VESTFOLD, TELEMARK OG BUSKERUD STATSADVOKATEMBETER

Politimester Ole B. Sæverud
Sør-Øst politidistrikt
Postboks 2073
3103 TØNSBERG

REF.: VÅR REF.: DATO: 31.01.2023

RAPPORT ETTER INSPEKSJON AV SØR-ØST POLITIDISTRIKTS ENHET FOR DIGITALT POLITIARBEID (DPA)

1. Innledning:

Vestfold, Telemark og Buskerud statsadvokatembeter har avholdt inspeksjon/tilsyn av arbeidet til Sør-Øst politidistrikts enhet for digitalt politiarbeid (DPA) i uke 50 i 2022. Inspeksjonen ble fra embetets side utført av førstestatsadvokat Anne M. Katteland, statsadvokatene Andreas Christiansen, Åsmund Yli og Vibeke Gjøslien.

Inspeksjoner og tilsyn er en viktig del av statsadvokatenes fagledelse av politiet. Vi har ikke tidligere hatt særskilt tilsyn med politiets enhet for DPA.

Riksrevisjonen har i sin undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT konkludert med følgende, jf. Dokument 3:5 (2020–2021):

- *Politiets evne til å avdekke og oppklare IKT-kriminalitet har klare svakheter som samlet sett er alvorlige.*
  - *Politiet mangler kompetanse innenfor etterforskning av IKT-kriminalitet.*
  - *Tiltakene for å styrke politiets kapasitet til etterforskning av IKT-kriminalitet holder ikke tritt med utfordringene.*
  - *Svakheter ved støttesystemer fører til ineffektiv ressursbruk og manglende oppklaring av IKT-kriminalitet.*
  - *Manglende samordning mellom distrikter gir utfordringer for oppklaring av IKT-kriminalitet.*
  - *Utfordringer ved internasjonalt samarbeid bidrar til lav oppklaring av IKT-kriminalitet.*
- *Politiet mangler oversikt over IKT-kriminalitet.*
- *Politiet prioriterer i liten grad etterforskning og oppklaring av ren IKT-kriminalitet.*

Postadresse: Postboks 2630 3129 TØNSBERG
Kontoradresse: Tollbodgaten 9 3111 TØNSBERG
Telefon: +47 35 58 88 58
E**-post**: post.vtb@statsadvokatene.no

- *Tips og etterretning om internettrelaterte seksuelle overgrep øker og utfordrer politiets kapasitet.*
- *Politiet mangler kapasitet til å møte utviklingen innenfor økonomisk IKT-kriminalitet.*
- *IKT-kriminalitet har i liten grad vært prioritert av Politidirektoratet og Justis- og beredskapsdepartementet.*

På bakgrunn av riksrevisjonens undersøkelse har riksadvokaten i sine føringer for statsadvokatenes fagledelse for 2022 blant annet uttalt følgende, jf. riksadvokatens brev av 27. september 2021 punkt 4:

> *Statsadvokatene bes, i forbindelse med inspeksjoner og eventuell annen fagledelse, sette seg inn i arbeidet til politidistriktenes enheter for digitalt politiarbeid (DPA). Formålet er å legge grunnlag for større aktivitet på fagledelsessiden rettet mot IKT-kriminalitet.*

I riksadvokatens rundskriv nr. 1/2022 Mål og prioriteringer for straffesaksbehandlingen i 2022 er internettrelatert kriminalitet omtalt i flere steder. Riksadvokaten har blant annet fremhevet at:

> *Kriminelle handlinger ved bruk av IKT,* som internettrelaterte seksuelle overgrep*, økonomisk IKT-kriminalitet* som bedragerier, identitetskrenkelser, og *datainnbrudd* eksempelvis med løsepengevirus, representerer utfordringer som setter politiets evne til effektiv og troverdig kriminalitetsbekjempelse på prøve. Oppklaring på dette området er særlig viktig.
>
> *Internettrelaterte overgrep mot barn* er et stort samfunnsproblem, og avgrensning av disse sakene kan by på utfordringer. Det er viktig at påtalemyndigheten tidlig vurderer tilskjæring av etterforskingen.
>
> Politiets innsats mot *alvorlige dataangrep, datainnbrudd*, *økonomisk IKT-kriminalitet* og annen *IKT-kriminalitet* skal intensiveres. Denne kriminaliteten er sterkt økende i omfang og kompleksitet, men relativt få lovbrudd straffeforfølges. For å kunne avdekke flere alvorlige straffbare forhold, er det nødvendig å legge til rette for mer samarbeid mellom politidistriktene, Kripos, Økokrim og næringslivet. Sakene krever høy teknologisk kompetanse. Politiet må rette oppmerksomhet mot sikring og bruk av digitale bevis. Dersom sentrale samfunnsinstitusjoner blir utsatt for dataangrep, må det også legges til rette for samarbeid med PST.

Alvorlig IKT-kriminalitet er også fremhevet som et særskilt prioritert område som skal ha forrang ved knapphet på ressurser i politidistriktet, jf. riksadvokatens prioriteringsrundskriv punkt V 1.

Det kan således oppsummeres med at bekjempelse av ulike former for internettrelatert kriminalitet står høyt på agendaen hos den høyere påtalemyndighet som følge av den sterke økningen i disse sakene i samfunnet i dag.

I den videre fremstillingen brukes begrepet IT-kriminalitet i stedet for det tidligere brukte "IKT-kriminalitet". Begrepet IT-kriminalitet kan deles i 3 undergrupper: (1) internettrelaterte seksuelle overgrep, (2) økonomisk IT-kriminalitet (bedragerier og identitetskrenkelser) og (3) «ren» IT-kriminalitet (datainnbrudd og uberettiget befatning med tilgangsdata).
.

I denne rapporten er begrepet IT-kriminalitet brukt som en fellesbetegnelse som favner alle de tre undergruppene med mindre annet fremgår særskilt av sammenhengen.

2. Gjennomføringen av inspeksjonen

Inspeksjonen ble gjennomført ved at statsadvokatembetet har mottatt informasjon fra ledelsen i politidistriktet om hvordan dette arbeidet er organisert og hvordan distriktet selv oppfatter situasjonen på dette fagområdet. Vi har som en del av tilsynet også gjennomført samtaler med personell som jobber på DPA, personell som har erfaringer med bruk av tjenestene til DPA og noen mellomledere som er tilknyttet dette. Samtalene ble gjennomført enkeltvis med de aktuelle medarbeiderne tirsdag 13. og onsdag 14. desember 2022. I samtalene ble det særlig rettet oppmerksomhet mot den enkeltes kompetanse og erfaringer med etterforskning av IT-kriminalitet og samhandling både internt i distriktet og utenfor eget distrikt. I kapitlene 3 til 7 redegjøres det for den situasjonsbeskrivelsen som vi har mottatt fra distriktet pr. medio desember 2022.

Formålet med inspeksjonen er, som nevnt over, å få innsikt i arbeidet til politidistriktets enhet for DPA slik at dette igjen kan danne grunnlag for større aktivitet på fagledelsessiden på området IT-kriminalitet i tiden fremover.

3. Organiseringen i politidistriktet

3.1 Organisering av DPA

I Sør-Øst politidistrikt ligger Digitalt politiarbeid (DPA) organisert som en egen seksjon under Felles enhet for etterretning og etterforskning (FEE). Seksjonen er ikke videre delt opp i avsnitt, men er lokalisert på to steder, henholdsvis Drammen og Skien. Seksjonen har ikke eget sakstrekk og er derfor en ren bistandsseksjon mot andre etterforskningsmiljøer i FEE og ved de geografiske driftsenhetene (GDE).

Organiseringen av seksjonen er gjort som følge av nærpolitireformen og en arbeidskravsanalyse etter følgende oppdrag gitt gjennom "rammer og retningslinjer for etablering av nye politidistrikt":
- sørge for at riktig og relevant digital informasjon sikres, analyseres og benyttes i politiarbeidet til rett tid ved å gjøre mer arbeid med sikring og foreløpig gjennomgang av digital informasjon på åstedet
- tilrettelegge for at hele politiet kan være til stede på internett og utføre politiarbeid der, blant annet ved kriminalitetsforebyggende nettpatruljer (denne er i etterkant overført til enhet for forebyggende)
- sørge for at de ulike fagmiljøene, som etterforskning og kriminalitetsforebygging, har kompetanse til å forstå og utføre enklere sikring og gjennomgang av digital informasjon
- bistå med sikring og tilrettelegging av digital informasjon, utføre de mest anvendte datatekniske undersøkelser av nettverksdata og digitale enheter som ikke krever spesielle, kostbare laboratoriefunksjoner
- bistå med å forebygge og etterforske IT-kriminalitet der etterforskningen er svært teknologikrevende, og sørge for at disse håndteres med tilstrekkelig datateknisk kompetanse

Som følge av utviklingen i teknologien og kriminalitetsbilde har også disse oppdragene utviklet seg siden de ble skrevet. Moores lov som tilsier at antall transistorer pr. integrerte krets dobles hvert andre år, samtidig som kostnaden halveres, forteller om den eksponentielle økningen i datakraft og tilgjengelighet for befolkningen. Moores lov vurderes av mange til å ikke lenger være gyldig, men den gir fremdeles en god beskrivelse av hvordan utviklingen har vært frem til nå. Dette i seg selv er ikke utfordringen, men det åpner for nye muligheter for teknologibedriftene til å utvikle produktene sine videre. Eksempelvis er det vanskeligere å gjennomføre foreløpig gjennomgang på stedet dersom man har til hensikt å beholde beslagets integritet. I tillegg fører økende bruk av kryptering til at tilgangen til denne dataen blir mer utfordrende. Og dersom man får tilgang er mengden data betydelig større enn hva den var for få år siden. Realiteten blir derfor at DPA i 2022 anslagsvis bruker 70-80% av tilgjengelig kapasitet til å sikre elektroniske spor fra mobiltelefoner, datamaskiner og skytjenester og deretter tilrettelegge for gjennomgang til etterforsker.

3.2 Bemanning DPA

Seksjonen består av 14 stillingshjemler. I desember hadde en medarbeider sagt opp sin stilling, og denne personen skal bli erstattet. Samlet vurderes seksjonen å ha lav utskifting av ansatte med unntak av seksjonssjef som har vært byttet ut flere ganger de siste årene.

Stillingene fordeler seg slik:

Drammen:
1 x seksjonssjef (sivil)
6 x dataetterforskere på elektroniske spor (4x politi, 2x sivil)
1 x etterforsker med spesialkompetanse innen telekommunikasjon og nettverk (sivil)
1 x etterforsker med spesialkompetanse innen OSINT og kryptovaluta (politi)
1 x etterforsker med spesialkompetanse innen IT-kriminalitet (politi)

Skien:
4 x dataetterforsker innen elektroniske spor (3x politi, 1x sivil)

Alle de ansatte har en eller flere tilleggsoppgaver som går utover deres kapasitet til å drive produksjon. Under beskrives et utvalg av de funksjonene som noen av de ansatte har som ikke er direkte produksjon (i tillegg til seksjonsleder). Anslagsvis utgjør dette 2-3 årsverk som ikke blir benyttet direkte inn i produksjon:

- Én dataetterforsker innen elektroniske spor har funksjon som oppdragskoordinator og registrerer og fordeler alle innkommende bistandsanmodninger som kommer til DPA. Funksjonen krever tett koordinering med seksjonssjef som sitter med drifts- og resultatansvaret for seksjonen og er seksjonssjefens nærmeste rådgiver.
- Én ansatt har ansvar for å drifte, vedlikeholde og oppdatere seksjonens infrastruktur som maskinpark, servere og nettverk. Kompleksiteten i kravene til infrastrukturen er høyere enn hva PIT lokalt har evne til å drifte, så ansvaret for dette ligger derfor hos DPA for å sikre at løsningene er tilpasset seksjonens særlige behov. Dette gjøres ved siden av å være dataetterforsker.
- Én dataetterforsker videreutvikler metoder som eksempelvis implementering av fjernløsning for gjennomgang av sikringer (løsningen er kjent som DPAD – digitalt politiarbeid desktop) og utvikling av verktøy for datahåndtering. Dette gjøres på siden av å være dataetterforsker.

- Én dataetterforsker forvalter oversikt over lisensavtaler som DPA og øvrige seksjoner i FEE benytter. Dette innebærer et koordineringsansvar opp mot PIT som forvalter kontraktene nasjonalt, samt kontinuerlig vurdering av behov og bruk for å sikre at forvaltningen av tildelte midler benyttes mest mulig effektivt. Dette gjøre på siden av å være dataetterforsker.
- Etterforskeren med spesialkompetanse innen IT-kriminalitet videreutvikler plan for å etablere egenevne på tvers av DPA og Seksjonen for Økonomi- og Miljøkriminalitet innen etterforskning av IT-kriminalitet.

3.3. Organisering i GDE

På GDE'ene er det ikke personell som jobber fast innen DPA. Det er i stedet etablert et konsept for fagkontakter som skal sikre at kompetansen innen digitalt politiarbeid er tilgjengelig i hele distriktet.

Med fagkontakter menes ansatte i politiet som gjennom intern kursing og tett oppfølging fra DPA vil kunne fungere som rådgivere i egen enhet og som dataetterforskere på saker som krever mindre teknisk kompetanse. Fagkontaktene vil ha en begrenset evne til å sikre, prosessere og analysere, og vil i mange saker i stor grad være avhengig av ekspertisen ved DPA. Ved at DPA står som premissleverandør for metodikk, utførelse og valg av dataverktøy knyttes arbeidet med sikring av elektroniske spor sammen for hele politidistriktet, og man vil få en helhetlig kontroll med kostnadene omkring dette arbeidet.

Distriktet har opplyst at implementeringen av denne ordningen ikke har oppnådd den ønskede effekten av flere årsaker. Pandemien gjorde det vanskelig å gjennomføre kursing, utdanning og samlinger. I mellomtiden har også løsningene for verktøy og infrastruktur endret krav, noe som medfører at dersom det teknisk sett skal være en egenevne til å sikre telefoner ved GDE så vil det kreve betydelige merkostnader for GDE da sikringsstasjoner er stasjonære. Utover dette kreves det verktøy for prosessering og tilrettelegging og øvrig infrastruktur må etableres og resulterer i årlige kostnader som strekker seg fra 200.000-800.000 kr for å inneha en egenevne. For at fagkontakter, som skal ha egenevne til å sikre, skal holde seg med riktig kompetansenivå vil det kreves at de benytter majoriteten av arbeidstiden på faget. Dette er utfordrende å sette i kraft på mindre lokasjoner hvor de ansatte har mange funksjoner som skal dekkes gjennom få stillinger som i tillegg har vakt og turnusordninger.

På bakgrunn av det ovennevnte, etablerte distriktet flere fagkontakter med kompetanse innen DPA fagfeltet som ikke har egenevne til sikringer, men som var ment å benyttes som rådgivere i etterforskninger og kontaktpunkt inn mot DPA i forbindelse med bistand. Dette for å sikre både kvalitet til etterforskningen gjennom en bedre digital strategi, men også effektivisering for DPA ved en økt gjensidig forståelse av DPA.

For fagfeltet IT-kriminalitet er det ingen egenevne på GDE som er etablert gjennom DPA. Årsaken til dette er både at DPA selv er under utvikling for å etablere egenevne på feltet og at denne fagkompetansen må samles i et miljø som kan jobbe på tvers av distrikter. I dag er vurderingen at den tekniske fagkompetansen bør sitte i DPA for å bygge et robust fagmiljø.

3.4. Egen internettgruppe – overgrepsmateriale av barn på internett – OP Dark web

I mars 2020 etablerte distriktet en egen gruppe for å håndtere overgrepsmateriale av barn på internett – overtredelser av straffeloven § 311 på nett. Gruppen er kalt internettgruppen eller OP Dark Web. Gruppen trekker alle § 311-sakene. Mange saker som starter med anmeldelse for overtredelse av § 311 viser etter gjennomgang av databeslag at det også er grunnlag for å etterforske mer alvorlige sedelighetsovertredelser, eksempelvis voldtekter over internett (§ 299 mv). I praksis blir sakene fortsatt etterforsket på internettgruppen. Slike saker kan fort vokse stort i volum og ta mye kapasitet.

Denne gruppen har også ansvaret for å følge opp NCMEC-rapporter fra Kripos og har jevnlige møter hvor de beslutter hvilke saker det skal startes etterforskning i. Gruppen har utarbeidet rutiner for hvilke saker som skal følges opp i straffesporet og hvilke saker som skal følges opp i det forebyggende sporet. Mengden meldinger som kommer synes å være jevnt økende.

Gruppen består pr desember 2022 av en påtalejurist (100%). Distriktet har besluttet å øke påtalekraften og fra nyttår styrkes gruppen med en påtalejurist til, som i praksis deles av to jurister med en halv stilling på hver. På etterforskersiden består gruppen av 5 etterforskere og 1 etterforskningsleder. Gruppen sitter på to lokasjoner, hvorav etterforskningsleder og 3 etterforskere er stedsplassert i Skien og 2 etterforskere i Drammen. Fra nyttår vil det være 1 påtalejurist knyttet til Drammen (nord) og den andre stillingen til Skien (sør).

Både representanter fra internettgruppen og representanter fra DPA gir uttrykk for at de samarbeider godt, og at det er en økende forståelse og økende kunnskap i internettgruppen for etterforskning tilknyttet data og internett mv, og herunder eksempelvis hvor ressurskrevende det kan være for DPA å "bare" sikre innholdet i en mobiltelefon. Det beskrives fra begge sider et godt samarbeidsklima og god dialog opp mot planlagte aksjoner hvor eksempelvis det avholdes planleggingsmøter med DPA i forkant og at DPA er tilgjengelig på telefon eller teams dersom det er noe etterforskerne er usikre på ute på et åsted den aktuelle aksjonsdagen.

4. Kompetanse

4.1. Kompetanse ved DPA

Distriktet legger til rette for at personellet på DPA skal ta utdanning på teknologi og metode gjennom NCFI-emner som tilbys av PHS, samt sertifiseringer og kurs på utvalgte verktøy. Grunnlinjen er at alle ansatte på DPA skal ha NCFI core som minimum (kan gjennomføres etter oppstart i stilling). Alle de ansatte har denne modulen, eller tilsvarende kompetanse gjennom sivile studier. Majoriteten innehar også NCFI 2 moduler og enkelte på NCFI 3.

Det største kompetansegapet er på verktøy og dybdeforståelse av den dataen som det letes etter sporkilder i. Denne typen kompetanse er viktig. Men det som er helt avgjørende, er at de ansatte holder tritt med den løpende utviklingen, og for å gjøre dette, kreves personlige egenskaper som nysgjerrighet og motivasjon til å løse nye problemer.

Etterforskeren innen IT-kriminalitet er på tilsvarende nivå som øvrige DPA ansatte, men med spesialisering innen en IT kriminalitetsspesifikk retning (NCFI 2C Network forensics and cybercrime) i tillegg til en pågående mastergradsutdanning i informasjonssikkerhet ved

NTNU. Kompetansen politiet ønsker å rekruttere er også en knapp ressurs i næringslivet og andre deler av offentlig sektor. Lønnsnivået på denne kompetansen tilligger derfor på et annet nivå enn hva som tilbys i politiet. Eksempelvis lyser NAV ut stillinger som dataingeniør med lønnsspenn opp til ltr. 86 (994.200kr), og næringslivet betydelig høyere enn dette.

4.2. Kompetanse ved påtale

Sør-Øst politidistrikt har gjennomført en omorganisering på påtaleenheten den senere tid. I den forbindelse er det med virkning fra oktober i 2022 også gjort endringer i distriktets trekkinstruks.

Seksjon for økonomi- miljøkriminalitet og inndragning (ØMI) har nå fått påtaleansvaret for visse typer IT-kriminalitet. Det omfatter følgende straffebud:

- Straffeloven § 201 – uberettiget befatning med tilgangsdata, dataprogram mv.
- Straffeloven § 204 – innbrudd i datasystem
- Straffeloven § 206 – fare for driftshindring

Frem til nå har saker innenfor disse statistikkgruppene stort sett blitt kodet på ulike generalist-jurister (GDE). Ved å plassere påtaleansvaret over på en spesialseksjon, ønsker politidistriktet å synliggjøre et behov for og en vilje til i langt større grad å legge til rette for økt satsning på en sakstype hvor utviklingen ser ut til å peke i retning av økt digital profittmotivert kriminalitet.

Løsningen som har vært valgt frem til nå, har ikke vært optimal men påtaleenheten har stor tro på en klar bedring av den påtalemessige oppfølging av disse anmeldelsene gjennom de rokkeringer som nå er gjort. Samtidig erkjennes det at påtalejuristene på ØMI per i dag har for lite kompetanse rundt etterforsking og påtalebehandling, herunder aktorering, av straffesaker som har funnet sted ved bruk av datateknologi. For å bedre på dette, og samtidig forhindre at saker om IT-kriminalitet blir nedprioritert i forhold til andre alvorlige lovbrudd som påtalejuristene på seksjonen steller med, blir ØMI nå styrket med ytterligere tre påtalejurister. I den forbindelse er det tenkt at minimum en av disse skal gis et særskilt ansvar for å følge opp denne type lovovertredelser. Politidistriktet er i den sammenheng innstilt på å bruke en god del ressurser på kurs eller annen type opplæring slik at den eller de som blir ansatt skal oppleve at de blir satset på gjennom å bli tilført nødvendig kompetanse.

I desember ble det opplyst at påtalestillingene hadde vært utlyst, men at det synes å være en utfordring å få rekruttert påtalejurister med ønsket kompetanse.

Det er egne påtalejurister knyttet til internettgruppa som beskrevet foran i punkt 3.2.

5. Digital kapasitet

5.1 Personell

DPAs bistand retter seg for det meste til saker som omhandler seksuallovbrudd, herunder også internettrelaterte seksuelle overgrep. Dette da sakene har høy prioritet i den totale straffesaksporteføljen i distriktet, og omfanget saker er stort. DPAs utvikling siden 2018 har i stor grad vært innrettet mot kapabilitet, samt noen verktøy som har økt kapasiteten. Etter internettgruppens økning fulgte ikke DPA etter i vekst. Dermed er distriktet i dag i en situasjon hvor DPA ikke er skalert for å støtte internettgruppen med deres behov (til tross for at også SEVO er utfordret på kapasitet til å etterforske alle saker som blir oversendt fra Kripos). Høy aktivitet inn i sakene som SEVO trekker gjør at andre saker, herunder økonomisk og ren IT-kriminalitet utgjør en vesentlig mindre del av oppgaveporteføljen per i dag. DPA opplever for øvrig liten grad av henvendelser i saker om økonomisk IT-kriminalitet. I saker om ren IT-kriminalitet antas det å være få henvendelser som følge av få anmeldelser. Det anslås at DPA har bistått i ca. 5 saker i kategorien ren IT-kriminalitet de siste 2 årene.

DPA har som nevnt over en ansatt med fagansvar for IT-kriminalitet (ren IT-kriminalitet, men også kompetanse på økonomisk IT-kriminalitet). For øvrig har ikke DPA kompetanse spesielt tiltenkt denne typen saker. Kompetanse som kan være nyttig i slike saker er for eksempel oppdatert teknisk spisskompetanse innen helt konkrete emner, som internett/webutvikling, sky- og nettverksinfrastruktur og lignende hvor det kreves utdanning og erfaring som dataingeniør eller utvikler.

Det er ingen særskilt etterforskerenhet i distriktet som har sak- og trekkansvar for ren eller økonomisk IT-kriminalitet. Ren IT-kriminalitet fordeles til GDE, og økonomisk IT-kriminalitet fordeles til GDE eller FEE avhengig av alvor i den enkelte sak. Spisskompetansen på den tekniske delen av disse kriminalitetsformene er derfor i hovedsak konsentrert hos DPA, og da hos en enkelt ansatt.

5.2 Infrastruktur

Distriktet har i dag egen infrastruktur for lagring av digitale beslag som er sikret eller klargjort for gjennomgang. Det er egne løsninger for Skien og Drammen. Disse nettene er ikke sammenkoblet og de er ikke tilgjengelige i hele distriktet, men fra enkelte lokasjoner kan man koble seg til fra egne enheter mot beslagsnettet i Drammen. DSB-nettet er da bærende for kommunikasjonen mellom enheten og beslagsnettet. DSB er for øvrig tilgjengelig i Drammen for deling av beslagsfiler mellom distrikt/særorgan. Implementering av DSB i større skala i distriktet er nå påbegynt, og det forventes å ha DSB oppe også mellom Drammen og Skien innen utgangen av 2022.

På programvaresiden er det noe underdekning for verktøy til sikring, prosessering og analyse av fysiske lagringsenheter som er av typen mobile enheter (Mobiltelefon, nettbrett). Innen sistnevnte kategori ser man at det er nødvendig med verktøy som innebærer store kostnader, og det finnes i dag kun ett av dette verktøyet på hver lokasjon (Skien, Drammen). Det finnes flere verktøy for mobile enheter tilgjengelig, men disse benyttes primært på eldre telefoner eller i unntakstilfeller fordi de har støtte for færre enheter.

6. Samhandling/grensedragning med Kripos og andre distrikter

Det foreligger ingen klar grensedragning i samhandlingen mellom distriktet og Kripos/NC3 i saker om IT-kriminalitet. Distriktet vil anmode NC3 om bistand ved behov, og deler av etterforskningen vil i de tilfellene avhenge av kapasiteten og mulighetene til NC3. NC3 har bistått i flere saker på enkeltelementer med god effekt, men en opplevd utfordring er de tilfellene hvor distriktet ikke har den nødvendige kompetansen i påtale og etterforskningsleder-rollen.

Eksempler på utfordrende saker distriktet har etterforsket innen IT-kriminalitet

Sak 15431889 m.fl. (phishing):
I dette komplekset etterforsket distriktet flere saker om økonomisk IT-kriminalitet som ble knyttet til en og samme aktør. Det begynte med saker i Sør-Øst, men det ble raskt konstatert at aktøren rammet enkeltpersoner i hele landet og dermed kunne knyttes til flere saker i andre distrikter.

De straffbare forholdene dreide seg om bedragerier, hvor aktøren fikk fornærmede til å utlevere Bank-ID ved å utgi seg for å være en seriøs jobbportal som inviterte til eksempelvis et jobbintervju og hvor fornærmede måtte logge seg inn med sin Bank-ID for å bekrefte intervjuet. Bank-ID'en ble deretter brukt til å tappe fornærmedes konto og kjøpe kryptovaluta. Fenomenet omtales ofte som phishing.

NC3 bisto aktivt i deler av etterforskningen, blant annet med oversikt over sakene man identifiserte nasjonalt, og internasjonalt samarbeid. Distriktet fikk også bistand av et privat firma som hadde en egeninteresse i undersøkelser da et av deres merkenavn ble benyttet av aktøren i noen av bedrageriene. Firmaet tilførte etterforskningen kompetanse innen enkelte digitale sporkilder (kildekode/domener/sertifikater) som ellers ikke ville vært tilgjengelig. Heller ikke NC3 kunne overta den jobben det private firmaet gjorde av kompetanse og/eller kapasitetshensyn.

En utfordring i denne etterforskningen ble et stadig voksende omfang av både muligheter og sporkilder, samt det faktum at sakene befant seg i flere ulike distrikt og ble registrert og håndtert ut fra geografisk plassering. Det lot seg ikke gjøre å samle sakene under en ledelse hos hverken Kripos, Økokrim eller i distrikt. Kripos viste til at distrikt må lede og "eie" saken. Da etterforskningen i distriktet var ledet av en GDE medførte det at påtaleansvarlig og e-leder hadde utfordringer med å forstå innholdet i saken etter hvert som etterforskningen beveget seg. De hadde også begrenset kapasitet til å være tett på, og begrenset mulighet til å styrke etterforskningen med ressurser. Hele komplekset ble til slutt henlagt, da det ikke lot seg å gjøre å drifte etterforskningen på hensiktsmessig måte videre i GDE eller FEE. På bakgrunn av den etterforskningen som var gjort stod i politiet denne saken med etterforskningsmuligheter og kunnskap om aktøren som var relativt unikt for en slik type sak, på henleggelsestidspunktet.

Aktøren var fortsatt aktiv i sitt kriminelle virke da saken ble henlagt tidlig 2022, og det har vist seg at i tiden frem til i dag har aktøren fortsatt sin virksomhet og begått en rekke nye bedragerier (kilde til kunnskap om dette har vært det aktuelle private firmaet, som har fulgt aktørens aktiviteter relativt tett i forlengelsen).

Sak 15367776 (løsepengevirus):
I februar 2021 ble en enhet i en av distriktets kommuner utsatt for et datainnbrudd med løsepengevirus. Saken ble prioritert, men det viste seg vanskelig å få nødvendige data for analyse fra et privat hendelseshåndteringsfirma som var involvert. Distriktet ble orientert mens hendelseshåndteringen var aktiv, og hadde dialog med både fornærmede og hendelseshåndteringsfirmaet.

Resultatet av etterforskningen ble til slutt en rapport fra hendelseshåndteringsfirmaet. Distriktet tilkjennegir at de skulle gjerne gjort egne analyser basert på grunnlagsmaterialet som firmaet baserte sin rapport på, men dette materialet fikk distriktet aldri i hende. Firmaet brukte lang tid på å svare på henvendelser og basert på tiden som gitt, minimale konsekvenser av angrepet, ble det til slutt ikke lenger ansett relevant med ytterligere egne analyser.

Saken viste at samarbeid mellom privat firma (som nødvendigvis må engasjeres av fornærmede for tidligst mulig å oppnå kontroll og normalisere drift) og politiet kan være en utfordring i initialfasen av slike saker. Erfaringen tilsier at politiet i samarbeid med fornærmede tidligst mulig må inn i håndteringen og påvirke slik at nødvendige data av relevans for en etterforskning ikke går tapt, kommer politiet tidlig i hende og dermed kan følges opp. Politiet må også enten selv eller i samarbeid med fornærmede, hendelseshåndterere og sørge for notoritet ved sikring av data som senere kan bli benyttet som bevis.

7. Distriktets egen vurdering av behovet for styrket kapasitet knyttet til IT-etterforskning

Personell
Dersom det skal utvikles egenevne til å etterforske saker innen økonomisk og ren IT-kriminalitet er distriktets vurdering at ny kompetanse må rekrutteres spesielt innen teknisk etterforskning. Kompetansen som behøves vil være mer spisset utviklerkompetanse innen ulike områder avhengig av hvilken type IT-kriminalitet man ønsker å bygge evne innen. Det er heller ikke kapasitet innen dagens rammer til å etterforske flere av disse sakene gitt prioriteringen som er i dag.

Kompetanse
Økning av kompetanse innen IT-kriminalitet ses som et behov i distriktet. Da de aktuelle sporkildene er tekniske og potensielt mange og ulike, er dette kompetanse som bør konsentreres, samtidig som en grunnkompetanse må etableres i etterforskningsmiljøer hos FSI og hos påtale. I dag synes kompetansen innen digitale sporkilder og IT-kriminalitet å være mangelfull og det vil være avgjørende at også taktiske etterforskere har en interesse og grunnkompetanse innen det tekniske domenet. Det finnes i dag ikke et system som ivaretar at saker inneholdende slike elementer håndteres og/eller vurderes av ansatte med særlig kompetanse på området.

Spisskompetansen hos tekniske etterforskere til å finne og følge sporkilder antas å måtte rekrutteres da dette er en dybdekompetanse som tar tid å utdanne og som krever en dypere interesse for å kontinuerlig videreutvikle egne ferdigheter i takt med utviklingen i samfunnet.

Infrastruktur
Distriktet vil dra nytte av en mer enhetlig infrastruktur for tilgang til og gjennomgang av digitale beslag enn den som er etablert i dag. Tilgjengelighet er varierende ut fra lokasjon, og det opereres med adskilte systemer på de to DPA-lokasjonene som beskrevet tidligere. Dersom DPA skal støtte GDE i saker om IT-kriminalitet, vil dagens løsning innebære ulike forutsetninger for distribusjon og tilgjengeliggjøring av datafiler avhengig av lokasjon. Dette antas å bedres i første kvartal av 2023 ved implementering av DSB i større omfang.

Programvare
Spesifikke verktøy for analyse av kryptovaluta, stordata og loggfiler fra servere, er i dag ikke tilgjengelig i distriktet. Dette er sporkilder som anses særlig aktuelle i saker om IT-kriminalitet. Seksjon for økonomi- og miljøkriminalitet og DPA har meldt inn behov for verktøy for å følge sporkilder innen kryptovaluta i styringsdialogen til 2023.

Pågående utvikling
Seksjon for økonomi- og miljøkriminalitet, DPA og andre miljøer i distriktet har iverksatt et arbeid for å kartlegge omfanget av IT-kriminalitetssaker (primært utenfor det som dekkes gjennom internettgruppen) og for å vurdere hva det er realistisk å bygge opp egenevne til å etterforske innenfor disse sakskompleksene. Deretter er målet å fremme en plan i linjen som forankres for hvordan denne evnen kan etableres i distriktet. Arbeidet er pågående.

8. Statsadvokatens merknader

Som nevnt innledningsvis er føringene fra riksadvokaten for statsadvokatenes fagledelse for 2022 at statsadvokatembetet skal *sette seg inn i arbeidet til politidistriktenes enheter for digitalt politiarbeid (DPA). Formålet er å legge grunnlag for større aktivitet på fagledelsessiden rettet mot IKT-kriminalitet.* Gjennom dette tilsynet har vi fått et godt innblikk i arbeidet til Sør-Øst politidistrikts DPA-enhet, herunder hvordan de er organisert og hva de i all hovedsak bruker sin kapasitet og kompetanse til. Dette er beskrevet ovenfor i kapitlene 3 til 7.

Selv om riksadvokaten "kun" har bedt statsadvokatene om å "*sette seg inn i arbeidet*" med DPA, finner vi det naturlig å også benytte anledningen til å knytte noen kommentarer til noe av det vi har blitt gjort kjent med under denne inspeksjonen.

Det er mye god fagkompetanse blant personellet i DPA. Vårt klare inntrykk er at medarbeiderne har stor interesse for fagfeltet og et sterkt engasjement og ønske om å bidra til distriktets kriminalitetsbekjempelse av ulike former for kriminalitet som begås over internett. Imidlertid er ressursene i stor grad båndlagt til sikring av mobiltelefoner og andre dataenheter og til bistand for å gjøre innholdet tilgjengelig for etterforskerne. Det er liten kapasitet igjen til å drive fagutvikling og til å bidra aktivt med sin spesialkompetanse inn i en mer komplisert internettrelatert etterforskning.

Omlag 70-80% av enhetens kapasitet benyttes til sedelighetssakene, herunder også til internettgruppas arbeid. På den ene siden så er dette et viktig kriminalitetsområde som skal ha høy prioritet i distriktet. Det er en stor økning av straffesaker med seksuelle overgrep begått over internett og på dette området gjør Sør-Øst politidistrikt en veldig god innsats. Når det i tillegg tas høyde for at det er behov for bistand til andre alvorlige kriminalitetsområder som

eksempelvis drap eller grove narkotikalovbrudd, gjenstår det svært lite eller ingen kapasitet til økonomisk kriminalitet begått over internett og "ren" IT-kriminalitet.

Det er viktig at distriktet tar aktive og konkrete grep for å høyne kompetanse og kapasitet slik at internett ikke blir tilnærmet en lovløs arena for ulike former for kriminalitet og da tenker vi særlig på det som ikke er seksuallovbrudd. Internett som arena for seksuelle overgrep er under en viss overvåkning og følges bedre opp internasjonalt, nasjonalt og også lokalt i Sør-Øst ved internettgruppa – selv om det også her må legges til grunn at det er store mørketall og politiet nok kun får kjennskap til "toppen av isfjellet".

Det gjennomgående inntrykket er at kompetansen og kapasiteten er for lavt jevnt over i distriktet og at politiet ikke er rustet til å håndtere en sak med såkalt "ren" IT-kriminalitet som eksempelvis løsepengevirus eller andre typer datainnbrudd. Det vises til funnene i riksrevisjonens undersøkelse som er omtalt innledningsvis i punkt 1. De to konkrete sakskompleksene som er omtalt ovenfor kapittel 6 viser at dette også gjelder for Sør-Øst politidistrikt.

Det er uheldig at phishing-saken ikke ble etterforsket videre, men vi har samtidig forståelse for at det ble slik grunnet manglende kompetanse både hos påtale og etterforsker på GDE. Ingen av de hadde erfaring med etterforskning av en slik sak. Kunnskapen som politiet tilegnet seg under etterforskningen har i ettertid blitt benyttet i det forebyggende sporet og det er positivt. Men denne saken viser tydelig at distriktet har et stykke å gå for å oppnå tilfredsstillende kapasitet på dette fagfeltet. Det er viktig at distriktet fremover ruster seg bedre og setter seg i stand til å håndtere en tilsvarende sak neste gang anledningen kommer. Det er nok ikke snakk om "hvis" en tilsvarende sak dukker opp, spørsmålet er heller "når" det skjer.

Fagkontaktordningen fungerer ikke i dag slik den var tiltenkt. Formålet med ordningen synes god og vi er av den klare oppfatning at den har et stort potensial for å bidra til å høyne kvaliteten på den internettrelaterte etterforskningen hvis den utbedres og settes i system. Vi har fått beskrevet at det i dag er en frivillig ordning og at det er opp til den enkelte enhet om de utpeker en fagkontakt eller ikke, da gjerne basert på om noen selv ønsker å ha en slik rolle. Videre har det til nå ikke vært et opplegg for opplæring og kursing av aktuelle kandidater. Statsadvokaten er av den klare oppfatning at fagkontaktordningen bør etablereres og styrkes i alle etterforskningsenhetene i distriktet. Det kan ikke fortsette slik som det er nå, med at det er frivillig hvilke enheter som investerer i dette. Å høyne kompetansen på etterforskningen av internettrelatert kriminalitet er ikke en frivillig oppgave, og det kan ikke overlates til den enkelte enhet selv å velge om den vil prioritere dette. Distriktet må videre gi de aktuelle kandidatene tilstrekkelig opplæring/kursing slik at det sikres en lik grunnkompetanse hos alle fagkontaktene. Videre bør de gis adgang til hospitering ved DPA-enheten, idet det antas å gi de viktig lærdom og erfaring samt øke muligheten for et godt samarbeid når de returnerer til sine enheter. I tillegg vil en hospiteringsordning også forhåpentligvis kunne avlaste DPA.

Distriktet bør sette inn tiltak for å øke kompetansen generelt for "brukerne" av DPA om hva som eksempelvis kreves av ressurser for å gjennomføre ulike undersøkelser, eksempelvis "bare" tapping av en mobil. Det er viktig at det skapes forståelse for den samlede pågangen til DPAs bistandsressurser. Dette kan typisk være noe godt opplærte fagkontakter kan bidra til. Det vil alltid være en viss begrensing og knapphet i ressursene politiet har tilgjengelig, da også hva gjelder dataetterforskning, slik at det er viktig å bedre den samlede ressursutnyttelsen og ha et bevisst forhold til å tilskjære saker/etterforskningen og å prioritere

de "riktige" gjøremålene. Fagkontaktene kan være viktige bidragsytere for å heve bestillerkompetansen hos etterforskerne.

Det bør også investeres tid og ressurser slik at DPA også kan drive fagutvikling og kan bistå med spesialkompetanse til etterforskning. I dag er enhetens kapasitet i stor grad bundet opp til produksjon. På kort sikt, har vi forståelse for at det blir slik siden pågangen til bistand er så stor, men dette er neppe en god løsning på litt lengre sikt. Distriktets ledelse må sørge for rammer som legger til rette for en bedre balanse i oppgaveløsningen til DPA-enheten enn det som er tilfellet i dag. Det er viktig at distriktet setter av tilstrekkelig med ressurser – både penger og tid – slik at personellet kan holde seg oppdatert på utviklingen og ha de rette verktøyene til å bistå enhetene med internettrelatert etterforskning. Vi har forståelse for at en del av verktøyene er dyre og at distriktet har en presset økonomi. Men samtidig er det et paradoks at disse verktøyene nok relativt raskt vil bli spart inn dersom etterforskningen også rigges med tanke på inndragning. Det meste av den kriminaliteten det her dreier seg om involverer store økonomiske utbytter for de kriminelle aktørene. Det vises eksempelvis til phishing-saken som er omtalt foran i kapittel 6.

Det er positivt at påtaleansvaret for de "rene" IT-kriminalitetssakene har blitt spesialisert som nevnt ovenfor i kapittel 4.2. Imidlertid er vi også bekymret for rekrutteringen til denne stillingen og håper at dette løser seg. Men selv om påtaleansvaret for disse sakene spesialiseres, er det ikke lagt opp til tilsvarende spesialisering på etterforskersiden. Med mindre sakene faller inn under dagens trekkregler til ØMI på etterforskersiden (over kr 500 000), er etterforskningsansvaret lagt til GDE hvor kompetansen generelt er lav hva gjelder IT-kriminalitet. Vi er derfor svært usikre på hvor stor effekt det vil ha å bare spesialisere påtalefunksjonen og oppfordrer distriktet til å vurdere å spesialisere etterforskerfunksjonen også.

Det er positivt at distriktet har etablert en egen intern arbeidsgruppe som jobber med forslag til tiltak for å heve kompetanse og kapasitet på internettrelatert etterforskning. Vi ser frem til å følge dette arbeidet videre og er spente på hva som kommer ut av det. Internettrelatert kriminalitet er kommet for å bli, og det må antas at fenomenet bare vil øke i tiden fremover. Det er viktig at politiet har en målrettet strategi og rigger seg slik at de henger med i utviklingen.

Vi takker politiet for velvillige og gode bidrag til inspeksjonen og ønsker lykke til i det videre arbeidet.

Med vennlig hilsen

Anne M. Katteland
Embetsleder

Vibeke Gjøslien
Statsadvokat

Kopi:
Riksadvokaten
Politidirektoratet
Påtaleleder Kjell Johan Abrahamsen

Leder FEE: Lena Reif
Seksjonssjef DPA: Magnus Moe
Påtaleleder ØMI: Jan Stapnes