POLITIET
KRIPOS

Cyberkriminalitet 2023

Politiets årlige temarapport om kriminalitet mot datasystemer og kriminalitet støttet av datasystemer

Cyberkriminalitet 2023, Kripos
Politiets årlige temarapport om kriminalitet mot datasystemer og kriminalitet støttet av datasystemer

Grafisk formgivning: Økokrim
Foto: Shutterstock, utenom s. 49, Pixabay
Opplag og trykk: 1 000x, Aksell

Forord

Trusselbildet i det digitale rom blir stadig mer komplekst. Omfanget av kriminaliteten er stort. Norge er et attraktivt mål for kriminelle i utlandet. Vår geografiske plassering langt nord er ingen beskyttelse i det digitale rom. Truslene er sammensatte, og verktøyene og virkemidlene som rettes mot oss er i stadig utvikling.

Teknologi er en betydelig driver for så godt som alle kriminalitetsutfordringer og trusler mot norske verdier. Den teknologiske utviklingen bidrar til at alle prosesser i samfunnet kan gå raskere, og påvirker samtidig selve endringshastigheten. Teknologier som kryptovaluta, anonymiseringstjenester, kryptering og nye betalingstjenester misbrukes til utpressing, hvitvasking og annen kriminalitet.

Cyberkriminalitet handler til syvende og sist ikke om hendelser, men handlinger. Det handler om gjerningspersoner med kriminell intensjon og global rekkevidde, med vilje og evne til utføre et bredt spekter av lovbrudd. Denne viljen og evnen må møtes med samlet motkraft fra det private og offentlige Norge.

Kripos er gitt i oppdrag av Politidirektoratet å produsere et nasjonalt situasjonsbilde for cyberkriminalitet 2023 med fremtidsrettede vurderinger, i produktkategorien grunnleggende etterretning etter politiets etterretningsdoktrine.

Nasjonalt cyberkrimsenter ble offisielt åpnet i januar 2019, som en avdeling på Kripos, som er politiets nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet. Dette er den første årlige strategiske temarapporten om cyberkriminalitet som Kripos har publisert siden 2017. Rapporten, og arbeidsmetodikken bak, vil understøtte framtidige rapporter fra politiet, og spesielt hovedproduktet politiets trusselvurdering.

Kripos ønsker med denne rapporten å bidra med vår kunnskap om cyberkriminaliteten, dens målrettethet og natur, og med begrepsapparatet vi benytter i vårt arbeid.

Kristin Kvigne
Sjef Kripos


NumLk
7
Home
CYBER
CRIME

Innhold

Dagens trusselbilde – sammendrag

Norge er et gjennomdigitalisert samfunn. Samtidig har deler av befolkningen forholdsvis liten kunnskap om digitale trusler, og den nasjonale sikkerhetstenkningen er fortsatt umoden. Dette gir de cyberkriminelle et større handlingsrom. Cyberkriminelle tar raskt ny teknologi i bruk, og er også raske til å utnytte oppdukkende sårbarheter.

Cyberkriminaliteten er dynamisk og flyktig av natur. Trusselbildet preges av opportunistiske gjerningspersoner, mange tjenestenektangrep, vedvarende uttesting av digitale sårbarheter og en pågående kommersialisering av kriminaliteten som bidrar til effektivisering av lovbrudd og vanskeliggjør etterforskning og straffeforfølgelse. Hovedvekten av kriminalitet mot datasystemer i Norge er opportunistisk og motivert av vinning.

Digitale bedragerier er utbredt og økende. Det er også mer svindel knyttet til BankID, sosial manipulasjon og investeringsbedragerier. Kripos har registrert en mindre nedgang i kriminalitet mot datasystemer, men har sett økt hyppighet av phishingforsøk og mer kriminalitet mot skytjenester.

Seksuelle overgrep mot barn begått med internett som redskap er en stabil og vedvarende kriminalitetstrussel. Gjerningspersonene utgjør en stor og sammensatt gruppe, med mange ulike modi og arenaer.

Gode muligheter for å utveksle tanker og erfaringer på både det åpne og det mørke nettet gjør at trender og nye oppdagelser raskt får effekt. Meningsutvekslingen er også med på å normalisere kriminaliteten. Dette er spesielt bekymringsverdig for seksuallovbrudd, der normaliseringen resulterer i en eskalering av grovhet, konsekvenser og stadig yngre ofre og gjerningspersoner.

Kripos registrerer svingninger i cyberkriminaliteten. Periodevis har det vært mindre volum om sommeren og mer aktivitet i høst og vintermånedene. Disse svingningene kan delvis forklares av ulike forhold, både samfunnsmessige,

geopolitiske, sikkerhetsmessige og teknologiske. Globale hendelser påvirker gjerningspersoners handlingsrom, kapabilitet[1], intensjon og vilje til å utføre cyberkriminalitet mot norske verdier.

De siste tolv månedene melder flere virksomheter om en nedgang i cyberkriminalitet, og peker på kombinasjonen av økt bevissthet og forebyggende arbeid, samt to år med pandemi og Russlands krig mot Ukraina, som mulige årsaker.

Lovarbeidet ligger etter utviklingen. Regulering vanskeliggjøres av at cyberkriminaliteten er grenseløs, mens lovgivningen begrenses av nasjonale grenser og av at de eksisterende internasjonale initiativene foreløpig ikke strekker til for en helhetlig og effektiv håndtering av trusselen. Dette kombinert med store mørketall og en lav anmeldelsesrate gjør at cyberkriminelle opplever en lav oppdagelsesrisiko og en enda mindre sjanse for å bli straffeforfulgt.

[1] Med kapabilitet menes i denne rapporten summen av en gjerningspersons ferdigheter og tilgjengelige ressurser. Et eksempel kan være en gjerningspersons datakyndighet, sammen med tilgang til programvare og personsensitiv informasjon.

Politiet vil også framover ha behov for informasjon om hva det norske samfunnet utsettes for av cyberkriminalitet, enten via anmeldelser eller gjennom informasjonsdeling.

Innledning

For å bekjempe trusselen fra cyberkriminalitet er det avgjørende at de viktigste samfunnsaktørene samarbeider og leser situasjonen likest mulig, samt at informasjonen mellom dem flyter lettest mulig. Det er viktig å utvikle et felles begrepsapparat og arbeide med like parametere for å kunne avdekke avvik og hurtig treffe samordnede og riktige tiltak. En virksomhets modenhet i å verge seg mot cyberkriminalitet avhenger blant annet av kunnskap om politiets rolle, politiets mandat og hva politiet kan bidra med.

Cyberkriminalitet utgjør en tverrsektoriell og grensekryssende trussel mot både privatpersoner og private og offentlige virksomheter i Norge. Det totale kriminelle trykket på norske borgere og virksomheter fra det digitale rom er betydelig. Enkelte samfunnssektorer og grupper er mer utsatte enn andre. Med digitalisering, og teknologisk utvikling generelt, følger først og fremst nye muligheter for legitim bruk, men også kriminelt misbruk.

I denne rapporten redegjør Kripos for det nasjonale situasjonsbildet for cyberkriminalitet slik det framstår for politiet. Rapporten beskriver også en forventet utvikling for 2023, og er ment å bidra til den påkrevde felles innsatsen gjennom å dele politiets kunnskap og vurderinger.

Rapporten skal videre bidra til et bedre kunnskapsgrunnlag for politiet i det forebyggende arbeidet med å redusere trusselen fra cyberkriminalitet. Kripos ønsker også å styrke politiets evne til aktivt å avdekke, forebygge og avverge alvorlig cyberkriminalitet, og straffeforfølge kriminelle gjennom etterforskning og påtale.

Datagrunnlaget for rapporten er i hovedsak fra 2021 og 2022. Norske kilder har blitt prioritert. Straffesaks- og etterretningsregister har blitt benyttet. Datagrunnlaget bygger også på informasjon innhentet gjennom besvarelser fra utvalgte private og offentlige samarbeidspartnere. Disse har bidratt til det samlede situasjonsbildet i betydelig grad. Politiet vil også framover ha behov for informasjon om hva det norske samfunnet utsettes for av cyberkriminalitet, enten via anmeldelser eller gjennom informasjonsdeling.

Analysen har tatt utgangspunkt i å beskrive cyberkriminelle aktører og

nettverk. Underveis har det også vist seg nødvendig å beskrive fenomener, sårbarheter og ofre. Analysen presenteres på tvers av kriminalitetstyper, for å tydeliggjøre drivere og andre fellesnevnere. Informasjon om aktører, nettverk og organisering gjenfinnes under disse overskriftene. På denne måten ønsker vi å lette arbeidet med å identifisere punkter hvor eventuelle tiltak kan ha størst effekt.

Begrepsavklaringer

Det finnes ingen etablert universell definisjon av *cyberkriminalitet*. Kripos definerer i denne rapporten cyberkriminalitet som helheten av to kriminalitetstyper: Kriminalitet mot datasystemer[2], og kriminalitet støttet av datasystemer.

Kriminalitet mot datasystemer kan ikke begås utenfor det digitale rom. Denne kriminaliteten rammer datasystemer direkte. Eksempler er tjenestenektangrep og løsepengevirus.

Kriminalitet støttet av datasystemer er kriminalitet som fantes før det digitale rom oppstod, men som nå også kan støttes av eller gjøres enklere ved bruk av datasystemer. Eksempler er bedragerier, seksualforbrytelser og kjøp og salg av narkotika og ulovlige våpen, som utføres både med og uten støtte fra datasystemer. Publisering av hatefulle ytringer i sosiale medier og digital oppbevaring av overgrepsmateriale inngår også i denne kategorien.

Det finnes ingen universell uttømmende liste over kriminalitet støttet av datasystemer. Følgelig er ikke alt som kan kalles cyberkriminalitet, redegjort for i denne rapporten. Kripos sitt mandat er *organisert og annen alvorlig kriminalitet*, og det er også avgrensningen for denne rapporten.

Det digitale rom refererer oftest til en global helhet av sammenkoblede datasystemer og informasjonsressurser, og brukes som en metafor på linje med begrepet *det offentlige rom*. I denne rapporten betegner det digitale rom helheten av datasystemer, nettverk, enheter og programvare hvor cyberkriminalitet begås.

Internett er et globalt nettverk av mindre digitale nettverk, systemer og enheter som er koblet sammen gjennom en felles kommunikasjonsprotokoll. Cyberkriminalitet finner sted i ulike deler av internett. Den delen av internett folk flest benytter kalles også *det åpne*

[2] Et datasystem er én eller flere datamaskiner, programvarer eller annet datautstyr som kommuniserer i et digitalt økosystem.

nettet. *Det dype nettet* er summen av alt på internett som ikke er indeksert og direkte søkbart ved bruk av standard søkemotorer. Det meste består av lovlig innhold, som adgangskontrollerte databaser og innhold bak betalingsmurer. *Det mørke nettet* er en liten del av internett som består av nettverk som ofte bruker egne kommunikasjonsprotokoller. For å navigere i disse nettverkene kreves spesialisert programvare.[3] Likemannsnettverk[4] for fildeling og TOR-nettverket er eksempler.

Med *skadevare*[5] menes programvare som er laget for å gi uberettiget tilgang til, skade eller lage forstyrrelser i et datasystem.

I denne rapporten brukes ordet *fornærmet* til å benevne både virksomheter og personer som har blitt utsatt for kriminalitet.

---

3 Slik spesialisert programvare er normalt lovlig, åpent tilgjengelig og har et enkelt brukergrensesnitt.

4 Eng: P2P Network; Peer-to-Peer Network

5 Eng: Malware, en sammentrekning av malicious software

> Kriminalitet støttet av datasystemer er kriminalitet som fantes før det digitale rom oppstod, men som nå også kan støttes av eller gjøres enklere ved bruk av datasystemer.

Cyberkriminalitet i Norge

Et bredt spekter av kriminelle med ulike intensjoner utnytter en stor og stadig skiftende sårbarhetsflate i det digitale Norge. Kriminelle tar, som alle andre, i bruk ny teknologi, og dermed får nesten all kriminalitet også en digital side. De kriminelle bruker i tillegg den nye teknologien målrettet for å øke sin slagkraft og for å nå nye ofre og verdier. Med økt digitalisering av samfunnet blir også hver enkelt borger stadig mer avhengig av digitale tjenester. Dette utgjør en egen sårbarhet.

Digitale verktøy understøtter kriminell virksomhet på en rekke områder. Mange verktøy er lovlige, gratis eller rimelige, og lett tilgjengelige for alle som ønsker å bruke dem. Den akselererende digitale utviklingen øker tilgjengeligheten på brukervennlige og avanserte verktøy. Utviklingen bidrar til at flere settes i stand til å utføre cyberkriminalitet. Spesialtilpassede verktøy produseres også av gjerningspersonene selv.

Cyberkriminaliteten er tverrsektoriell. Det er usikkerhet knyttet til cyberkriminelles kapabiliteter og handlingsrom. Det er også usikkerheter knyttet til cyberkriminalitetens omfang og utvikling. Usikkerheten forsterkes av faktorer som effektive og bredt tilgjengelige anonymiseringstjenester, og et grenseløst, dynamisk og flyktig kriminalitetsfelt. I tillegg besitter politiet et begrenset tallmateriale, blant annet på grunn av mangelfull rapportering og få anmeldelser.

Kripos har over tid sett at det særlig er enkelte drivere som påvirker og understøtter cyberkriminalitet i Norge.

Sterke drivkrefter er den teknologiske utviklingen i seg selv, kombinert med at nye teknologiske sårbarheter hele tiden skapes, men sjelden forsvinner helt. Økt tilgjengelighet på avanserte digitale verktøy og kommersialiseringen av ulovlige tjenester gjør det enklere å begå cyberkriminalitet. Anonymiseringsteknologier, lav oppdagelsesrisiko, pengestrømmer gjennom virtuelle verdier som kryptovaluta, samt generelt dårlig data-

sikkerhet[6] gjør det lite risikofylt å være kriminell i det digitale rom. Tilgjengeligheten av datasett som eksponerer sårbarheter, og sensitiv personinformasjon på avveie enten på grunn av lekkasjer eller datatyveri, bidrar til et stort cyberkriminelt handlingsrom.

Cyberkriminalitet begås med bakgrunn i mange forhold: Ønske om vinning, seksuelle behov, gruppepress, behov for status, tilhørighet og anerkjennelse, ønske om å latterliggjøre, sjokkere og ha tilgang på ekstremt materiale, mestringsfølelse, politisk ideologi, spionasje og hevn.

Kripos observerer at flere aktører går igjen i ulike sammenhenger og konstellasjoner. Det eksisterer underliggende dynamikker i aktørgalleriet, som fører til at kriminelle samarbeider på tvers og sporadisk bytter gruppetilhørighet. Anerkjente aktører etterspørres eksempelvis gjerne av flere for spesifikke oppgaver, som skadevareutvikling.

Vi har alle en digital sårbarhetsflate. Privatpersoner kan utsettes for kriminalitet direkte, eller rammes indirekte når private bedrifter og offentlige virksomheter som forvalter informasjon om oss og tilbyr tjenester vi benytter, rammes av cyberkriminalitet. Likeså kan bedrifter og offentlige virksomheter utsettes for kriminalitet direkte, eller rammes indirekte gjennom sårbarheter i digitale forsyningskjeder eller tjenestenektangrep rettet mot andre, på delt digital infrastruktur.

Tverrgående drivere

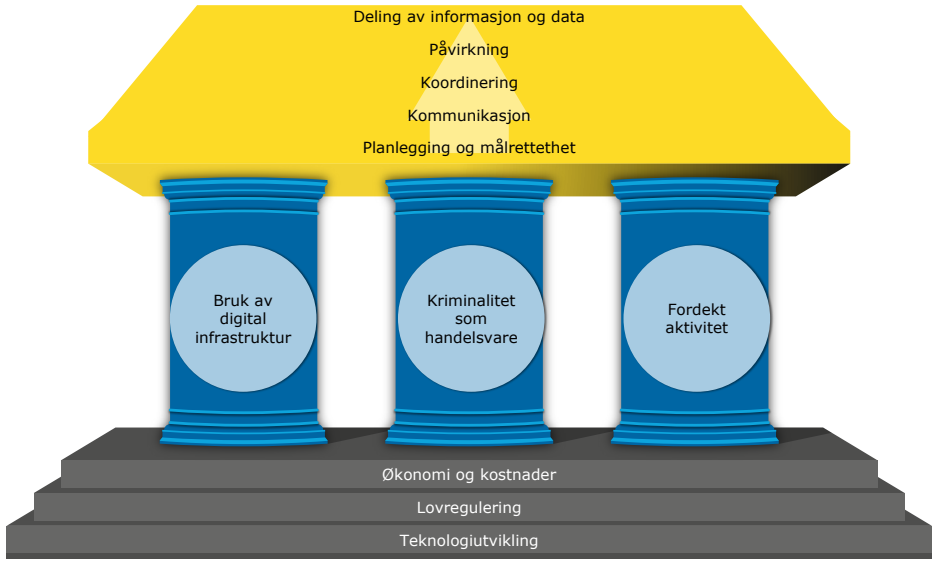
I det videre presenteres elleve drivere som er sentrale for organisert og annen alvorlig cyberkriminalitet. Det er Kripos sin vurdering at disse driverne vil påvirke utviklingen av cyberkriminaliteten i årene framover, både på operasjonelt, strategisk og taktisk nivå.

Driverne har varierende grad av relevans for ulike kriminalitetstyper, men utgjør til sammen et konseptuelt rammeverk for å forstå cyberkriminalitetens kompleksitet.

Planlegging og målrettethet

Menneskers kapabilitet til å behandle store informasjonsmengder har økt i takt med den digitale utviklingen. Cyberkrimi-

[6] Dette gjelder særlig IoT (Eng: Internet of Things; No: tingenes internett) som innebærer produksjon av et høyt antall enheter på billigste måte, hvor sikkerhetsaspektet ofte ikke ivaretas godt nok.



Elleve drivere for cyberkriminalitet

nalitet fordrer planlegging, informasjonsinnhenting og rekognosering. Avhengig av kriminalitetstypen kan fasene være relativt enkle og umiddelbare, eller forseggjorte, komplekse og tidkrevende. Store mengder informasjon er lett tilgjengelig på nett, uavhengig av hvor du befinner deg fysisk. Den enkle tilgangen på informasjon gjør planleggingsfasen til mange kriminelle enklere enn før, og mer tilpasset formålet. Følgelig øker også sannsynligheten for å lykkes med cyberkriminalitet.

Særlig blir kartleggingsdelen av planleggingsfasen enklere med digitale verktøy. Både privatpersoner og offentlige og private virksomheter tilgjengeliggjør mye informasjon som kan brukes for å avdekke eller skape sårbarheter. I tillegg er sensitiv informasjon fra tidligere datalekkasjer forholdsvis enkelt tilgjengelig på både det åpne og det mørke nettet. Selv om slik informasjon kan foreldes, kumuleres den totale mengden personsensitiv og annen skjermingsverdig informasjon på avveie. Vi legger over tid en voksende sum av opplysninger om oss selv på internett, som cyberkriminelle kan krysskoble med en voksende databank av stjålet eller lekket informasjon.

Samtidig som digitalisering og økt informasjonstilfang gjør privatpersoner og offentlige og private virksomheter mer sårbare enn før, får cyberkriminelle økt rekkevidde og en utvidet verktøykasse, og dermed flere muligheter. Planleggingsfasen er blitt viktigere, spesielt når det gjelder kompleks kriminalitet som involverer flere personer, og kriminalitet der egensikkerhet og anonymisering er sentralt.

Planleggingsfasen henger sammen med grad av målrettethet i kriminaliteten. I målrettet cyberkriminalitet har gjerningspersonene satt seg et mål i form av en bestemt verdi hos en bestemt person eller virksomhet. Et eksempel fra den analoge verden vil være å bryte seg inn i et museum for å stjele et maleri med høy verdi.

Opportunistisk cyberkriminalitet kjennetegnes av at gjerningspersonene skyter bredt i håp om å finne mål blant mange potensielle fornærmede, for eksempel gjennom masseutsendelse av e-post eller automatisert leting etter sårbarheter i mange datasystemer. Det finnes egne gratis søkeverktøy for sårbarheter hos internettilknyttede digitale enheter. Terskelen for slik opportunisme er derfor lav.

Hvis gjerningspersonene oppnår aksess, vil de forsøke å hente ut det maksimale utbyttet av denne tilgangen. Det kan være i form av å benytte aksessen til videre kriminalitet, for eksempel løsepengevirus eller datatyveri. Det kan også være å videreselge tilgangen til et system. Et eksempel fra den analoge verdenen vil være at en gjerningsperson kjenner på dører helt til hen finner en som er ulåst, for så å gå inn og ta alt av verdi.

Hvem som helst kan bli offer for opportunistisk cyberkriminalitet, og sjansen er større dersom man har «ulåste dører». Det er rimelig å forvente at det til enhver tid vil være kriminelle som leter etter digitale sårbarheter i stor skala. Grunnleggende og utbredte sikkerhetssystemer hindrer i de fleste tilfeller at opportunistiske gjerningspersoner lykkes, mens utdatert programvare og nye sårbarheter øker risikoen for å bli rammet av slik cyberkriminalitet.

Målrettet cyberkriminalitet vil i større grad treffe fornærmede som sitter på store verdier. Hva som har en stor verdi, vil være avhengig av fornærmedes situasjon og gjerningspersonens intensjon. For seksuallovbrytere kan fornærmedes kjønn og alder ha en stor verdi. Kritisk forretningsinformasjon kan være verdifull for vinningskriminelle. Kriminalitet hvor denne informasjonen blir kryptert eller kommer på avveie, vil gjøre fornærmede sårbar for utpressingsforsøk. Gjerningspersonens intensjon kan også virke inn på verdien av informasjonen, for eksempel ved at

gjerningspersonen kjenner til hvordan informasjonen kan misbrukes eller selges til andre.

Cyberkriminalitet kan være både opportunistisk og målrettet. Gjerningspersoner kan eksempelvis utføre bred og automatisert opportunistisk skanning, og gjennom det avdekke femti sårbare virksomheter. Disse virksomhetene utgjør utvalget som de kan gå videre med i utnyttelsen av sårbarhetene, i form av datatyveri eller kryptering og påfølgende utpressing. Blant de femti virksomhetene kan det være noen som skiller seg ut, eksempelvis fordi de har stor omsetning eller er avhengige av tidskritiske prosesser. En kryptering av deres filer vil medføre produksjonsstans og betydelige økonomiske tap. Gjerningspersonene kan derfor anta at effekten av et løsepengevirusangrep mot disse vil være større enn mot andre, med en tilsvarende større mulighet for økonomisk vinning. Kripos kjenner til kommunikasjon mellom organiserte cyberkriminelle hvor det diskuteres hvilke bransjer og regioner som er mer betalingsvillige enn andre.

Det private næringsliv og offentlige bedrifter beskriver at normalbildet for dem i stor grad kjennetegnes av opportunisme, hvor cyberkriminelle kaster ut vide nett og forsøker å oppnå uberettiget tilgang til mange datasystemer. Forsøkene virker i hovedsak å være automatiserte tester av internetteksponert infrastruktur for å finne svakheter. Cyberkriminelle utnytter både gamle teknologiske sårbarheter som ikke er utbedret og nye sårbarheter etter hvert som de oppstår eller blir kjent. Noe av kriminaliteten er mer avansert og bærer preg av målrettethet. På grunn av den store mengden automatiserte forsøk på å utnytte sårbarheter kan hovedvekten av kriminalitet mot datasystemer i Norge kalles opportunistisk, samtidig som flere av de alvorligste lovbruddene er rettet spesifikt mot store verdier.

Kommunikasjon

Organisert cyberkriminalitet forutsetter samhandling mellom mennesker. Slik samhandling er avhengig av kommunikasjon. Digital kommunikasjon gir cyberkriminelle nye muligheter og utfordrer politiets kriminalitetsbekjempelse. Den er blant annet vanskelig både å spore, identifisere og lese innholdet av.

I Norge har nesten alle privatpersoner og virksomheter kontaktinformasjonen sin åpent tilgjengelig. Det har derfor blitt enklere å identifisere og komme i kontakt med ofre, for eksempel for å forlede, trakassere eller formidle intensjoner, trusler eller krav. Gjerningspersoner kan enklere skjule sin identitet, eller utgi seg for å være noen en fornærmet har grunn til å

Digital kommunikasjon gir cyberkriminelle nye muligheter og utfordrer politiets kriminalitetsbekjempelse. Den er blant annet vanskelig både å spore, identifisere og lese innholdet av.

stole på. De kommuniserer via kanaler de fornærmede er vant til å kommunisere med sine venner og familie på, da det kan inngi økt grad av tillit.

En vanlig handlemåte innen seksuallovbrudd for å etablere kontakt med mindreårige er å benytte etablerte og mye brukte kommunikasjonsplattformer[7], for deretter å flytte samtalen over på en mer egnet ende-til-ende-kryptert meldingstjeneste[8] eller kommunikasjonskanal.

For andre seksualforbrytere kan kontakt med fornærmede etableres på lovlige nettpresentasjonstjenester som selger direkteoverført seksuelt innhold med voksne.

I noen tilfeller oppretter de cyberkriminelle sine egne kommunikasjonsplattformer for å kommunisere sikkert med fornærmede. Da vil de selv ha full kontroll over all aktivitet.

I sitt arbeid mot seksuelle overgrep har Kripos observert en kommersialisering av kommunikasjon.[9] For å vinne et offers tillit gjennom sosial manipulasjon finnes det produsenter som selger forhåndsinnspilte videosekvenser der personen i videoen gjennomfører forskjellige seksuelle handlinger på seg selv. Videosekvensene kan spilles av med enkle kommandoer på tastaturet for å gi inntrykk av at det er en direkteoverført videosamtale. Enkelte produsenter selger også stillbilder som kan oversendes til offeret hvis behovet skulle oppstå. Ved å bruke slike produkter kan den kriminelle villede offeret uten å tilkjennegi egen identitet. Den kriminelle vil forsøke å få offeret til å gjøre tilsvarende eller lignende handlinger på seg selv. Opptak av offeret kan benyttes til utpressing, materialet kan deles vederlagsfritt for økt status, eller selges for profitt, som beskrevet over.

Når kontakt er etablert kan det være både tid- og ressurskrevende for den kriminelle å opprettholde nødvendig kontakt med fornærmede. Blant annet kan betydelige ressurser måtte brukes på administrering, som for eksempel av e-postkontoer. Ofte er hurtig respons på henvendelser fra offeret en avgjørende suksessfaktor for den kriminelle handlingen.

Koordinering

Koordinering kan foregå på meldingstjenester med ende-til-ende-kryptering,

---

7 Eksempelvis Instagram; Omegle; Snapchat.

8 Eksempelvis Signal; Telegram; WhatsApp; Wickr.

9 Eng: Virtual Cam Whoring, eWhoring.

kriminelles egne kommunikasjonstjenere[10], internettfora og nettsider på både det åpne og det mørke nettet.

Kripos ser at den økte evnen til koordinering gjør at kriminelle lettere kan organisere seg. Det digitale roms grenseløse natur gir aktørene mulighet til å være på forskjellige steder, verden over. Dette gir i seg selv cyberkriminelle et effektivitetsfortrinn, sammenlignet med andre organiserte kriminelle.

Når cyberkriminelle samarbeider fordeles ofte ansvar og arbeidsoppgaver mellom spesialister. Samarbeidet består gjerne av en liten kjernegruppe og en større ytre krets av løsere tilknyttede kriminelle.

Utenfor den ytre kretsen finnes lovlige og ulovlige tjenester som gjerningspersonene benytter seg av, for eksempel utleiere av infrastruktur[11] eller programvare. Tjenestetilbyderne kjenner ikke nødvendigvis til lovbruddene bak aktiviteten. Slik infrastruktur kan også være spesielt rettet mot kriminell bruk. Programvare og tjenester som tilbys kan være skreddersydde for å unngå deteksjon, sporing og nedstengning.[12]

Det er vanlig at utbyttet deles mellom de forskjellige gjerningspersonene. Utbyttet etter løsepengevirusangrep fordeles ofte prosentvis til de som har hatt ulike funksjoner i angrepet, eksempelvis den som skaffet tilgangen, utvikleren av skadevaren og den som leide skadevaren.

Fordekt aktivitet og anonymiseringsteknologier

En avgjørende faktor for mye cyberkriminalitet er muligheten til å kunne operere fordekt. Anonymiseringsteknologier gjør dette mulig. Utviklingen drives av legitime personvernbehov og ønsket om frihet i det digitale rom. Dette kommer også cyberkriminelle direkte til gode. Anonymiseringsteknologiene lar en gjerningsperson operere på tvers av landegrenser og jurisdiksjoner med ulik lovregulering.

Cyberkriminelle ønsker ikke at kriminaliteten skal knyttes til deres virkelige identitet, siden det øker risikoen for straffeforfølgelse. Samtidig har flere nytte av anerkjennelse blant andre kriminelle, slik at de fremstår som relevante samarbeidspartnere. Gjerningspersone-

[10] En tjener kalles også en server, fra engelsk.

[11] Eng: Hosting

[12] Eksempelvis BPH: Eng: Bulletproof Hosting; No: Sikker utleie

ne og deres infrastruktur må heller ikke kunne la seg spore, da det øker risikoen for at de blir stanset, forstyrret eller at politiet tar beslag i utstyr som benyttes til kriminaliteten. En enkel metode for å oppnå en viss grad av anonymitet er å benytte flere alias i ulike sammenhenger.

Cyberkriminelle bruker, som veldig mange andre, VPN-tjenester[13] som gir tilgang til mellomtjenere[14] og ulike grader av kryptering av trafikk. Flere tilbyr ende-til-ende-kryptering for all trafikk mellom brukerens datamaskin og målene de kobler seg til via tjenestens mellomtjenere. De fleste VPN-tjenester gir brukeren mulighet til å velge mellomtjenere i mange ulike land. For nettsidene og tjenestene brukeren kobler til vil brukerens utgangsadresse framstå som VPN-tjenestens mellomtjener. Brukeren oppnår slik en viss anonymitet, i tillegg til at trafikken skjules bak kryptering. Det er også vanlig å benytte VPN-tjenester på mobiltelefoner og nettbrett. Mange VPN-tilbydere reklamerer med lite eller ingen loggføring av kunders informasjon og bruk.

Cyberkriminelle bruker også mellomtjenere utenom VPN-tjenester for å anonymisere og skjule sin aktivitet. Mellomtjenere kan eies eller leies gjennom egne tjenester eller et datasenter.[15]

Tilgjengelige anonymiseringsteknologier vanskeliggjør i høy grad forebygging, avverging, etterforskning og straffeforfølgelse av cyberkriminelle. Teknologisk kompetente gjerningspersoner gjør etterforskningen av lovbrudd utfordrende.

Deling av informasjon og data

Cyberkriminelle benytter både det åpne og det mørke nettet til deling og formidling. Fora for deling av informasjon og data kan grovt deles inn i ulovlige markedsplasser med hovedvekt på narkotikahandel, salg og deling av overgrepsmateriale, diskusjon og handel av skadevare og tjenester myntet på kriminalitet mot datasystemer. Deltagelse på

---

13 VPN: Eng: Virtual Private Network; No: Virtuelt privat nettverk

14 Eng: Proxy Server

15 I utgangspunktet oppnår man samme type og bedre sikkerhet (ende-til-ende-kryptering) gjennom en VPN-tjeneste enn ved bruk av en mellomtjener. Det kan likevel være grunner til at man velger en mellomtjener fremfor en VPN-tjeneste. Det kan være billigere, og en privat mellomtjener kan skreddersys til det formålet den skal brukes til.

slike fora kan gi økt kriminell kunnskap og en følelse av tilhørighet. Det kan bryte ned barrierer og normalisere eller bagatellisere ulike former for cyberkriminalitet. Slike fora kan tjene samme funksjon som andre former for ekkokamre, og for eksempel oppmuntre seksualforbrytere som ikke har forgrepet seg fysisk på noen tidligere, til å begynne.

For TOR-nettverket vurderer Kripos at det er en rekke forutsetninger som må være på plass for at et forum skal bli hovedarena for salg og deling av overgrepsmateriale. Teknologisk kompetanse, økonomisk handlekraft, fungerende ledelse og moderasjon, samt tilstedeværelse av produsenter av unikt materiale er alle viktige elementer.

En mye brukt metode for deling av ulovlige data på det åpne nettet er fillagringstjenester der en lenke til en nettadresse gir tilgang til direkte hurtig nedlasting av store filer. Vanlige egensikkerhetstiltak tas ved å dele lenkene på det mørke nettet og bruke VPN ved nedlasting av data på det åpne nettet.

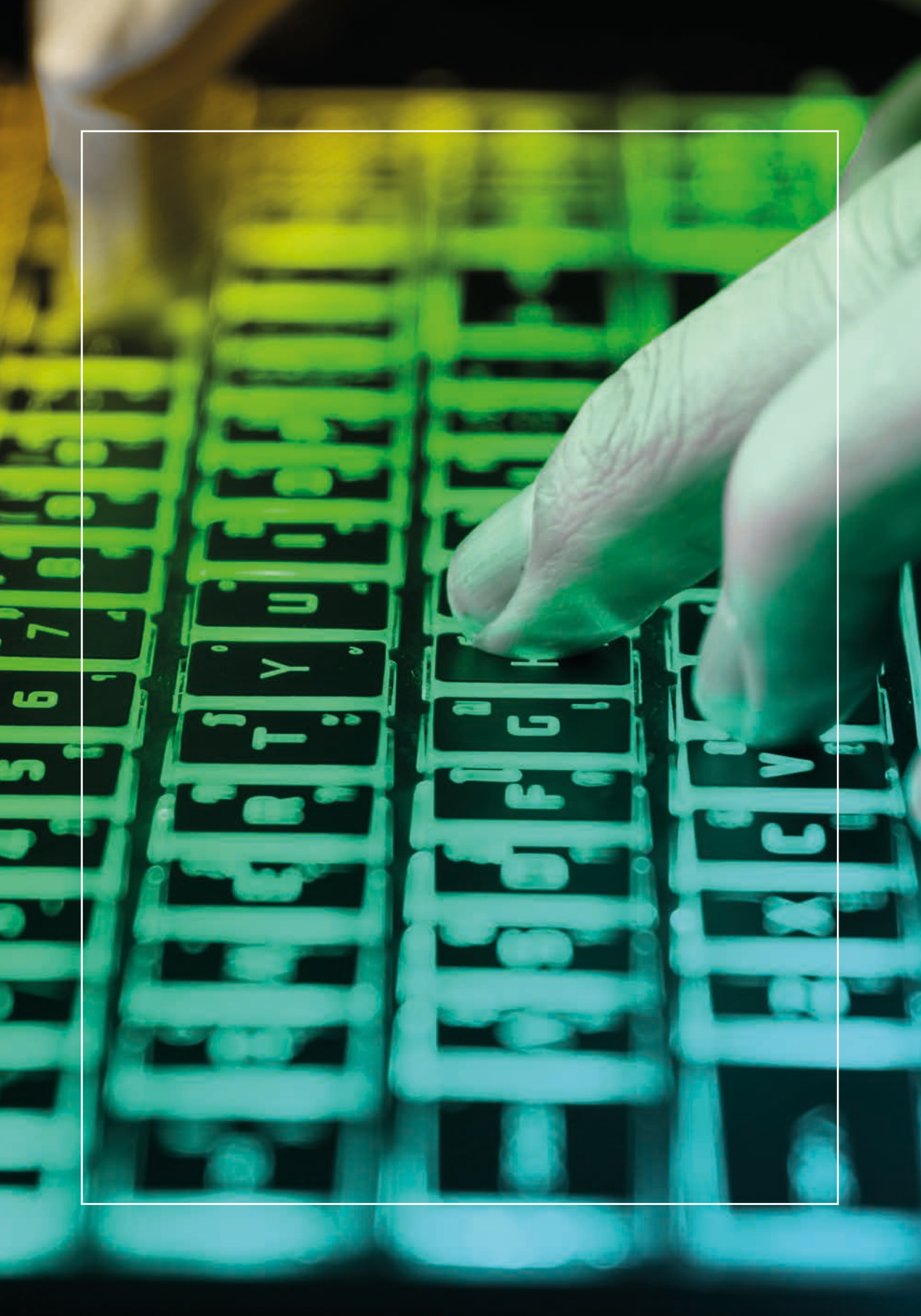
Informasjonsdeling skjer også i likemannsnettverk. Dette er nettverk som knytter brukerne direkte sammen uten bruk av en tjener i sentrum. Normalt vil et spesialtilpasset likemannsnettverk gi høy datadelingshastighet. Kripos ser at likemannsnettverk med enkle brukergrensesnitt foretrekkes av kriminelle. Slike nettverk kan gi lavere nettverkshastigheter, og den kriminelle må derfor gjøre en avveining mellom brukervennlighet og overføringshastighet når hen velger likemannsnettverk.

Økonomi og kostnader

Digital økonomi utfordrer tradisjonelle økonomiske systemer. Med digitale verktøy kan kriminelle enkelt beskytte og bruke sine likvider. Brukervennlige, hurtige, lett tilgjengelige og trygge digitale løsninger sikrer økonomisk samhandling. Ved å akseptere høyere risiko for tap og med spesiell kompetanse kan den kriminelle økonomien også skjules for myndighetene.

Virtuelle verdier som kryptovaluta gir mulighet til å motta, flytte og anvende likvider samtidig som brukeren forblir anonym. Ettersom kryptovalutamarkedet opererer utenfor det tradisjonelle finansielle systemet, vanskeliggjør dette offentlige myndigheters kartlegging og etterforskning. Kjøp og salg av ulovlige varer som narkotika, samt utpressing med løsepengevirus ville vært vanskelig å gjennomføre med samme grad av anonymitet uten kryptovaluta. Kryptovaluta er sentralt i hvitvasking av utbytte fra cyberkriminalitet.

Cyberkriminelle benytter ulike digitale



økonomiske tjenester som bidrar til anonymisering, og tar raskt i bruk nye muligheter innen hvitvasking. Utvalget av kryptovalutaer[16] og tilhørende vekslingstjenester[17] er stort. Bruk av vekslingstjenester bidrar til å anonymisere gjerningspersoner og hvitvaske kriminelt utbytte. Egne tjenester for miksing av valuta brukes for å blande ulike strømmer med kryptovaluta og å øke anonymiteten ytterligere, og gjøre transaksjoner med kryptovaluta vanskeligere å spore.[18] Kripos registrerer at flere av de samme tilbyderne og valutapreferansene går igjen. Digitale gavekort benyttes også.

Direkte økonomiske kostnader fra cyberkriminalitet kan for en virksomhet være nedetid på systemer, og tap av evne til å levere produkter og tjenester. Kriminaliteten kan ramme en virksomhet direkte, og i tillegg ha en forsinket effekt ved at økonomiske konsekvenser manifesterer seg på et senere tidspunkt eller over tid.

Tap av rykte og tillit til virksomheten, markedsverdi og konkurranseevne er eksempler på indirekte økonomiske konsekvenser. Det å beskytte seg mot cyberkriminalitet gjennom forebygging og sikkerhetsarbeid koster også virksomheter mye penger.

Kripos kjenner ikke til at det i Norge er foretatt noen helhetlig samfunnsøkonomisk analyse av kostnadene ved cyberkriminalitet.

Påvirkning

Gjerningspersoner har behov for å påvirke mennesker, utstyr eller tjenester på ulike måter i mange typer cyberkriminalitet. Avhengigheten av digitale produkter og tjenester gjør samfunnet sårbart for slik manipulasjon.

Menneskelige sårbarheter inkluderer at vi kan bedras, villedes, krenkes og trues. Lavt kunnskapsnivå, godtroenhet, høy tillit til medmennesker og institusjoner, begjær, frykt for omdømmetap og håp om profitt gjør oss sårbare. Mennesker begår også brukerfeil, og kan være en innsidetrussel. Alt dette bidrar til handlingsrom for påvirkning. Teknologien er en ny dør inn til disse sårbarhetene.

Virksomheter og personer kan studeres av cyberkriminelle for å forstå aktivitet, adferd og relasjoner som kan avdekke

[16] Bitcoin, Monero, Ethereum m.fl.
[17] Coinbase; Wirex m.fl.
[18] Såkalte tumblere og miksere.

muligheter for manipulering. Hvis ønsket er urettmessig tilgang til en virksomhets nettverk, kan gjerningspersonen igangsette masseutsendelse av e-post med skadelig nyttelast til ansatte. En slik fremgangsmåte kalles phishing.

Ved å studere en virksomhet kan kriminelle aktører identifisere nøkkelpersoner som sikkerhetssjefer, resepsjonister eller mellomledere, eller personer nær dem, som kan brukes til å oppnå aksess indirekte. Disse personenes sårbarheter søkes så brukt for å få tilgang til sensitiv informasjon. Nøkkelpersonene kan bli utsatt for målrettet phishing.[19] Aktiviteten kan foregå over tid for å bygge tillit. Antall phishing- og målrettede phishingforsøk har økt i 2022.

Masseutsendelse av SMS med lenker til nettsteder med skadevare, såkalt smishing, fungerer på samme måte som masseutsendelse av e-post. Tilsvarende framgangsmåte via telefon kalles vishing.

Metoder som phishing og smishing avhenger av at gjerningspersonene framstår som legitime aktører, for eksempel ved at man får kommunikasjonen til å se ut som den kommer fra et norsk nummer eller et kjent nettsted fornærmede allerede stoler på. Dette kalles spoofing. Spoofing omfatter også å utgi seg for å være en annen på telefon eller video i forbindelse med svindel og bedragerier.

Når kontakten og den nødvendige tilliten er etablert i forholdet, kan den sosiale manipulasjonen fortsette. Målsetningen kan være at fornærmede oppgir sensitiv informasjon som gir gjerningspersonen tilgang til en persons nettbank eller en virksomhets datasystem, eller at offeret installerer skadevare i systemet, med eller uten viten om det.

Grupper som barn og eldre er mer sårbare for ulike typer påvirkning. Eldrebedragerier starter ofte med phishing, smishing eller telefonoppringninger. Seksualforbrytere kan skape tillit hos barn ved å utgi seg for å være jevnaldrende. Sårbare personer kan selv søke seg til fora hvor de risikerer å bli radikalisert eller utnyttet.

Politiet har begrenset kunnskap om rekruttering av norske borgere til organisert kriminalitet mot datasystemer. Fra utlandet er det kjent at unge mennesker kan tiltrekkes gjennom teknologisk mestringsfølelse og anerkjennelse i sosiale miljøer på internett. Noen begynner med modifisering av og juks i dataspill, og går

[19] Eng: Spearphishing

derfra til fora for datakriminalitet uten å vurdere konsekvensene.

Kriminelles bruk av digital infrastruktur

Cyberkriminelle bruker digital infrastruktur til en rekke formål, som administrasjon, lagring, deling, gjennomføring av datainnbrudd, kommunikasjon og kommando og kontroll (K2[20]). Kriminelle benytter gjerne flere K2-enheter for å minimere oppdagelsesrisiko og sikre at infrastrukturen forblir operasjonell selv om deler av den skulle avsløres. Avanserte cyberkriminelle kan også skifte ut K2-infrastrukturen sin hyppig for å minske oppdagelsesrisikoen.

Kriminelle kan bruke egne datamaskiner til å opprette den digitale infrastrukturen de trenger. De kan også bryte seg inn i andres systemer og benytte dem som sin infrastruktur i neste omgang. Det er også mulig å leie datamaskiner og nettverkstjenester lovlig, for så å benytte dem til ulovlig aktivitet. Slike tjenester med fysisk infrastruktur i Norge benyttes til ondsinnet aktivitet av flere ulike aktører.

Noen tilbydere leier ut tjenere de selv har leid av andre tjenestetilbydere. Slik framleie kan foregå i flere ledd, hvor de ulike tilbyderne har sine kontorer i ulike land med forskjellige lover og regler.

En gjerningsperson er derfor ikke avhengig av å benytte ulovlige tjenester for å kunne utføre ulovlig aktivitet fra norske IP-adresser, med lav risiko for straffeforfølgelse. Gjerningspersonen kan oppnå en tilsvarende grad av anonymitet og vern mot tvangsmidler ved å benytte leid infrastruktur.

Framleie av legitim infrastruktur og vertstjenester plassert i Norge til leverandører i utlandet gjør det utfordrende å lokalisere datautstyr som ønskes underlagt tvangsmidler i Norge.

Framleiepraksisen, sammen med de utenlandske tjenestetilbyderne, medfører at sluttbrukere av norske IP-adresser i praksis er anonyme og beskyttet mot rettslige tvangsmidler, samtidig som det gjør det vanskelig for norske myndigheter å stoppe ondsinnet aktivitet når den oppdages.

Markedets globale natur og de medfølgende ulikhetene i lovregulering gjør det enkelt og formålstjenlig for kriminelle å benytte seg av leid infrastruktur. Det skjer også at utleietilbydere ikke svarer på henvendelser fra myndigheter. Denne markedsmekanismen er med på å øke dynamikken og flyktigheten i cyberkri-

[20] No: K2: Kommando og kontroll; Eng: C2: Command and Control

minalitet. I tillegg blir det enklere å skjule sporene etter aktiviteten.

Kripos observerer at infrastruktur som har blitt benyttet i kriminalitet mot norske verdier befinner seg i USA og land over hele Europa, eksempelvis Nederland og Litauen. Samme infrastruktur har blitt benyttet i tilsvarende kriminalitet i mange andre land.

En handlemåte for å få tilstrekkelig datakraft til å gjennomføre tjenestenektangrep eller masseutsendelse av e-post er å benytte et nettverk av kompromitterte enheter, et såkalt botnett[21]. Kontroll over slike enheter kan den kriminelle selv skaffe seg, eller leie på det mørke nettet.

Kriminalitet som handelsvare

En del av den kriminelle aktiviteten i det digitale rom krever spesiell kompetanse. Dette har skapt et eget marked, der digitale verktøy, kompetanse og ressurser leies ut og selges til kriminelle formål. Slik kommersialisering av kriminalitet omtales som kriminalitet som handelsvare eller tjeneste.[22] Dette markedet gjør mindre avanserte aktører i stand til å gjennomføre kriminelle handlinger de ellers ikke hadde vært i stand til å gjennomføre.

Kontraantivirustjenester[23] er et eksempel. Slike tjenester tilbyr en test av skadevare for å se hvilke kommersielle og gratis tilgjengelige beskyttelsestiltak som vil avsløre skadevaren. Slik får skadevareutviklere hjelp til å unngå at skadevaren oppdages av mottiltak formulert av cybersikkerhetsbransjen.

Kripos har sett at mengden av slike handelsvarer er økende.

Løsepengevirus er en annen handelsvare i dette markedet.[24] Skadevareutviklere og kriminelle som begår datainnbrudd jobber sammen med profesjonelle forhandlere i utpressingen og hvitvaskere i et digitalt kriminelt økosystem. Deler av utbyttet fra utpressingen reinvesteres i økosystemet ved å støtte utvikling av ny skadevare, opparbeidelse av urettmessig tilgang til nye datasystemer, og nye utpressinger. Det ligger insentiver innebygd i modellen som driver etterspørselen etter skadevare og relaterte

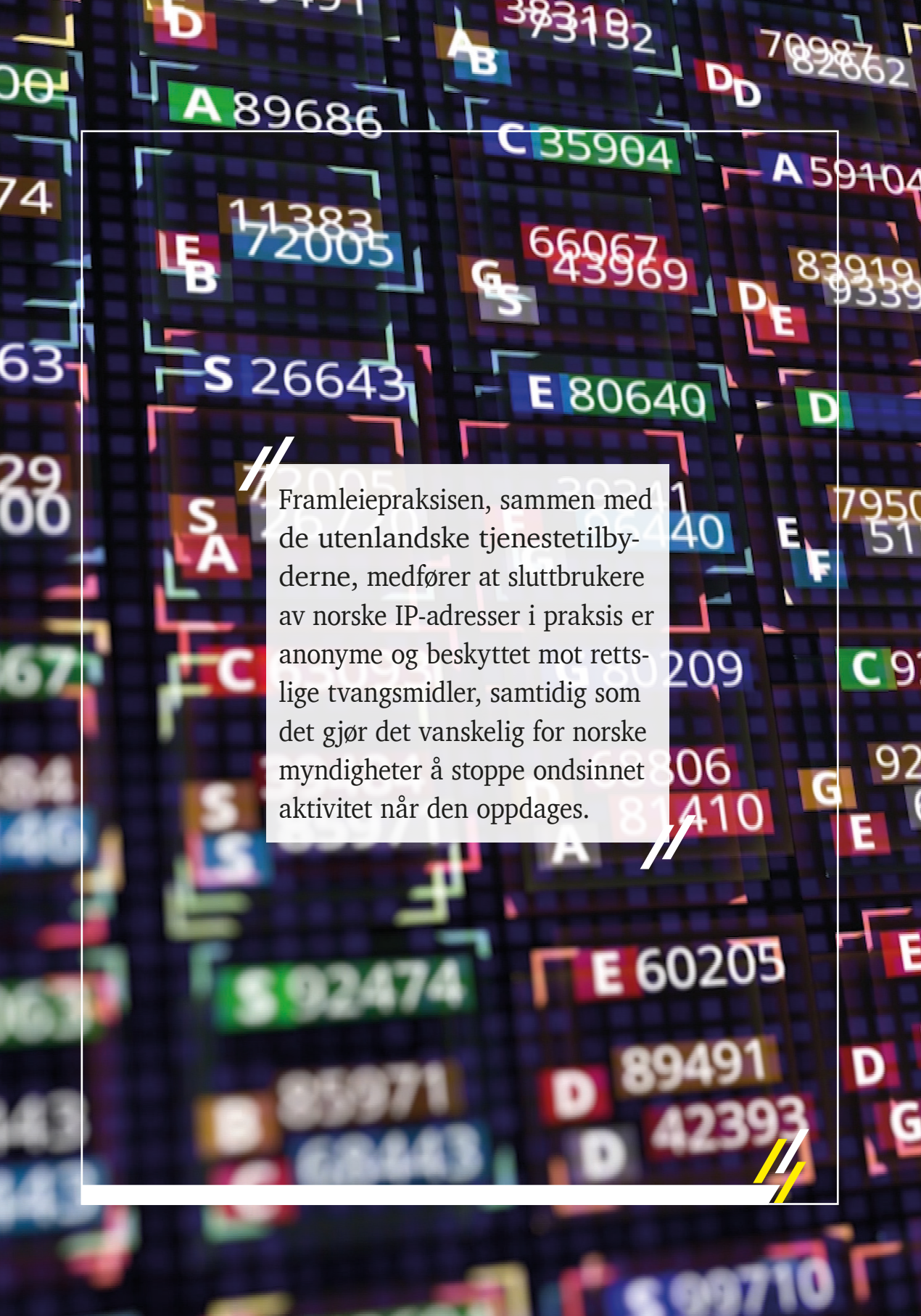
---

[21] Et botnett er et nettverk av allerede kompromitterte datamaskiner og andre enheter, som utgjør en desentralisert ressurs.

[22] CaaS: Eng: Crime as a Service

[23] Kjent som CAV: Eng: Counter Antivirus Service

[24] RaaS: Eng: Ransomware as a Service



Framleiepraksisen, sammen med de utenlandske tjenestetilbyderne, medfører at sluttbrukere av norske IP-adresser i praksis er anonyme og beskyttet mot rettslige tvangsmidler, samtidig som det gjør det vanskelig for norske myndigheter å stoppe ondsinnet aktivitet når den oppdages.

kriminelle tjenester. At løsepengevirus selges som en tjeneste gjør i tillegg kriminalitetsformen tilgjengelig for flere, også de som mangler ulike typer teknologisk kompetanse til å utføre kriminaliteten på egen hånd.

Strukturen Kripos har observert blant kriminelle som samarbeider om løsepengevirus kan beskrives som en pyramide. På toppen av pyramiden sitter de som gjennomfører selve datainnbruddet. Disse gjerningspersonene oppnår urettmessige tilganger til datasystemer, kartlegger og stjeler data og krypterer filer. På nivået under finnes tilretteleggere som utvikler skadevare, selger stjålne påloggingsdetaljer og tilbyr ulike andre tjenester. Nivået under tilretteleggerne er de som hvitvasker utbyttet.

En slik struktur kan eksempelvis bestå av ti kjernemedlemmer, med ulike ferdigheter innen og ansvar for skadevareutvikling, forhandling og hvitvasking. Kjernegruppen kan igjen ha hundre tilknyttede personer som leier løsepengeviruset mot at de betaler en profittandel. Kjernegruppen kan også bistå dem med forhandlinger. De ulike nivåene mottar penger fra vellykkede utpressinger.

Kriminelle som har brukt løsepengevirus mot virksomheter i Norge har i enkelte saker operert innenfor slike økosystemer. Politiet har kunnskap om slike grupperinger med tilhold i Ukraina og Russland. Det er usikkerhet rundt hvordan Russlands krig mot Ukraina har påvirket organisert cyberkriminalitet med base i Øst-Europa. Flere kjente kriminelle nettverk, som i utstrakt grad har benyttet løsepengevirus over tid, har blitt oppløst som følge av interne uenigheter i nettverket. Uenighetene har oppstått fordi medlemmene har valgt forskjellige sider i den pågående krigen. Det er uavklart hvorvidt oppløsningen av grupperingene er av permanent karakter eller kun midlertidig, i påvente av en fremtidig reetablering.

Teknologiutvikling

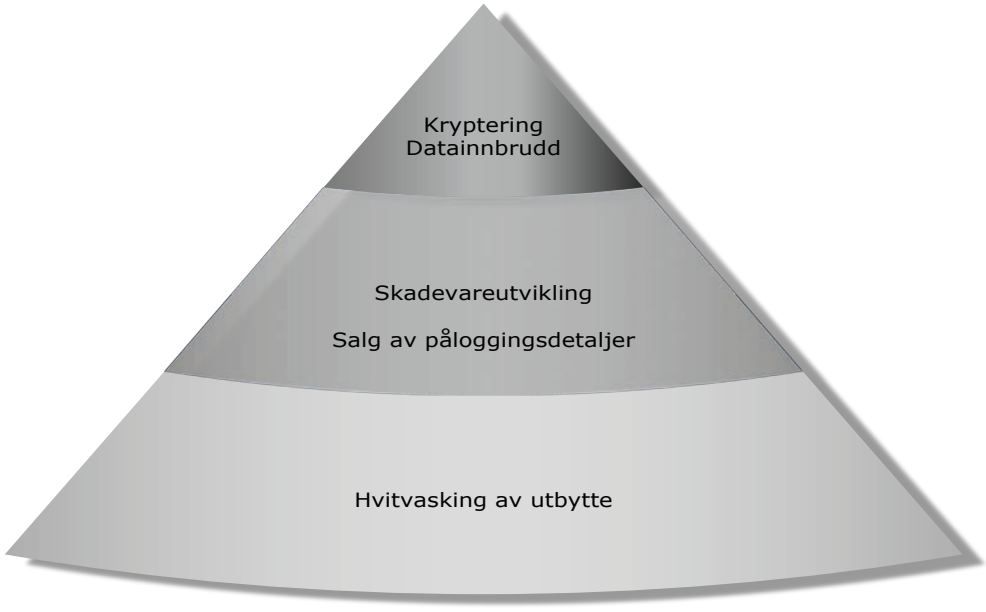
Teknologiutviklingen for både program- og maskinvare går hurtig fremover. Utviklingen drives av ressurser på statlig, akademisk, kommersielt og frivillig nivå, og vil både fremme og hemme cyberkriminalitet. Det finnes mange eksempler på dette. Ett eksempel er at økningen i dataoverføringshastighet har kommet samfunnet til nytte, samtidig som den har gjort kriminalitet enklere og mer effektiv.

De teknologiske sårbarhetene som følger i takt med utviklingen består av økte digitale sårbarhetsflater, leid infrastruktur, lange verdikjeder, uoversiktlige og sårbare leverandørkjeder og utilstrekkelig sikring.

En del av teknologiutviklingen vil være direkte rettet mot å øke sikkerheten i produkter og tjenester, og derigjennom redusere det cyberkriminelle handlingsrommet. Kriminelle aktører må derfor bruke ressurser på å omgå slike nyskapninger. Samtidig utføres det mye frivillig arbeid med åpen kildekode som også kommer cyberkriminelle til gode, ved at de kan benytte lovlige verktøy til ulovlig virksomhet.

Lovregulering

Lovverket utfordres av den teknologiske utviklingen, og henger som regel etter. Det rettslige grunnlaget for internasjonalt juridisk samarbeid har ikke blitt utarbeidet med dagens cyberkriminalitet som bakgrunn. Det kan ta lang tid å få informasjon fra utenlandske samarbeidspartnere, og i enkelte saker er det risiko for at sakene blir foreldet. Utfordringer i regulering, herunder framleie og bruk av mellomtjenere og VPN kan sies å utgjøre juridiske sårbarheter som kan utnyttes til cyberkriminalitet.



Eksempel på struktur blant organiserte cyberkriminelle

Ekomlovens[25] nye bestemmelser om ekomtilbyderes lagringsplikt og vilkår for deling med politiet trådte i kraft 1. januar 2022. De nye bestemmelsene pålegger ekomtilbydere å lagre identifiserende opplysninger om en abonnent i tolv måneder, kontra tidligere sletteplikt etter 21 dager. Politiet kan blant annet kreve å få informasjonen utlevert ved etterforskning av lovbrudd med en strafferamme over tre år.

Lovendringen gjør identifisering av brukere noe enklere, og medfører at flere cyberkriminelle vil kunne etterforskes av politiet.

Forholdet mellom kriminelle og statlige aktører

I det digitale rom grenser Norge direkte til alle andre land, inkludert land som Nord-Korea, Iran, Kina og Russland. Den samme verdien i en norsk virksomhet kan være ettertraktet både av vinningskriminelle og fremmede statsmakter.

Forholdet mellom en stat og cyberkriminelle aktører kan ta mange ulike former, alt fra statens effektive bekjempelse av aktørens cyberkriminalitet, til en så fullkommen integrering mellom de to at det er staten selv som begår kriminaliteten.

En statlig aktørs aktivitet vil innledningsvis ikke framstå ulikt andre lovbrudd. Videre undersøkelser vil være nødvendige for å avdekke om kriminaliteten faller inn under PSTs eller politiets mandat.

Det kan ta lang tid å finne ut av hvem som sto bak et datainnbrudd, uansett om undersøkelsene ender i attribusjon[26] eller strafferettslig tiltale.

Cyberkriminalitet med vinningsmotiv, som industrispionasje eller utpressing med løsepengevirus, kan ha varierende grad av knytning til statlige aktører.

Både cyberkriminelle og statlige aktører kan benytte verdikjedeangrep. Slike angrep kan treffe norske virksomheter, enten målrettet eller utilsiktet fordi de er kunder av de kompromitterte leverandørene. Data stjålet i en cyberkriminell kontekst kan i tillegg ha etterretningsverdi for statlige aktører.

---

[25] Lov om elektronisk kommunikasjon

[26] Basert på tekniske analyser og annen kunnskap tilskrives i noen tilfeller et datainnbrudd til en aktør. I cyberetterretning kalles dette attribusjon. Sikkerhetsselskaper og stater benytter ofte attribusjon i hendelser der det ikke foreligger en rettskraftig dom i en straffesak.


Data
User Admin 0001
[C4]
[C2]
[C3]
[B3]
[B2]
[B1]
[A1]

Kriminalitetsområder

Det er nødvendig å redegjøre spesielt for noen forhold ved ulike typer cyberkriminalitet, med de tverrgående driverne som bakgrunn.

Bedragerier og svindel

Bedrageri er manipulasjon av mennesker i vinnings øyemed.[27] Det har vært en økning i digitale bedragerier mot privatpersoner de to siste årene.

Digitalt bedrageri forekommer i mange varianter, men noen har vært særlig utbredt i Norge. Flest privatpersoner har blitt ofre for bedrageri i forbindelse med phishing, kjøp og salg på digitale markedsplasser eller ved netthandel. Normalt foregår slike bedragerier ved at kjøper ikke får varen de har betalt for. Eksempelvis er ikke selger å oppdrive i etterkant av kjøpet. Kripos har også sett tilfeller der virksomheter selger større kvanta av en handelsvare for så å slå seg konkurs, og pengene går tapt for kjøperne.

Kjærlighetsbedragerier og bedrageri mot eldre[28] forekommer også. Da benyttes sosial manipulasjon til å utvikle følelser og bygge tillit, som setter gjerningspersonen i stand til å få overført penger fra fornærmede. I bedragerier rettet mot eldre benytter gjerningspersonen også sosial manipulasjon, men her fremstiller hen seg som en autoritetsperson, oftest som en funksjonær i fornærmedes bank. Når tilliten er etablert, brukes denne til å få tilgang til den fornærmedes nettbank. Tilgangen brukes så til å overføre penger til gjerningspersonen.

Investeringsbedrageri er en annen variant. Her vil en fornærmet bli lurt til å investere penger i et prosjekt som ikke er reelt eller som ikke gir avkastning. Investeringer er forbundet med risiko, og det er ikke unormalt å tape de investerte midlene. Det kan dermed være utfordrende å avdekke slikt bedrageri. Det regnes imidlertid som bedrageri hvis det er tilsiktet at investeringen ikke ville gi avkastning.

Generelt har det vært en økning av bedragerier som involverer kryptovaluta.

---

27 Strl, §§ 371 flg.

28 Også omtalt som Olga-svindel.

Privatpersoner utsettes også for ID-tyveri med påfølgende bedrageri. Det kan kreve både tid og ressurser å håndtere og begrense skadene ID-tyveri fører med seg.

Virksomheter utsettes ofte for direktør- og fakturabedrageri, og kan bli påført store tap.[29] Ved direktørbedrageri vil cyberkriminelle ofte søke å få urettmessig tilgang til en virksomhets internkommunikasjon over tid for å tilegne seg kunnskap som høyner sjansene for at bedrageriene lykkes. Svindel og bedragerier begås her ved bruk av både datainnbrudd og påvirkningsmetoder som målrettet phishing.

Utpressing

Det digitale rom er arena for både høy- og lavteknologiske avarter av utpressing. Digital utpressing kan handle om digitale verdier eller at utpressingen foregår digitalt. Det vanligste er at gjerningspersonen besitter digital informasjon om eller eid av den fornærmede, og at informasjonen brukes til å presse den fornærmede for penger eller seksuelle tjenester. Truslene dreier seg normalt om ødeleggelse, spredning eller offentliggjøring av informasjonen.

De fornærmede har ingen garanti for at truslene ikke settes ut i livet selv om de imøtekommer kravene til utpresseren. Det er så godt som umulig å hindre videre spredning av digital informasjon når den først har kommet på avveie. Noen blir også utsatt for gjentatt utpressing, enten av samme gjerningsperson, eller av flere som utnytter den samme sårbarheten. Dette bidrar til å øke utpressingens avkastningspotensial.

Seksuell utpressing med seksuelt eller økonomisk motiv er en vedvarende trussel. Som regel tilegner gjerningspersonen seg seksualisert materiale ved å forlede offeret til å dele dette frivillig. Deretter benyttes materialet til å presse de fornærmede til å dele mer og grovere seksualisert materiale, eller de presses til å betale gjerningspersonen penger. Dersom ofrene ikke gjør som gjerningspersonen sier, trues de med at det seksualiserte materialet deles på offerets egen konto i sosiale medier eller sendes til venner og familie. Tidligere var ofrene for seksuell utpressing med økonomisk motiv voksne menn, men det siste året har flere og flere barn og unge gutter blitt utsatt for dette.

Løsepengevirus er skadevare som blir

[29] Dette inkluderer såkalt BEC – fra engelsk: Business Email Compromise.

benyttet til å kryptere filer i datasystemer slik at de blir utilgjengelige for de rettmessige brukerne, med mindre de betaler løsepenger. Utbyttet kreves betalt i kryptovaluta. Å betale løsepenger garanterer ikke at filene blir tilgjengelige igjen. Fornærmede som betaler, kan oppleve å bli utpresset på ny. Kriminelle begår ofte datatyveri i kombinasjon med kryptering og påfølgende utpressing, og truer med offentliggjøring av stjålne data som en del av utpressingen.[30] Man har også sett tilfeller av at gjerningspersonene i tillegg truer med tjenestenektangrep,[31] alt for å legge mer press på offeret og øke sjansen for at utpressingen skal lykkes.

Alle samfunnssektorer og både offentlige og private virksomheter, utsettes for løsepengevirus. De senere årene har kriminelle fokusert på virksomheter framfor privatpersoner.

Skadevarene brukt mot norske mål er godt kjent fra kriminalitet i andre land. Kriminelle som begår datainnbrudd og løsepengevirusangrep mot norske virksomheter, begår slik kriminalitet mot mål over hele verden, og fremgangsmåtene er ofte de samme.

Løsepengevirus kan føre til store tap og høye kostnader for å gjenopprette driften hos den enkelte virksomhet. Når en virksomhet med en kritisk samfunnsfunksjon[32] blir rammet av løsepengevirus, vil bortfall eller forringelse av funksjonen kunne få store konsekvenser for samfunnet. Både private og offentlige virksomheter i Norge har slike funksjoner.

Antallet anmeldte løsepengevirusangrep har sunket det siste året. Flere oversikter viser en mindre nedgang i registrert kriminalitet mot datasystemer fra 2021 til 2022. Dette kan tyde på en reell nedgang i antall gjennomførte utpressinger med løsepengevirus mot norske virksomheter i 2022, sammenlignet med 2021. Tallgrunnlaget er imidlertid lite.

Det er koblinger mellom flere sentrale personer i løsepengevirusmiljøet internasjonalt. Aktører skifter og bytter grupper, og samarbeider med andre. Krypteringsskadevarer endres og bytter navn. Denne

---

30 Såkalt dobbel utpressing

31 Såkalt trippel utpressing

32 Kritiske samfunnsfunksjoner er de funksjoner som er nødvendige for å ivareta befolkningens og samfunnets grunnleggende behov og befolkningens trygghetsfølelse. Grunnleggende behov er definert som mat, vann, trygghet m.m.

flyktigheten gjør det mindre relevant å fokusere på én type skadevare eller en gruppe. Det er derfor nødvendig å fokusere på de komponentene av utøvelsen som benyttes av flere aktører.

Veldig få personer i Norge trenger å være bekymret for utpressing i den analoge verden. I det digitale rom er situasjonen annerledes. Privatpersoner kan bli ofre for direkte utpressing, eller indirekte ved at deres personlige data kan bli stjålet og publisert av kriminelle i forbindelse med løsepengevirus mot både offentlige og private virksomheter.

Seksuallovbrudd

Seksuallovbrudd støttet av datasystemer omfatter straffbare handlinger som voldtekt, oppbevaring og deling av overgrepsmateriale, og seksuell utpressing. Norske fornærmede er utsatt for kriminelle lokalisert både i Norge og utlandet. Tilsvarende begår norske gjerningspersoner kriminalitet mot ofre over hele verden.

Seksuelle overgrep mot mindreårige begått med internett som redskap rammer en særlig sårbar offergruppe. De fleste mindreårige bruker ulike digitale kommunikasjonsplattformer, som del av deres vanlige sosiale liv. For voksne som ønsker å begå overgrep mot barn er det enkelt å tilnærme seg mindreårige på nett, med relativt lav oppdagelsesrisiko.

Politiet mottar stadig flere tips fra tjenestetilbydere, blant annet via National Center for Missing and Exploited Children (NCMEC), som gir mulighet for å avdekke overgripere og opprette flere straffesaker innen seksuallovbrudd. Det økende informasjonstilfanget vil kunne føre til en økning i den registrerte kriminaliteten, men gjenspeiler ikke nødvendigvis en reell økning i kriminaliteten.

Selv om det er registrert flere faktorer som påvirker utviklingen har truslene knyttet til seksuelle overgrep mot barn på internett vært relativt stabile det siste året. Det er likevel registrert en endring av kjente modi blant annet i organiseringen av kriminaliteten, grovheten ved blant annet seksuell utpressing, og ved at både fornærmede og gjerningspersoner blir yngre.

Fra 11–12-årsalderen har omtrent alle barn i Norge egen mobil. Den unge alderen på mobilbrukerne gjenspeiles i kriminalitetsutviklingen. Barn som selger egenprodusert overgrepsmateriale, blir stadig yngre. Barn ned i 10-årsalderen selger seksualisert materiale av seg selv. Barn og unge som selger overgrepsmateriale av seg selv, er ofte veldig aktive på digitale plattformer og er generelt ukritiske med tanke på nettvett. Motivene de oppgir er spenning og lettjente penger.

Teknologien gjør det enklere for en

gjerningsperson å begå overgrep mot mange ofre. Direkteoverførte bestillingsovergrep, kjøp av egenprodusert overgrepsmateriale fra barn og seksuell utpressing på internett er eksempler på sakstyper der gjerningspersonene ofte har mange ofre, samtidig som de fornærmede sjelden anmelder overgrepene, og oppdagelsesrisikoen generelt er lav.

Mange av de kriminelle som begår seksuallovbrudd støttet av datasystemer har kjennskap til enkelte av politiets metoder og fremgangsmåter, og utvikler mottiltak for å unngå oppdagelse og straff. Flere gjerningspersoner har god teknisk kompetanse. De yngre gjerningspersonene besitter ofte mer kunnskap og har en bedre operasjonell sikkerhet enn de eldre. Kjente anonymiserings- og skjermingsteknologier blir tatt i bruk.

Deling av overgrepsmateriale krever samhandling blant seksualforbrytere over internett, men organiseringsgraden varierer. Ende-til-ende-krypterte meldingstjenester ser for eksempel ut til å kreve lite organisering og administrering. Til gjengjeld vil det ofte være strengere sikkerhetstiltak for å få tilgang til chattegruppene. Til sammenligning ser seksualforbrytere på TOR-nettverket i større grad ut til å organisere seg i forbindelse med deling av overgrepsmateriale på chattesider eller i internettfora.

Overgrepssider med forum og chattesider skaper et fellesskap der overgrep mot barn normaliseres, noe som kan føre til at enkelte seksualforbrytere som tidligere ikke har begått seksuelle overgrep, velger å begå fysiske overgrep. Spesielt er TOR-nettverket en trussel ikke bare knyttet til deling av overgrepsmateriale. Det er også et sted for opplæring og erfaringsdeling seksualforbrytere imellom, og det preges av gruppepress og tilhørighetsbehov.

I et globalt perspektiv vil bedre internettilgang i stadig flere land sannsynligvis føre til at flere barn og unge blir utsatt for seksuallovbrudd støttet av datasystemer. Spesielt bekymringsverdig er dette i land preget av fattigdom, der det å selge overgrep mot barn over internett kan være en attraktiv måte å tjene penger på.

Direkteoverførte bestillingsovergrep mot barn i land preget av fattigdom er en alvorlig trussel innen seksuelle overgrep mot barn over internett. Til tross for at de norske gjerningspersonene ikke er i fysisk kontakt med barna utsetter de barn over hele verden for voldtekt og overgrep ved hjelp av enkel teknologi, i samarbeid med voksne som er fysisk til stede med barna.

De mest prominente aktørene blir gjerne etterspurt og vil oppnå større profitt gjennom sitt rennomé.

Kriminalitet mot datasystemer

Tilnærmet all verdiskapning i Norge er avhengig av datasystemer. De fleste datasystemer har en kontaktflate mot internett. Dette åpner opp for nye muligheter og sårbarheter.

Norge har opplevd en mengde kriminalitet mot datasystemer, både hos privatpersoner og hos offentlige og private virksomheter. Motivene bak de kriminelle handlingene varierer, men de er som oftest vinning. Andre motiver kan være ideologi, behov for anerkjennelse og tilhørighet, hevn og spionasje.

Datainnbrudd

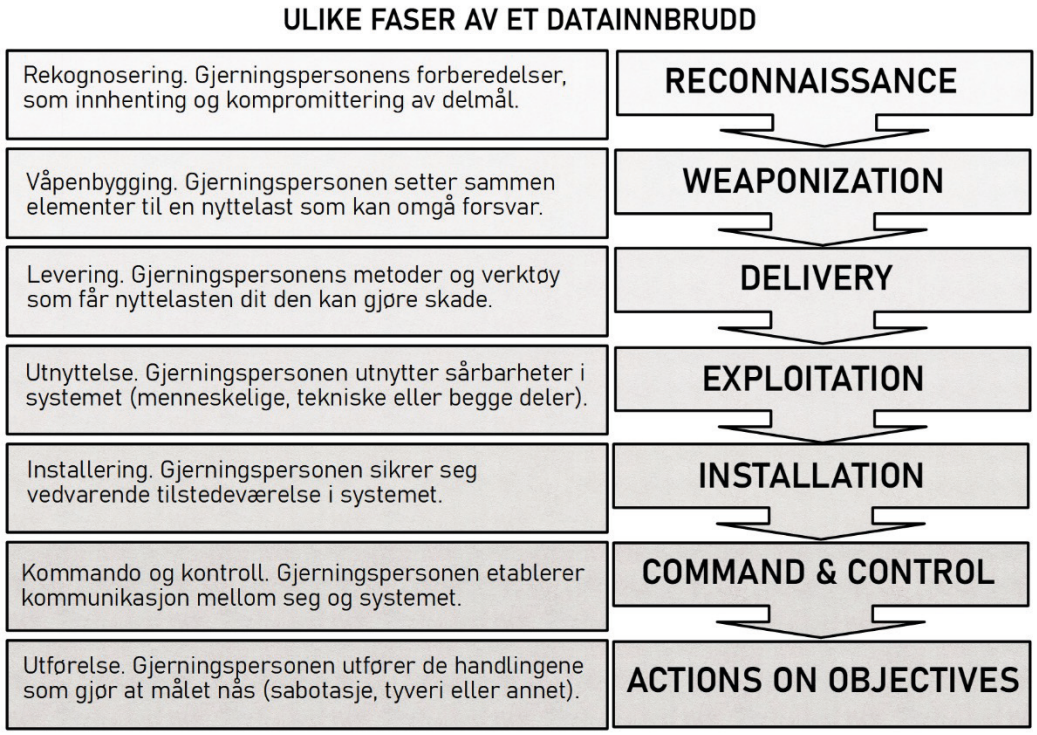
Datainnbrudd er en forutsetning for mye annen kriminalitet. Datainnbrudd skal sikre gjerningspersonen urettmessig tilgang til datasystemet der videre kriminalitet kan utøves[33], og er et lovbrudd i seg selv.

I etterkant av datainnbrudd har Kripos registrert tilfeller av datatyveri, kryptering med påfølgende utpressing, utvinning av kryptovaluta, og etablering av botnett.

Gjerningspersonene må lykkes med en rekke steg for å gjennomføre kriminalitet mot datasystemer via datainnbrudd. Først må de kjøpe, utvikle eller stjele tilgang til skadevare eller privateid[34] programvare med de nødvendige funksjonene, eller de må benytte åpent tilgjengelig programvare. Deretter må de oppnå tilgang til fornærmedes datasystem, for eksempel ved bruk av stjålne påloggingsdetaljer, sosial manipulasjon eller sårbarheter i systemets knytning til internett. De må også etablere en egen digital infrastruktur som lar dem utnytte denne tilgangen, overføre skadevare, stjele, oppbevare og offentliggjøre

[33] Tilgangen kan for eksempel benyttes til å skaffe seg tilgang til andre datasystemer, stjele, kryptere eller slette informasjon, eller plassere ut skadevare i datasystemet.

[34] Kjent som proprietær programvare, til forskjell fra åpen kildekode.



Illustrasjonen over er basert på cybersikkerhetsbransjens såkalte Cyber Kill Chain.

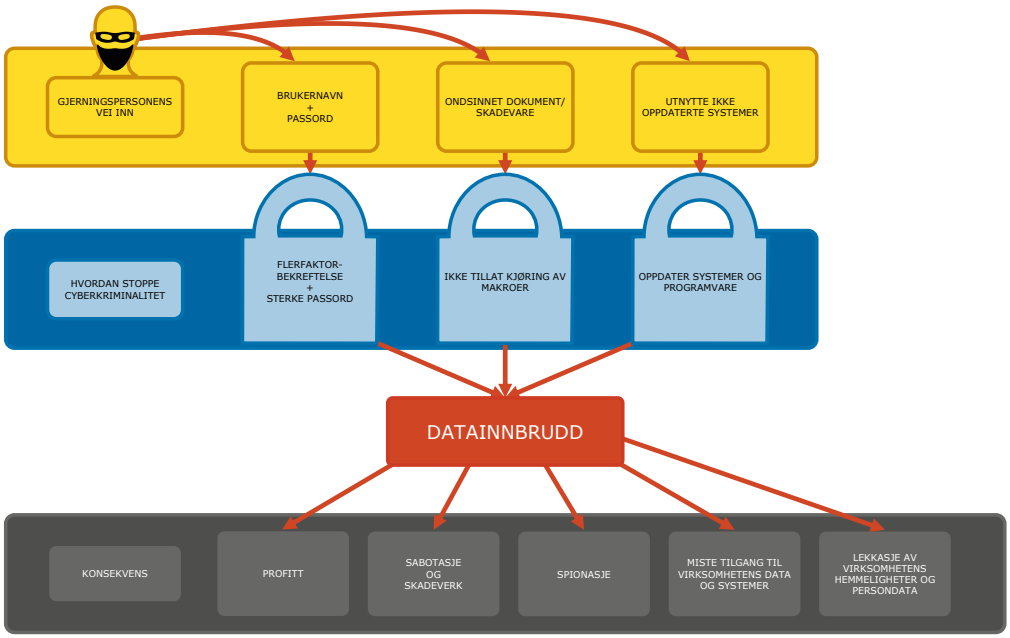
potensielt store mengder data, kryptere filer og slette sikkerhetskopier. Til sist må de ha systemer og folk som administrerer eventuell kontakt med ofrene, betaling av løsepenger og hvitvasking av utbytte. Selve datainnbruddet følger som regel en stegvis oppskrift som starter med rekognosering og ender med måloppnåelse:

Et datainnbrudd kan bestå av flere elementer som kan kreve betydelig kompetanse hos gjerningspersonene. Kripos ser at komplekse datainnbrudd gjerne utøves av flere i et samarbeid fremfor av enkeltpersoner. De ulike gjerningspersonene har forskjellige roller og ansvar, og de tilbyr ekspertisen sin der behovet måtte være. Slik skifter samarbeidskonstellasjonene hele tiden. De mest prominente aktørene blir gjerne etterspurt

og vil oppnå større profitt gjennom sitt renommé.

Urettmessig tilgang til et datasystem oppnås på flere måter. Gjerningspersonene kan stjele gyldig påloggingsinformasjon selv eller kjøpe den fra andre kriminelle. De kan bruke rå datakraft[35] til å teste ut alle mulige kombinasjoner fram til pålogging lykkes, utnytte tekniske sårbarheter i systemets koblinger til internett, eller utnytte menneskelige sårbarheter gjennom phishing. Sårbarheter i hjemmekontor-, fjernarbeids- og VPN-løsninger gjør slik kommunikasjon over internett utsatt.

Kripos har registrert alle de nevnte angrepsvektorene, noen ganger i kombinasjon med hverandre.



Modellen viser eksempler på gjerningsmenns vei inn i et datasystem og de etterfølgende konsekvensene. Figuren er inspirert av Oslo PD.

[35] Eng: brute-force

Flere oversikter viser en liten nedgang i registrert kriminalitet mot datasystemer fra 2021 til 2022. Kripos mener mørketallene er store.

Datatyveri

Målet for mye cyberkriminalitet er andres data. Alt som er digitalisert, kan stjeles. Dette innebærer ikke at den rettmessige eieren nødvendigvis mister tilgangen til sine digitaliserte produkter. Kriminelle vil i utgangspunktet sikre seg kopier av de digitale produktene for å få hånd om informasjonen.

Sannsynligheten for å bli oppdaget kan øke med mengden av informasjon som hentes ut og hvor lang tid gjerningspersonene oppholder seg i fornærmedes nettverk. Oppdagelse kan resultere i at man mister tilgangen, og at ens identitet blir avslørt. Det er vanlig å slette digitale spor etter at datatyveriet er gjennomført.

Politiet mottar jevnlig informasjon om e-poster med lenker til falske sider hvor hensikten er å lure til seg passord eller annen sensitiv informasjon som kan gi tilgang til ulike private kontoer.[36] Der kontoen har blitt overtatt har gjerningspersonen i noen tilfeller tatt kontakt og krevd penger eller truet med vold. Sensitiv informasjon har i andre tilfeller blitt tilegnet ved at det arrangeres falske konkurranser der man må oppgi informasjon for å delta eller for å få premien. Noen har opplevd å bli kontaktet av noen som de tror er en venn, men der det viser seg at vennen i realiteten har blitt utsatt for datatyveri. Det er også observert at kompromitterte kontoer benyttes til å dele eller spre overgrepsmateriale.

Digitalt skadeverk

Digitalt skadeverk kjennetegnes ved at digitale verdier blir utilgjengeliggjort, forringet eller gjort verdiløse ved ødeleggelse. Ødeleggelse kan skje ved at hele eller vitale deler av den digitale informasjonen slettes. Digitale verdier kan gjøres ubrukelige gjennom for eksempel kryptering, eller ved at den kriminelle først stjeler informasjonen og lagrer den på et sted utilgjengelig for den fornærmede, for så å slette informasjonen eller fornærmedes tilgang til den.

Tjenestenektangrep er et eksempel på slikt digitalt skadeverk. De har som formål å forhindre eller forringe tilgangen til en tjener, tjeneste eller et nettverk. Tjenestenektangrep mot virksomheter er en del av det cyberkriminelle normalbil-

[36] Facebook, Instagram m.fl.

det. Gjerningspersoner utnytter botnett til å overvelde mål med nettverkstrafikk. Tilgang til slike botnett selges ofte av kriminelle med ekspertkompetanse som en tjeneste til mindre sofistikerte kriminelle.

Konsekvensene av et tjenestenektangrep er som regel ikke store, og angrepet blir ofte håndtert raskt.

Samtidig er det viktig å forstå at noen angrep kan få større konsekvenser enn andre. Det er stor forskjell på om det er en tjenestes nettside eller selve tjenesten som blir utsatt for et tjenestenektangrep. I det siste tilfellet vil tjenesten ikke fungere, noe som vil ha mye større følger enn om publikum ikke får tilgang til tjenestens hjemmesider. Et tjenestenektangrep kan også rettes mot deler av en virksomhet, som gjør at de ansatte ikke kan benytte seg av tjenester de trenger for å utføre sitt arbeid.

Et tjenestenektangrep kan ramme en hel virksomhet, men også privatpersoner. Angrepene er som regel målrettede, men kan også ramme utilsiktet. Mengden datatrafikk som må til for å gjennomføre et vellykket tjenestenektangrep, avhenger av trafikk- og responskapasiteten til den som rammes. Deler av cybersikkerhetsindustrien har spesialisert seg på å selge tjenester som forsvarer mot tjenestenektangrep.

Politisk motiverte, ulovlige aksjoner på nett utføres av ulike grupper for å fremme deres sak.[37] I 2022 erfarte Kripos at tjenestenektangrep ble brukt som politisk virkemiddel for å skape oppmerksomhet. Ved Russlands invasjon av Ukraina valgte flere kriminelle grupperinger å støtte forskjellig side i konflikten offentlig.

[37] Såkalt hacktivisme.

Forventet utvikling i 2023

Med det redegjorte situasjonsbildet som bakgrunn, og med egne og innsamlede data som grunnlag, har Kripos gjort vurderinger av cyberkriminalitetens utvikling i 2023.

Tidligere har gjerningspersoner som har rammet norske virksomheter vært lokalisert i utlandet. Det er *sannsynlig* at vi framover vil registrere organiserte cyberkriminelle som opererer fra Norge, med fornærmede i både inn- og utland.

Cyberkriminelle tar raskt ny teknologi i bruk, og er også raske til å utnytte oppdukkende sårbarheter. Endringen i ekomloven vil *meget sannsynlig* føre til at flere gjerningspersoner vil benytte anonymiseringsteknologier som VPN. Kripos vurderer at det er *sannsynlig* at anonymiseringsmulighetene vil øke i tiden fremover som følge av videre teknologisk utvikling. Avdekking og etterforskning av cyberkriminalitet vil følgelig bli vanskeligere.

Det er *sannsynlig* at det totale antall forsøk på datainnbrudd vil øke fra foregående år. Teknologisk utvikling og økt tilgjengelighet av tjenester tilbudt av kriminelle aktører vil profesjonalisere metoder og kapabiliteter, samtidig som flere kriminelle aktører vil ha mulighet til å leie inn slike tjenester.

Det er *sannsynlig* at det totale antallet vellykkede datainnbrudd mot små og mellomstore bedrifter vil øke på grunn av spesialisering av roller og oppgaver hos kriminelle tjenestetilbydere. Samtidig som det digitale kriminelle økosystemet modnes, vil også metoder og kapabiliteter optimaliseres. Det pågående våpenkappløpet krever økt kapabilitet og spissere kompetanse både hos mulige ofre og hos gjerningspersonene. Bedriftene som ikke har eller ikke prioriterer ressurser til å beskytte sine verdier i takt med trusselens utvikling, vil være spesielt sårbare for datainnbrudd.

Det er *sannsynlig* at svindel og bedragerier støttet av datasystemer vil øke de neste tolv månedene, på grunn av økt kommersialisering av cyberkriminalitet,

og få effektive reduserende mottiltak.

Det er *sannsynlig* at cyberkriminelle vil benytte eksisterende og nye virtuelle verdier til bedragerier og hvitvasking, eksempelvis gjennom investeringer i kryptokunst. Norske offentlige og private virksomheter vil bli rammet av løsepengevirus i 2023. Det er *meget sannsynlig* at hoveddelen av løsepengevirusangrep mot offentlige og private virksomheter i 2023 vil være opportunistiske, profittmotiverte angrep. Løsepengevirusangrep har tidligere rammet virksomheter innen eksempelvis offshore, varehandel og industri. Virksomhetene som rammes, er generelt av en viss størrelse med en viss inntjening. Det er *meget sannsynlig* at virksomheter med tilknytning til samfunnskritiske funksjoner vil rammes av løsepengevirus i 2023.

Seksuallovbrudd støttet av datasystemer er en vedvarende høy trussel. Det er *sannsynlig* at det vil være en eskalering av allerede kjente modi i form av grovhet, konsekvenser og stadig yngre ofre og gjerningspersoner.

Det er *sannsynlig* at norske seksualforbrytere i stadig større grad vil benytte ende-til-ende krypterte meldingstjenester til en-til-en distribusjon av overgrepsmateriale og til deling i grupper.

Det er *sannsynlig* at politisk motiverte tjenestenektangrep vil fortsette i 2023. Kjente grupperinger som har valgt side i Russlands krig mot Ukraina forventes å fortsette sin aktivitet. Det er *mulig* at det vil oppstå flere og nye former for politisk motiverte, ulovlige aksjoner på nett mot norske virksomheter.

Det er *sannsynlig* at pandemien og Russlands krig mot Ukraina har bidratt til noe nedgang i flere typer cyberkriminalitet i 2021–2022, spesielt kriminalitet mot datasystemer. Norge kan i 2023 *mulig* erfare en økning i slik kriminalitet, hvis en ny sikkerhetspolitisk normalsituasjon etablerer seg.

Det er *sannsynlig* at vi framover vil registrere organiserte cyberkriminelle som opererer fra Norge, med fornærmede i både inn- og utland.

Vedlegg

Sannsynlighetsord

Vurderinger vil alltid inneholde en grad av usikkerhet. For å håndtere dette på en standardisert og strukturert måte, er det benyttet sannsynlighetsord (se tabell):

Nasjonal standard	Beskrivelse	NATO standard
Meget sannsynlig	Det er meget god grunn til å forvente...	Highly likely (>90%)
Sannsynlig	Det er grunn til å forvente...	Likely (60-90%)
Mulig	Det er like sannsynlig som usannsynlig...	Even chance (40-60%)
Svært lite sannsynlig	Det er svært liten grunn til å forvente...	Highly unlikely <10%

POLITIET
KRIPOS

Kripos
Postadresse: Postboks 2094 Vika, 0125 Oslo
Besøksadresse: Nils Hansens vei 25, 0667 Oslo

Kontakt: 23 20 80 00 / kripos@politiet.no
Tips politiet om cyberkriminalitet: https://tips.politiet.no/web/