knyttet til etterforskingen av digital kriminalitet.

Politiet er ved politiloven § 2 gitt et omfattende samfunnsoppdrag, herunder innen orden, sikkerhet og kriminalitetsbekjempelse. Sentralt for løsningen av dette oppdraget er politimyndigheten, som inneholder en fullmakt til å gjennomføre myndighetsbeslutninger ved bruk av makt. Utgangspunktet er at politiet har enerett til å gjøre bruk av maktmidler i fredstid. Dette er gjerne omtalt som politiets maktmonopol. Politiets ansvar for å forebygge kriminalitet og andre krenkelser av den offentlige orden og sikkerhet gjelder generelt, og er ikke begrenset til den fysiske verden. Det samme gjelder politiets ansvar for å avdekke og stanse kriminell virksomhet og forfølge straffbare forhold. I denne sammenheng er det helt sentralt å påpeke at politiet besitter eksklusive fullmakter til å nedlegge forbud, gi pålegg, uskadeliggjøre farlige gjenstander og treffe andre tiltak når dette er nødvendig. Disse fullmaktene gjelder uavhengig av mistanke om straffbare forhold og vil være svært relevante for å forhindre eller redusere skade også i digitale kriser.

Det fremgår blant annet av utredningen vedrørende "Hendelseshåndtering og varsling" at NSM NorCERT gjør en vurdering og prioritering av meldte hendelser. Enkelte saker diskuteres også i CKG, og NSM NorCERT bistår videre virksomheter som rammes med støtte til håndtering av hendelser. Det er svært sjelden at politiet blir kontaktet eller varslet i slike tilfeller. Dette til tross for at det utvilsomt er kriminelle handlinger som utløser hendelsene. NSM NorCERT tar her i realiteten den rollen som politiet er gitt, og det er vanskelig for Kripos å se at denne forskjellen i handtering av en "digital hendelse" og "fysisk hendelse" er godt begrunnet eller representerer en god og riktig løsning.

Erfaring viser at digitale kriser er mer enn angrep på digital samfunnskritisk infrastruktur. Digitale kriser vil fort få lokale fysiske følger som bare politiet er i stand til og kan håndtere. NSM og politiets fullmakter ved digitale kriser overlapper til en viss grad hverandre, men det er bare politiet som har myndighet til å benytte makt som del av sin oppdragsløsning. Samtidig er det ingen tvil om at politiet ofte vil være helt avhengig av et godt samarbeid med NSM for å kunne bidra med nødvendige tiltak for å stoppe pågående kriminalitet, uavhengig av hvor angrepet kommer fra. Det er heller ikke tvilsomt at det er politiet og PST som skal etterforske mulige straffbare handlinger. Det er derfor viktig at denne "handlingskjeden" kjenner hverandres kapasitet, evne og myndighet, samt deltar på samme arena både i øvelser og når reelle kriser oppstår.

Eksempler fra "kombinerte kriser" hvor digitale problemer har skapt fysiske kriser (eller omvendt), viser at andre sikkerhetsaktører mangler evne og mulighet til å lede krisehåndteringen uten bistand fra politiet. Et par relativt ferske eksempler på dette er også omtalt av utvalget.

Behovet for samhandling med og bistand til andre myndigheter og/eller private virksomheter synes åpenbart i krisesituasjoner. Det er derfor nødvendig å øve på slik samhandling med utgangspunkt i eksisterende planverk, og utvikle dette videre. I situasjoner hvor digitale hendelser har alvorlige, krisepregede, fysiske virkninger, kan det være nødvendig å etablere samme ledelsesapparat og samarbeid med andre offentlige etater, både lokalt og sentralt, som ved redningsaksjoner.

Styrke politiets evne og kapasitet til å bekjempe IKT-kriminalitet
Flere rapporter og utredninger har fokusert på behovet for å styrke politiets evne og kapasitet til å bekjempe IKT-kriminalitet, sist "Datakrimstrategien". Det er ved flere anledninger avdekket usikkerhet omkring hvem som er rett adressat for anmeldelse av IKT-kriminalitet, og Kripos har også registrert at flere undersøkelser har vist at mange har lave forventninger til politiet på dette området. I lys av dette har Kripos merket seg at utvalget (pkt. 21.11.5) støtter Justis- og beredskapsdepartementets forslag om å opprette et nasjonalt senter (NC3) for IKT-kriminalitet.

Slik Kripos vurderer sitasjonen er det nødvendig med et solid kompetanse- og kapasitetsløft for å gjøre norsk politi rustet til å takle dagens og morgendagens utfordringer. Vi mener derfor at det er svært viktig at forslaget om å opprette et NC3 følges opp og realiseres. Etableringen av NC3 vil kunne være avgjørende for i større grad å lykkes med å forebygge, avdekke og bekjempe IKT-kriminalitet. Vi viser til våre tidligere uttalelser om dette i brev av 3. september 2015. Selv om det etableres et NC3 og de sentrale funksjonene på den måten blir styrket, er det nødvendig at politidistriktenes fagmiljøer for sikring av elektroniske spor og etterforskning av IKT-kriminalitet også styrkes, slik det er fremhold at utvalget.

Kripos er derfor enig med utvalget i at de pågående organisatoriske endringer, i form sammenslåingen av politidistrikter og større fagmiljøer, ikke alene er tilstrekkelige for å sikre nødvendig kapasitet og evne for håndtering av fremtidige utfordringer med IKT-kriminalitet.

Personvern
Utvalget har blant annet i pkt. 21.11.8 tatt til orde for at man gjennom utredninger og offentlig debatt sikrer "…*balansen mellom personvern og et sikrere samfunn…*". Dette er et utgangspunkt Kripos er enig i. Uavhengig av hvilken definisjon man legger til grunn for personvern er det enighet om at ivaretakelse av den personlige integritet, rett til privatliv og ytringsfrihet representerer grunnleggende verdier i det norske samfunnet.

Slik Kripos vurderer det forutsetter imidlertid en slik balanse at man også i tilstrekkelig grad tar hensyn til offerets personvern gjennom å gi politiet tilstrekkelige muligheter og virkemidler for effektiv rettshåndhevelse. I motsatt fall kan det stilles spørsmål ved om manglende muligheter til å sikre borgerne mot kriminalitet kan være i strid med menneskerettighetene (EMK). Kripos vil påpeke at det for politiet er svært viktig at man, i tråd med den teknologiske utviklingen, sikrer grunnleggende

muligheter for bevissikring. Økt bruk av kryptering tilsier at muligheten for bevissikring blir mindre, og prosessene knyttet til dette blir mer utfordrende og tidkrevende.

Samtidig som innføring av nye metoder på den ene siden kan utfordre noens personvern, er det viktig å ta i betraktning at metodene samtidig vil være avgjørende for politiets muligheter til å ivareta andres personvern. Disse "andre" er da normalt ofre for kriminelle handlinger, med et klart behov for og en berettiget forventning om oppfølging fra politiets side. Dette er et perspektiv som synes å falle bort i debatten om personvern og myndighetenes kapasiteter.

Dette er et viktig perspektiv også i debatten om personvern og rettsikkerhet på internett. Det er en lite tilfredsstillende situasjon at rettsikkerheten for ofre for IKT-kriminalitet i Norge ofte avhenger av utenlandske tjenestetilbyderes godvilje. Det er viktig at problemer som rent samfunnsmessig er "små", men som oppleves som store for dem som rammes, også får en tilstrekkelig beskyttelse og oppfølging. Utviklingen viser at det i fremtiden neppe er rom for verken full frihet eller total kontroll. Kripos mener at det vil være nødvendig å gjennomføre regulatoriske tiltak, også på internett. Hvis ikke vil vi risikere at man i iveren etter å "sikre personvernet og hindre et overvåkingssamfunn" får en situasjon hvor det i hovedsak er de kriminelle som gis beskyttelse.

Offerets personvern[4] er anerkjent gjennom flere avgjørelser i EMD. I dommen K.U. v Finland[5] (2. desember 2008) var saksforholdet at noen hadde lagt ut en kontaktannonse på internett i navnet til en mindreårig gutt. I annonsen søkte gutten tilsynelatende etter jevnaldrende gutter for seksuell kontakt. Da dette ble oppdaget av gutten og hans familie ble forholdet anmeldt til politiet som ba om å få utlevert IP-adressen til den som hadde lastet opp annonsen. Anmodningen ble avslått fra kommunikasjonsleverandøren, og politiets begjæring om rettslig utleveringspålegg førte heller ikke frem, idet dette straffbare forholdet ikke ga hjemmel til utlevering av opplysningene etter finsk rett. EMD kom til at Finland hadde brutt sin plikt til effektiv beskyttelse av retten til privatliv etter artikkel 8, ved ikke å ha hjemmel for utlevering av opplysninger som var nødvendige for etterforskning og oppklaring av saken. Domstolen uttalte blant annet:

> *"The Court considers that practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement. In the instant case, such protection was not afforded. An effective investigation could never be launched because of an overriding requirement of confidentiality. Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of*

[4] Offerperspektivet og EMKs positive forpliktelse til å forplikte borgerne som følger av bl.a. EMK art. 2 og art. 8 er slått fast i flere avgjørelser i EMD, se bl.a. også Osman v UK (1998) og M.C. v Bulgaria (2004).
[5] http://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/KU%20v%20Finland%20en%20presse.pdf

expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others".

Dommen viser at menneskerettighetene inneholder en plikt for statene til å sikre politiet tilgang til nødvendige bevis for å beskytte borgerne. Dette vil for etterforsking av IKT-kriminalitet blant annet forutsette tilgang til tilstrekkelig kommunikasjonsdata for å kunne oppklare straffbare handlinger som innebærer krenkelser av personers rettigheter. Slik Kripos vurderer avgjørelsen er et av de sentrale momentene i EMDs avgjørelse at garantien for anonymitet på internett og i bruken av kommunikasjons-tjenester, ikke kan være absolutt. Dette er også et vektig argument for at statene i tilstrekkelig grad må sikre at slike data er tilgjengelig ut over det som telekommunikasjonsselskapene selv finner nødvendig å oppbevare. Regelverk omkring lagring og tilgang til kommunikasjonsdata må utformes og praktiseres etter en avveining mellom konkurrerende grunnleggende rettigheter. På den ene siden individenes rett til en effektiv beskyttelse mot krenkelser, og på den annen side inngrep i kommunikasjonsfriheten som kan medføre inngrep i personvernet og ytringsfriheten.

Utviklingen har på enkelte områder bragt internett til et punkt hvor Kripos er usikker på om man har balanse. Statens plikt til å sikre politiet tilgang til nødvendige bevis for å beskytte borgerne er i dag under et klart press i Norge. Det er nødvendig at dette perspektivet kommer klart frem i kommende utredninger og den offentlige debatten, slik at man sikrer en balanse mellom personvern og et sikrere samfunn som også tar tilstrekkelig hensyn til IKT-kriminalitetens ofre.

Straffeprosessuelle bestemmelser mv.
Utvalget har i pkt. 11.7.5 tatt til ordre for å regulere utlevering av blant annet teledata til politiet. Utvalget argumenterer med at politiets innhenting av teledata, som lagres hos teleselskapene for faktureringsformål og tekniske driftsformål, representerer en "formålsutgliding". Utvalget foreslår derfor at bruk av teledata bør vurderes regulert som et særskilt tvangsmiddel. Kripos vil på det sterkeste advare mot en utvikling hvor man, basert på et "lagringsformål", innfører særhjemler for bevisinnhenting avhengig av type opplysning. Det finnes i dag knapt en opplysning som opprinnelig er lageret med det formål at den skal kunne tjene som bevis ved en mulig fremtidig etterforsking. Det er helt avgjørende for politiets mulighet til effektiv kriminalitetsbekjempelse at relevante opplysninger kan hentes inn der de er tilgjengelige uavhengig av hvorfor de er der. Straffeprosessens system, med generelle regler om utlevering og beslag,[6] gir tilstrekkelige skranker og rammer for en behovsprøvet mulighet for innhenting, undergitt legalitetskontroll. En utvikling i retning av det utvalget foreslår vil bryte med et gjennomarbeidet system, og vil virke sterkt begrensende på politiets mulighet for nødvendig bevisinnhenting upåvirket av hvor bevisene til en hver tid finnes.

Dette er for øvrig også klart adressert i vårt vedlagte høringssvar av 8. februar 2016 vedrørende tiltak 15 i Justisdepartementets strategi for bekjempelse av IKT-

[6] Straffeprosessloven §§ 175 flg. og §210 flg

kriminalitet. Vi vil i den forbindelse også uttalelse i samme brev om nødvendigheten av teknologinøytrale bestemmelser.

Kryptering
Utvalget har i pkt. 23.8 vurdert bruk av kryptografi og kommet til en tredelt konklusjon. I utgangspunktet tar utvalget til orde for at bruk av kryptografi ikke bør reguleres eller forbys i Norge, og at norske myndigheter bør engasjere seg internasjonalt og arbeide aktivt mot regulering eller forbud. Videre tar utvalget til orde for at det må utvikles nye etterforskningsmetoder for å sikre et effektivt politi- og etterretningsarbeid.

Kripos ser at det er åpenbare dilemmaer knyttet til dette. For å oppnå et sikkert internett er kryptografi en forutsetning, og det er i alles interesse at internett og kommunikasjon på internett er sikkert. Selv om graden av kryptering varierer vil kryptering generelt sett også bidra til å verne de interesser politiet er satt til å beskytte. Dilemmaet består i at norske kriminelle, som i utgangspunktet kun kommuniserer i Norge, flytter sin kommunikasjon til utenlandske tilbydere og en kryptert digital infrastruktur som er helt utenfor norsk jurisdiksjon. I mange tilfeller foregår kommunikasjonen uten regulatorisk kontroll og myndighetsoppfølging overhodet. I denne sammenheng blir dette svært krevende for politiet, fordi man gradvis mister evne og mulighet til å utføre lovpålagte oppgaver på internett.

En naturlig parallell er mobiltelefonnettet, som i stor grad er kryptert. Her er infrastruktur og tilbydere underlagt norsk regulatorisk kontroll og myndighet, og man har en lovgivning som sikrer og legger til rette for at politiet kan utføre sine lovpålagte oppgaver gjennom for eksempel kommunikasjonskontroll. Nødvendigheten av slik kontroll på særlige kriminalitetsområder er det bred enighet om. Regelverk, rammer, prosess og kontrollsystemer sikrer riktig balanse i forhold til det personverninngrep metodebruken kan representere. I prinsippet burde ikke kommunikasjonstjenester som Skype[7] og lignende tjenester reguleres annerledes, men fordi denne kommunikasjonen skjer over internett mangler politiet slike muligheter.

I dagens debatt fremstår det for Kripos som om mange oppfatter det som nærmest uakseptabelt å sikre hjemler for å avlytte denne type kommunikasjon, uavhengig av kontrollen har et legitimt formål eller hvor streng kontroll og tilsyn metoden blir underlagt. I et kriminalitetsbekjempende perspektiv er det vanskelig å akseptere at kommunikasjon på internett skal ha et sterkere vern mot innsyn og kontroll, enn annen kommunikasjon. Slik Kripos vurderer det vil en sterk motstand mot regulering, som utvalget tar til ordet for, i økende grad bidra til å svekke etterforskningsevnen til norsk politi på dette området.

[7] Skype er et dataprogram som brukes til IP-telefoni. Samtalene skjer kryptert over Internett. Det er det ingen kostnader knyttet til bruken av programmet, annet enn når man kommuniserer med andre tjenester. I tillegg til at brukerne kan ringe til hverandre, har programmet også funksjonalitet for meldingsformidling, filoverføring, videosamtaler mv.

Utvalget foreslår avslutningsvis at "…*nye etterforskningsmetoder må utvikles for å sikre effektivt politi- og etterretningsarbeid i en verden der mer og mer krypteres…*". Kripos er ikke uenig i dette synspunktet. Samtidig er det vanskelig å se for seg at Norge kan innføre egne regler uavhengig av den internasjonale utviklingen, eller at man at man vil enes om en regulering som sikrer politiets behov på det globale internettet. Kripos mener at de metoder og virkemidler som allerede eksisterer, og som er innført og utprøvd i andre land, bør vurderes innført også i Norge. Et eksempel på dette er datalagring, som allerede er/blir innført i flere andre europeiske land, herunder Tyskland[8] og Danmark[9]. Sammen med lagring av IP-adresser er dette et sentralt virkemiddel som etter Kripos' vurdering vil ha svært stor betydning for politiets evne til å bekjempe IKT-kriminalitet. Det er derfor viktig at det settes fart i prosessene for etablering av hensiktsmessig regulering av disse områdene.

Med hilsen

Ketil Haukaas

Saksbehandler:
Knut Jostein Sætnan
politiadvokat
tlf: 99286416

Vedlegg:
Kripos' høringssvar av 11.01.2016
Kripos' høringssvar av 08.02.2016

Kopi:
Det nasjonale statsadvokatembetet

[8] www.dw.com/en/german-parliament-votes-for-new-data-retention-law/a-18786345
[9] http://www.dr.dk/ligetil/regeringen-vil-registrere-vores-aktivitet-paa-nettet

POLITIET
KRIPOS

Politidirektoratet

NCIS Norway

pr. e-post

Deres referanse:	Vår referanse:	Sted, dato
201504848	201502604	Oslo, *04*.03.2016

TILLEGG TIL HØRINGSSVAR – NOU 2015:13 DIGITAL SÅRBARHET – SIKKERT SAMFUNN

Det vises til Kripos høringssvar av 1.mars 2016, hvor Kripos avga innspill til NOU 2015:13. Kripos har i ettertid blitt oppmerksom på et punkt i NOU som vi ønsket å kommentere, men som ved en forglemmelse hadde blitt utelatt. Dette gjelder kap. 21.11.2 og spørsmål knyttet til å forbedre den nasjonale operative evnen gjennom samlokalisering.

Utvalget har på dette punktet delt seg i et flertall og et mindre tall og Kripos vil i all hovedsak sluttet seg til mindretallets forslag om å samle ressurser fra privat og offentlig sektor for å få bedre informasjon deling, hendelseshåndtering og teknisk analyse i et nytt Nasjonalt datakrimsenter (NC3). Flertallet vil bygge videre på dagens modell hos NSM NorCert.

Som påpekt i den opprinnelige høringsuttalelsen ser Kripos et generelt behov for god samhandling med og bistand til andre myndigheter og/eller private virksomheter i krisesituasjoner. Videre er det utvilsomt at både det løpende arbeidet med å bekjempe IKT-kriminalitet og evnen til samarbeid i krisesituasjoner vil blitt vesentlig styrket ved et mer permanent samarbeid mellom private og offentlige sikkerhetsaktører. Ved etablering av et Nasjonalt datakrimsenter vil økt tverrfaglig samarbeid være en forutsetning for å kunne lykkes med de sentrale oppgavene et slikt senter er tenkt å i vareta. I rapporten Datakrimstrategien[1] er det er på side 83 flg. gjort rede for "Pittsburg-modellen[2]" hvor det er etablert et samarbeidsforum mellom bl.a. politiet, relevante offentlige- og private virksomheter og akademia. Sentralt i dette samarbeidet ligger informasjonsdeling – som anses som en helt

[1] https://www.regjeringen.no/contentassets/4d2ba37bf2ae4cc9ac39afdf20a2f41b/datakrimstrategi_2015.pdf
[2] National Cyber-Forensics & Training Alliance (NCFTA), http://www.ncfta.net

Kripos

Post: Pb. 8163 Dep., 0034 Oslo
Besøk: Brynsalléen 6, 0667 Oslo
www.politi.no/kripos

Telefon: (+47) 23 20 80 00
Telefaks: (+47) 23 20 88 80
E-post: kripos@politiet.no

Org. nr: 974 760 827

avgjørende faktor for å lykkes med så vel etterforsking som forebygging og avverging av IKT-kriminalitet.

En utbygging av dagens modell vil etter Kripos oppfatning, basert på både erfaring med dagens situasjon og uttalelser fra NSM NorCert omkring deres muligheter til å dele opplysninger, ikke føre til økt samarbeid. I tillegg til at en slik utvidelse trolig ikke vil gi politiet tilstrekkelig mulighet til deltakelse eller tilgang til nødvendige opplysninger, så vil den heller ikke sikre den grunnleggende kontrollen med straffesaksbehandlingen som norsk straffeprosess bygger på. Dette i alle fall hvis utvalget har ment at man også skal bedre den nasjonale evnen til etterforsking av IKT-kriminalitet.

En utbygging i regi av et fremtidig NC3 vil kunne ivareta disse delvis kolliderende formålene på en vesentlig bedre måte og bidra til et generelt løft i den nasjonale evnen til å bekjempe IKT-kriminalitet, både når det gjelder "rikets sikkerhet" og mer alminnelig ikt-kriminalitet.

Med hilsen

Ketil Haukaas

Saksbehandler:
Knut Jostein Sætnan
politiadvokat
tlf: 99286416

Kopi:
Det nasjonale statsadvokatembetet

POLITIET
OSLO POLITIDISTRIKT

Politidirektoratet
Postboks 8051 Dep
0031 OSLO

OSLO POLICE DISTRICT

Deres referanse:	Vår referanse:	Sted, Dato
	201600094-6 008	Oslo, 01.03.2016

HØRINGSSVAR – NOU 2015:13 DIGITAL SÅRBARHET - SIKKERT SAMFUNN

Det vises til Politidirektoratets oversendelse av 5. januar 2016 med frist for svar til 29. februar 2016. En mindre fristoversittelse beklages.

Høringen gjelder samfunnets digitale sårbarhet, og foreslår konkrete tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet.

Vi har forelagt saken for relevante enheter i politidistriktet. To områder er særlig kommentert.

Finans- og miljøkrimseksjonen har påpekt at rapporten er meget omfattende og dekker en rekke temaer. Oslo politidistrikts kommentarer relaterer seg til politiets rolle og oppgaver og hvordan disse er beskrevet i rapporten. Først vil vi kort omtale trusselbildet og gi noen eksempler på saker knyttet til IKT-kriminalitet. IKT-kriminalitet er omtalt i rapportens kapittel 7.2.1. Vi mener dette gir et viktig supplement til rapporten. Deretter omtales noen teknologiske utfordringer og behovet for lovendringer. Til slutt beskrives dagens sikkerhetsutfordringer og håndteringen av dem, jf. rapportens kapittel 21, samt våre betraktinger rundt kompetanse og kapasitet.

NOUen gir, etter vår oppfatning, et meget grundig, godt og dekkende bilde av de digitale sårbarhetene i Norge.

Trusselbildet og eksempler på saker
Internasjonale og nasjonale rapporter gir et bilde av IKT-kriminaliteten som stadig voksende, mer truende i sin form og potensielt skadelig for vår nasjonale økonomi. Industrispionasje og grov organisert IKT-kriminalitet tapper det norske samfunnet for betydelige verdier. Det digitale sårbarhetsutvalget anslår i rapporten dette til 20 milliarder kroner årlig.

Ondsinnet programvare er et bestående problem. Oslo politidistrikt ser økende bruk av "ransomware**"**, som hindrer brukernes tilgang til egne data og presser brukerne for penger. Dette gjelder både privatpersoner og bedrifter og kan medføre store tap for den enkelte ved at det ikke er mulig å gjenskape dataene.

Oslo politidistrikt

200 Ledelse - Kriminalavdeling
Post: Postboks 8101 Dep, 0032 OSLO
Besøk: Grønlandsleiret 44, 0190 OSLO

Tlf: 22 66 90 50
Faks: 22 66 87 37
E-post:

Org. nr.: 961398142
Giro: 7694.05.08319
www.politi.no

For tiden etterforskes en sak hvor en bedrift er forsøkt bedratt for 2,5 millioner kroner ved hjelp av en avansert banktrojaner. Uskyldige borgere i Oslo har uvitende medvirket til bedrageriet. 1,5 millioner ble utbetalt. Saken viser at phishing er et utbredt problem og at manglende sikkerhetsbevissthet i befolkningen og bedriftene er en utfordring. Vi låser våre hjem, men setter døren på vid gap for datakriminelle som i cyberdomenet i praksis står rett utenfor døren til enhver tid.

Vi har videre under etterforskning en sak der de kriminelle har overtatt kontrollen med en persons e-post, antagelig ved bruk av malware, for deretter å få tatt ut 790.000 kroner av personens bankkonto. Saken viser at det fortsatt er utfordringer med bankenes rutiner med kontroll av utbetalinger. Ondsinnet programvare er og vil fortsatt være en betydelig trussel.

Et annet eksempel er saker der borgerne blir oppringt av noen som utgir seg for å være Microsoft Tech Support. Ofte fremstår det som om det ringer fra et norsk nummer. Dette lar seg gjøre ved hjelp av programvare man finner på Internett. Mange lar seg dessverre lure og gir de fra seg informasjon som senere kan brukes til id-tyveri og annen kriminalitet. Ofte befinner svindlerne seg i utlandet, i store call-centres som driver dette profesjonelt. Den organiserte kriminaliteten i cyberdomenet rammer ikke bare Oslos bedrifter, men også den jevne borger.

Økende forekomst av trusler fremsatt over internett truer borgernes ytringsfrihet og har medført en uheldig ungdomskultur. Bak innbrudd i sosiale medier har vi sett eksempler på at det skjuler seg saker om grov vold eller trakassering. Internett oppleves som et rom der politiet ikke er til stede hvor det er fritt frem for straffbare ytinger, trusler og seksuelle krenkelser.

Et ferskt eksempel er en sak der to unge menn filmet seksuell aktivitet med mindreårige jenter, uten at jentene var kjent med eller hadde samtykket til filmingen. De la deretter ut filmene på lukkede Instagram-kontoer, med megetsigende navn som "vibareknuller" og "villetrekanter". Gruppene hadde over 80 følgere. Vi etterforsker også saker der voksne menn kontakter en mengde barn over internett og manipulerer og truer dem til å begå seksualiserte handlinger.

Datakrimenheten har også etterforsket DDOS-angrep. I et av tilfellene hadde en 16 år gammel gutt chattet med en jente via Skype, men da kontakten mellom dem ikke ble slik han ønsket, ble hun og familien utsatt for et DDOS angrep. Etterforskningen viste at gutten, som ikke hadde noen spesielle dataferdigheter, hadde brukt ukelønnen til å kjøpe en mengde DDOS-angrep av en tjeneste på Internett. Andre eksempler er bedrifter som blir truet til å betale løsepenger for å unngå å bli angrepet. DDOS-angrep kan være en form for digitalt hærverk, men kan også være en del av et større angrep, bidra til å skjule ulovlig inntrengning eller brukes i politisk øyemed.

Oslo politidistrikt har sett flere saker med eksempler på såkalt "CEO-fraud" eller "Fraud au President". Fremgangsmåten ser ut til ha bredd om seg, også i Norge, og går i korthet ut på at de kriminelle kartlegger en bedrifts ledelse og utgir seg for å være konsernets sjef. Deretter kontaktes en underavdeling i et annet land av den angivelige konsernsjefen, som sier han befinner seg på reise og er i ferd med å gjennomføre en stor transaksjon på vegne av konsernet. Ved sosial manipulering og spoofing (forfalskning av telefonnumre og e-postadresser) lures den lokale ansatte til å foreta utbetalingene.

Teknologiske og juridiske utfordringer
Vi har bare sett begynnelsen på kryptering av data. I dag kommer Apple-produkter med kryptering som standard. Dette vil antagelig bli helt alminnelig. Krypteringen gjør det svært utfordrende for politiet å få tak i dataene. Dersom politiet ikke får andre metoder, vil dette i økende grad stenge for politiets etterforskning og forebygging i cyberdomenet. Som følge av sammenvevingen av den digitale og fysiske verden, innebærer kryptering at politiet etter hvert kan få store utfordringer med helt alminnelig kriminalitetsbekjempelse.

I stadig flere sakstyper ser Oslo politidistrikt kryptering og anonymisering. I en aktuell sak er det tatt beslag i et kryptert privat datalager med 13 harddisker som politiet mistenker inneholder overgrepsmateriale. Eier av beslaget nekter å oppgi tilgangsnøkler i avhør, og det har ikke lyktes politiet å knekke krypteringen ved hjelp av teknologi. Det er i økende grad utfordrende å dokumentere distribusjon av overgrepsmateriale. Når vi vet at en del av de som distribuerer slikt materiale også begår overgrep og at bevisføring rundt overgrepsmateriale ofte er viktige i saker om fysiske overgrep, medfører økt bruk av kryptering og anonymisering en risiko for at det også blir vanskeligere å avdekke overgrep mot barn.

En utfordring med etterforskning av IKT-kriminalitet er at det eksisterer så mange muligheter for å være anonym. De kriminelle benytter VPN eller anonymiseringstjenester som TOR, noe som gir tilnærmet fullstendig anonymitet. Dette gjør identifisering av kommunikasjonsanlegg og gjerningsperson svært utfordrende.

Ved kommunikasjon mellom to datamaskiner, vil det så godt som alltid legges igjen spor i form av en IP-adresse. I etterforskning må politiet identifisere hvem som kommuniserte med fornærmedes datamaskin på det tidspunktet det straffbare forholdet fant sted. Informasjon om hvilken abonnent som disponerte hvilken IP-adresse på et gitt tidspunkt er helt sentral i etterforskningen av IKT-kriminalitet fordi den kan identifisere datamaskinen eller brukeren som begikk det straffbare forholdet.

I dag lagres informasjon om hvem som benyttet hvilken IP-adresse i tre uker. Dette betyr at politiet må ha funnet frem til aktuell IP-adresse før det har gått tre uker fra det straffbare forholdet ble begått. Erfaring viser at dette ikke er tilstrekkelig. Blant annet forutsetter det at politiet får kjennskap til forholdet før det har gått tre uker, at politiet har klart å identifisere kritiske spor på et svært tidlig tidspunkt i etterforskningen, og at den kriminelle virksomheten ikke har sitt utspring utenfor Norge.

Større internasjonale etterforskninger ledet av andre lands politimyndigheter, for eksempel mot pedofile nettverk, tar som oftest lang tid. I mange tilfeller får ikke norsk politi kjennskap til saken før IP-sporene er slettet. Dette fører til at etterforskning mot norske involverte i nettverket vanskelig- eller umuliggjøres. Handlingene blir i praksis straffrie. Tilsvarende utfordringer opplever vi når det er nødvendig med rettsanmodninger fra andre land, da prosessen i seg selv er så tidkrevende at det som regel har gått mer enn tre uker før anmodning om utlevering av IP-adresser kan fremsettes.

Identifisering av IP-adresser er helt grunnleggende for etterforskning av IKT-kriminalitet og den korte tiden IP-adressene lagres er en stor utfordring for politiet. Dagens regelverk for lagring gjør at en rekke saker aldri blir etterforsket fordi informasjonen om hvem som

disponerte datamaskinen til gjerningspersonen er slettet. IP-adressene bør lagres i minimum seks måneder.

Den utfordringen kryptering og anonymisering utgjør for politiet, vil øke etter hvert som teknologien forenkler metodene for kryptering og anonymisering og gjør denne mer tilgjengelig for den alminnelige bruker og dermed også de kriminelle. I saken med de 13 krypterte harddiskene kunne den antatte gjerningspersonens vært identifisert og knyttet til det straffbare forholdet før ransaking og pågripelse dersom politiet hadde hatt anledning til å benytte såkalt dataavlesning.

Dagens kommunikasjon og sosialt samvær skjer i utstrakt grad i sosiale medier, e-post og andre meldingstjenester. Dette gjelder naturligvis også kriminelle. Hvis mistenkte nekter å oppgi passord til slike tjenester, må politiet sende en rettsanmodning til det landet der tjenesten er registrert. Erfaringer, blant annet fra drapssaker, viser at det kan ta opp til et år før politiet får svar på slike anmodninger, selv i så alvorlige saker. I tillegg varsler flere tjenestetilbydere brukeren om politiets anmodning. Dataavlesning vil kunne gi politiet tilgang på passord og annen informasjon uten at man er avhengig av gjerningspersonenes samtykke. Manglende rettslig adgang til å benyttet slike metoder har gjort at mange oppfatter det som tilnærmet helt trygt å begå alvorlig kriminalitet ved hjelp av IKT og internett.

Dagens sikkerhetsutfordringer og håndteringen av dem
Den teknologiske utviklingen har medført store endringer i samfunnet de siste tiårene. Samfunnet er i dag avhengig av IKT, både i næringslivet, i offentlig og i privat sammenheng. Dette har medført at IKT er blitt en sikkerhetsutfordring. Infrastrukturen som ligger til grunn for at tjenestene fungerer, har blitt kritisk. DSB overleverte i desember 2014 rapporten «Nasjonalt risikobilde 2014» til Justis- og beredskapsministeren. Rapporten beskriver alvorlige hendelser som det norske samfunnet bør være forberedt på å møte. Målet med rapporten er at aktører som berøres av konsekvensene, eller har en rolle i å forebygge og håndtere kriser, skal få bedre oversikt og innsikt gjennom risikoanalysene som presenteres. «Nasjonalt risikobilde 2014» inneholder totalt 20 scenarioer og to av dem omhandler cyberangrep, henholdsvis cyberangrep mot finansiell infrastruktur og cyberangrep mot ekom-infrastruktur (kap 18). Scenarioet som viser cyberangrep mot ekom-infrastrukturen er utarbeidet av Post og teletilsynet (nå Nkom) og Forsvarets forskningsinstitutt med utgangspunkt i en skisse fra NSM. Scenarioet viser at angrepet vil ramme samfunnet med følgende konsekvenser:

> *Scenarioet omfatter angrep mot Telenors transportnett som fører til at sentrale tele- og datanett faller ut i fem døgn. Den umiddelbare konsekvensen av angrepet er at fasttelefon, mobiltelefon og internett ikke vil fungere eller være svært ustabilt i hele landet. Dette vil i stor grad påvirke kritiske funksjoner i samfunnet som helse og omsorg, transport, finans og evnen til å håndtere krisen. Det vil ikke være mulig å kontakte ambulansetjeneste, politi og brannvesen på telefon. Jernbane- og flytrafikk stopper helt opp. Økonomiske transaksjoner og bruk av betalingsterminaler blir svært begrenset. Krisehåndteringen på alle nivåer blir svært vanskelig på grunn av manglende kommunikasjon og koordinering mellom aktørene og manglende informasjonskanaler til befolkningen. Manglende mulighet til å ringe etter ambulanse eller varsle nødetatene ved akutte hendelser kan medføre 50 ekstra dødsfall. Det økonomiske tapet som følge av cyberangrepet er anslått å bli svært stort – mellom 10 og 20 milliarder kroner.*

Sannsynligheten for et så komplisert angrep vurderes som lav, men det er likevel mulig å gjennomføre. Scenarioet vurderes å ha *lav* sannsynlighet, men med *store* til *svært store* samfunnsmessige konsekvenser. En hovedutfordring innenfor IKT-kriminalitet er å identifisere

hvem som står bak og hva formålet er (kriminalitet, spionasje, terror eller krigføring). I noen tilfeller er angrepskoden kjent og man vil ganske raskt kunne danne seg en oppfatning av angrepet. I andre tilfeller er koden ikke kjent. Innledningsvis er det da svært vanskelig å fastslå hvem som står bak. Dette utfordrer arbeidsfordelingen mellom ulike myndighetsorganer på området.

Vi har beredskap for de fysiske konsekvensene av en alvorlig IKT hendelse, men politiet har i dag begrenset kompetanse til å håndtere de digitale sidene av en slik hendelse. Politiet hverken kan eller bør bygge opp detaljkunnskaper om ulike samfunnskritiske IKT-systemer, men politiet må ha kompetanse, evne og kapasitet til å lede håndteringen av også de digitalt utløste krisene. Vi trenger en "beredskapstropp" i det digitale rom og et beredskapsplanverk som ivaretar håndtering og ledelse av alvorlige IKT-hendelser for å avverge eller begrense skade. De lokale planverk må utfylle og supplere regionalt og nasjonalt planverk, slik at disse henger godt sammen også ved alvorlige IKT-hendelser.

Ansvarsforholdene mellom ulike myndighetsorganer for håndtering av alvorlige IKT-angrep er ikke klare. Rapporten bidrar til ytterligere forvirring rundt hvilke offentlige myndigheter som har ansvar for hva. Politiet har det hele og fulle ansvar for borgernes sikkerhet ved sivile kriser. Rapporten får ikke dette godt frem, selv om dette for så vidt sies helt til slutt i kapittel 21.3.3 om håndtering av alvorlige IKT-hendelser utløst av tilsiktede handlinger. Det fremstår som om politiet ikke har noen rolle hverken i planlegging, forebygging eller avverging av slike kriser. Dermed etterlater rapporten et inntrykk av at andre myndigheter har større ansvar enn de faktisk har. Vi mener det er kritisk for befolkningens sikkerhet å få en rask avklaring av de uklare ansvarsforholdene.

Alvorlige IKT-angrep og IKT-kriminalitet rettet mot kritisk infrastruktur håndteres av NSMs operative avdeling – NorCERT-funksjonen og Cyber Koordineringsgruppen (CKG) i et samarbeid mellom EOS-tjenestene, hvor eierne av kritisk infrastruktur og andre offentlige organer deltar i begrenset utstrekning. Det bør vurderes hvordan (det ordinære) politiets deltakelse i dette arbeidet kan styrkes, uten at dette kommer i konflikt med den nødvendige konfidensialitet som eksisterer i forhold til klausulert informasjon og informasjon fra private aktører som har sensorer utplassert hos seg.

Internett er en integrert del av norske borgeres hverdag, og av hensyn til borgernes sikkerhet bør politiet ha mulighet til å være til stede i denne hverdagen. Politiets deltakelse i arbeidet bør i like stor grad skje i forebyggende øyemed som en del av politiets "patruljering". I det digitale rom har politi og påtalemyndighet mindre muligheter for pågripelse, tiltale og iretteføring, noe som medfører at politiets innsats i det digitale rom i langt større grad enn ellers må rettes mot forebyggende arbeid, herunder bygge opp kunnskap om, stanse og forstyrre kriminell virksomhet. Det er behov for en arena hvor politiet, sammen med andre myndigheter og næringslivet, kan dele og formidle informasjon om IKT-kriminalitet hvor publikum også gis mulighet til å tipse politiet og hvor politiet kan gi informasjon.

IKT-kriminalitet som er egnet for etterforskning kommer ikke til politiets kunnskap. Svært lite anmeldes og informasjon om det som oppdages av ande etater tilflyter ikke politiet. Når politiet likevel får kunnskap om kriminaliteten, har anmelder eller andre etater gjort egne undersøkelser som ikke nødvendigvis ivaretar straffeprosessens krav til bevissikring og rettssikkerhet. Deltagelse i de relevante fora hvor alvorlige IKT-hendelser – CKG og NorCERT - håndteres vil gi politiet nødvendig informasjon for å kunne iverksette etterforskning.

Det arbeides i disse dager med endringer i våre nasjonale beredskapssystemer. Endringene som diskuteres må reflektere at det er politiet som er samfunnets sivile maktapparat og kan gripe inn overfor borgerne ved for eksempel å ta seg inn på annen manns eiendom, påby stenging av virksomhet eller uskadeliggjøre farlige gjenstander. Ingen annen myndighet har slike fullmakter, med mindre vi befinner oss i krig eller en krigslignende situasjon. Prinsippene for samfunnssikkerhet (ansvar, nærhet, likhet og samvirke) er i og for seg hensiktsmessige, men så lenge rollene er uklare risikerer vi sviktende krisehåndtering ved at relevant og riktig myndighet ikke kommer på banen til rett tid.

Kompetanse og kapasitet
Datateknologi tas i bruk i stadig økende grad, også av kriminelle. Næringer og tjenester flytter til den digitale verden, det samme gjør kriminaliteten. Tradisjonelle spor erstattes av elektroniske spor, og vi får flere spor enn tidligere. Dette medfører både utfordringer og muligheter for politiet. Politidirektoratet utførte i 2012 et arbeid med å kartlegge politiets arbeid med IKT-kriminalitet, datatekniske undersøkelser og politiarbeid på nett, og vurderte hvordan det bør arbeides med disse områdene fremover. Arbeidet resulterte i rapporten "Politiet i det digitale samfunnet".[1] Under arbeidet med rapporten, ble det blant annet gjennomført en intervjuundersøkelse blant utvalgte politidistrikt og særorgan, hvorav Oslo politidistrikt var ett av dem. Resultatet av undersøkelsen viste at politiet utfører noe arbeid på Internett, men tilstedeværelsen er ikke god nok. Videre viste undersøkelsen at politiet har små, men gode fagmiljøer for undersøkelser av elektroniske spor. Den begrensede kapasiteten medfører at denne kompetansen brukes i hovedsak bare i de aller mest alvorlige sakene. I de alvorlige, men ikke aller mest alvorlige sakene, blir elektroniske spor sjeldnere undersøkt. Alle politidistriktene som ble intervjuet mente at det var store mørketall innenfor IKT-kriminalitet. En stor del av de sakene som blir anmeldt, henlegges. De sakene som politidistriktene etterforsker innenfor IKT-kriminalitet, etterforskes både ved hjelp av tradisjonelle etterforskningsmetoder (for eksempel avhør) og ved hjelp av datatekniske undersøkelser.

Vi ser et behov for å bygge kompetanse og kapasitet fremover knyttet til bekjempelse av IKT-kriminalitet. Distriktet bygger solid kompetanse og kapasitet innenfor avanserte datatekniske undersøkelser, men ser behov for å se nærmere på hvordan IKT og internett kan integreres i alt politiarbeid. Ulike kriminalitetsformer som økonomisk kriminalitet, sedelighetskriminalitet og organisert kriminalitet begås i økende grad ved hjelp av IKT og internett. I etterforskning av alvorlig kriminalitet som drap, voldtekt og andre alvorlige hendelser er det stadig større behov for å benytte elektroniske spor og internett i etterforskningen.

I kapittel 21.3.4 sies det at det bare er Oslo politidistrikt som har tilstrekkelig "kompetanse til å møte dagens utfordringer knyttet til IKT-kriminalitet." Dette er en sannhet med modifikasjoner. Det er riktig som det videre sies i rapporten at det alt vesentligste av denne kompetansen og kapasiteten i dag benyttes til etterforskning av annen kriminalitet. Som et første steg på veien mot en mer helhetlig bekjempelse av IKT-kriminalitet arbeider Oslo politidistrikt med å etablere fagkontakter for digitalt politiarbeid i distriktets øvrige fagmiljøer og stasjoner. Vi ser imidlertid at kompetansen, både hos politi- og påtaleansatte, trenger et betydelig løft før vi kan si at vi er rustet for bekjempelse av IKT-kriminalitet i vid forstand.

[1] https://www.politi.no/vedlegg/rapport/Vedlegg_1866.pdf

Teknologibruken vil fortsatt akselerere og vi vil se en stadig større integrering mellom det fysiske og det digitale. Om noen år vil vi kanskje ikke lenger snakke om "IKT-kriminalitet" fordi IKT og internett er integrert i alt. På veien mot en tilsvarende integrering av IKT og internett i "alt" politiarbeid, vil det være nødvendig å vurdere å "kraftsamle" en enhet for digitalt politiarbeid. Den bør ikke bare ivareta digital etterforskningsteknikk som i dag. Den bør også håndterer mye av IKT-kriminaliteten, både den svært teknologikrevende kriminaliteten og der KT og internett benyttes til bedragerier, overgrep, trusler og annen tradisjonell kriminalitet. Etter hvert som andre enheter erverver tilstrekkelig kompetanse og kapasitet til å håndtere de digitale sidene av politiarbeidet, vil en slik enhet kunne spisses mer mot det teknologiske.

Rapporten tar til orde for å etablere et nasjonalt datakrimsenter. Et slikt senter bør i første rekke arbeide med internasjonale saker og nasjonale problemstillinger og være et ressurssenter for distriktene. IKT-kriminalitet i vid forstand må løses i politidistriktene, også selv om den er teknologisk komplisert. En ensidig satsing på et nasjonalt senter vil kunne lede til at resten av politiet blir hengende etter den teknologiske utviklingen. Det vil kunne hemme den samlede kriminalitetsbekjempelsen på sikt.

Oslo politidistrikt har mange prioriterte oppgaver. Vi har også nasjonale funksjoner som krever ressurser. Det er viktig at distriktenes rammer gir mulighet for den omstilling og nyrekruttering som vil være nødvendig for å bekjempe IKT-kriminalitet og videreutvikle politiets tilstedeværelse i det digitale rom. Skal politiet lykkes med forebyggende tiltak som kunnskapsbygging gjennom etterretning, samarbeid med andre etater og næringsliv og andre tiltak som forstyrrer og hindrer de kriminelle aktivitetene, må distriktenes målekriterier tilpasses dette. Kunnskapsbygging og deling har en verdi i seg selv og det bør være like naturlig å åpne en forebyggende sak som en etterforskning.

Fellesoperativ seksjon har påpekt at NOU'en er grundig i sin gjennomgang av den digitale sårbarheten og har forslag til tiltak for å redusere denne sårbarheten.

Det savnes likevel en sterkere vurdering av avhengigheter mellom el-forsyning og bruk av digitale verktøy. Dette er i liten grad berørt bortsett fra i kapittel 11 – Elektronisk kommunikasjon og i kapittel 13 – Energiforsyning. Dagens digitale samfunn er totalt avhengig av en stabil strømforsyning i alle deler av samfunnet. Det hadde derfor vært naturlig å se sårbarheten for el-forsyning og digitale verktøy i en helhet.

Sett isolert fra politiets side er det en utfordring at krav om back-up kapasitet til basestasjoner både for mobilnettet og nødnettet kan måles i timer. Erfaringer fra stormer de siste årene har vist oss at det kan ta dager før normal strømforsyning er gjenopptatt etter kraftig uvær.

Med vennlig hilsen

Gro Smogeli
visepolitimester

Saksbehandler: T. Austad/T.Magnussen/T.Stephansen/ RB

POLITIET

Politidirektoratet
Postboks 8051 Dep
0031 OSLO

SØR-VEST POLITIDISTRIKT

Deres referanse:
Justisdep. 15/8216

Vår referanse:
201600081-2

Sted, Dato
Stavanger, 23.02.16

HØRINGSBREV – DIGITAL SÅRBARHET – SIKKERT SAMFUNN

Det er etter vår mening gjort et svært godt arbeid i forbindelse med utredningen, både i forhold til å gjøre rede for dagens ordninger og slik det fungerer i dag, og i forhold til forslag om nye tiltak.

I vårt svar vil vi ikke kommentere hvert kapittel, men kommentere fellesnevnerne som vi har funnet ved gjennomgangen av utredningen.

Sporbarhet er et hovedpunkt som i særlig grad merker seg ut. De ulike kapitlene tilkjennegir at vi har ulike ekom tjenesteleverandører innenfor de ulike sektorene. Tjenesteleverandørene er private og offentlige, og de har ulik grad av profesjonalitet tilknyttet sin tjeneste/leveranse. Etter vår mening må det være sammenfallende kriterier/mål i forbindelse med sporbarhet. Altså; det må være et minste minimum i forhold til hva som skal være innholdet i loggen, - slik at det kan være mulig å spore tilbake til hvem som har utøvet de ulike handlingene.

De ulike sektorene bør også ha et forum hvor de kan utveksle informasjon og kompetanse om ikt-sikkerhet. Forumet må være på et nivå hvor det er ny kunnskap og informasjon som står i sentrum.

Utredingen trekker frem at olje- og gass-sektoren har en lang sikkerhetstradisjon, og at bransjen driver frem IKT sikkerhetsarbeidet. Flere bransjer/sektorer kan lære av dem hvordan initiativ og felles standarder driver ITK-sikkerhetsarbeidet videre.

Det vil også være viktig å se til de sektorene som har tjenester som samhandler internasjonalt og på tvers av flere sektorer, da de tradisjonelt vil ha et større trusselbilde på grunn av utbredelse, samt flere ulike aktører. De kan være med å forme veien videre for sektorer som ikke er like eksponert.

I og med at det er mange ulike ekom-tilbydere bør det være tydelig fokus på IKT-sikkerhet, og dette bør være nedfelt i forskrifter. Små ekom-tilbydere/selskap må med i IKT-sikkerhetskjeden, og det må avholdes egne sektor- og sektorovergripende øvelser som fokuserer på ekom-/IKT-sikkerhet. Tiltak om tilknytning/bygging av responsmiljø for IKT-hendelser støttes, og de bør forefinnes på sektornivå og i sektorovergripende miljø.

Sør-Vest Politidistrikt

Stavanger
Post: Postboks 240, 4001 STAVANGER
Besøk: Lagårdsveien 6

Tlf: 51 89 90 00
Faks: 51 89 91 00
E-post: post.sor-vest@politiet.no

Org. nr.:
Giro:
www.politi.no

Vi må forholde oss til nasjonale og internasjonal ekom-tilbydere/selskap. Selskapene jobber ut fra ulike lover, retningslinjer og forskrifter, og har ulik tilnærming til personvern. Vi må ikke få en situasjon hvor for eksempel private setter standarden for registrering og behandlingen av personvern, da ekom-tilbydere har for mange og ulike agendaer til å ha et slikt ansvar. Det kan for eksempel nevnes siste avsløring om *VIPS-appen* som anonymt sendte brukerdata til Facebook, uavhengig om brukerne hadde Facebook-konto. Det kan ikke være ekom-tilbydere som skal bestemme graden eller formen for ytringsfrihet, ved for eksempel at de kan redigere bort (for dem) upassende meninger/innlegg. Det må være forutsigbarhet, slik at brukeren er kjent med hva tjenesten tilbyr og hvordan den opptrer.

Lagring av ekom antas å bli en voksende bransje, hvor det er nasjonale og internasjonale tilbydere. Utredningen ser for seg en begrenset lagring utenlands, eventuelt at det bør være et sekundært nasjonalt lager av fungerende skyggekopier. Dette tiltredes. Vi må ha nærhet til lagringen, slik at den kan administreres og brukes, selv om det blir helt eller delvis bortfall av ekom.

Skytjenester kan tjene som lagring. Utredningen har nevnt ulike sider ved skytjenester. Felles er at bruken av skytjenester øker i omfang, både privat og hos arbeidsgiver. Det er behandlingsansvarlig som er ansvarlig for forvaltning av opplysningene. Skytjenester lager data i "skyen" og brukeren har ikke kontroll eller nærhet til hvor de fysiske dataene befinner seg. Dette utgjør en risiko for at data/tjenesten kan misbrukes eller kompromitteres av andre. Snowden-avsløringen viste tydelig hvordan en statsmakt hadde skaffet seg "fri tilgang" til metadata og innholds-data fra store leverandører slik som Google, Microsoft, Yahoo, Skype m.m. Det må legges til grunn at dette også forekommer i dag, noe annet vil være naivt å tro. Skytjenester har fysiske lagringsparker i ulike kontinenter og land, som har helt andre regler/lover og styresett en Norge. Vi risikerer å miste råderett og nærhet til dataene. Vi stiller oss bak vurdering og tiltak slik som foreslått i punkt 23.7.5 - side 306.

Vi ønsker å knytte noen bemerkninger og tanker til kapittel 11 – elektronisk kommunikasjon.

Under flom og andre uforutsette hendelser har vi erfart at det har vært helt eller delvis utfall i Telenor sin kjerneinfrastruktur (mobilnettet). Ut fra vårt syn det dette svært kritisk, da vi mottar og sender kommunikasjon gjennom denne kanalen. Ved fullt eller delvis bortfall når vi ikke frem med, eller klarer å motta, tidskritisk informasjon. Følgelig støtter vi utvalgte sin tilrådning om å redusere kritikaliteten av Telenors kjerneinfrastruktur. Vi er positive til det igangsatte arbeidet med CSIRT for ekom-sektoren.

Videre deler vi bekymringen vedrørende at ekom er under press og at selskaper konsoliderer virksomhetene sine ved å sentralisere tjenesteproduksjonen til et land, for så å tilby ekom på tvers av landegrenser. Reduksjon av bemanning og tjenesteutsetting/flytting av ekom utenfor Norges grenser gjør samhandling vanskeligere. I et samfunnssikkerhets- og etterforsking-perspektiv er politiet avhengig av samhandling med ekom-tilbydere, og at samhandlingen i tidskritiske situasjoner kan skje fort. Når norske tjenester er lokalisert og jobber under ulike jurisdiksjoner, nasjonale sikkerhetskrav og beredskapsplanverk vil det erfaringsmessig gjøre samhandlingen mer krevende.

Avslutningsvis ønsker vi å påpeke kapasitet- og kompetanseutfordringer knyttet til håndteringen av digitale angrep. Mørketallundersøkelsen avdekker at det er manglende rapportering/anmeldelser av IKT-kriminalitet. Politiet etterforsker i relativet liten grad IKT-

kriminalitet, da slik etterforsking er vanskelig og tidkrevende og krever samarbeid med eksterne nasjonale og internasjonale aktører. Slik som beskrevet i utredningen ønsker vi et kompetanse- og kapasitetsløft for å gjøre oss i stand til å etterforske og påtaleavgjøre IKT-kriminalitet.

For øvrig mener vi at det er nødvendig med et sektorovergripende kompetanseløft for å kunne ivareta nåværende og fremtidens IKT-sikkerhet.

Med hilsen

Hans Vik
Politimester

Saksbehandler:
Knut Erik Rame
Politioverbetjent