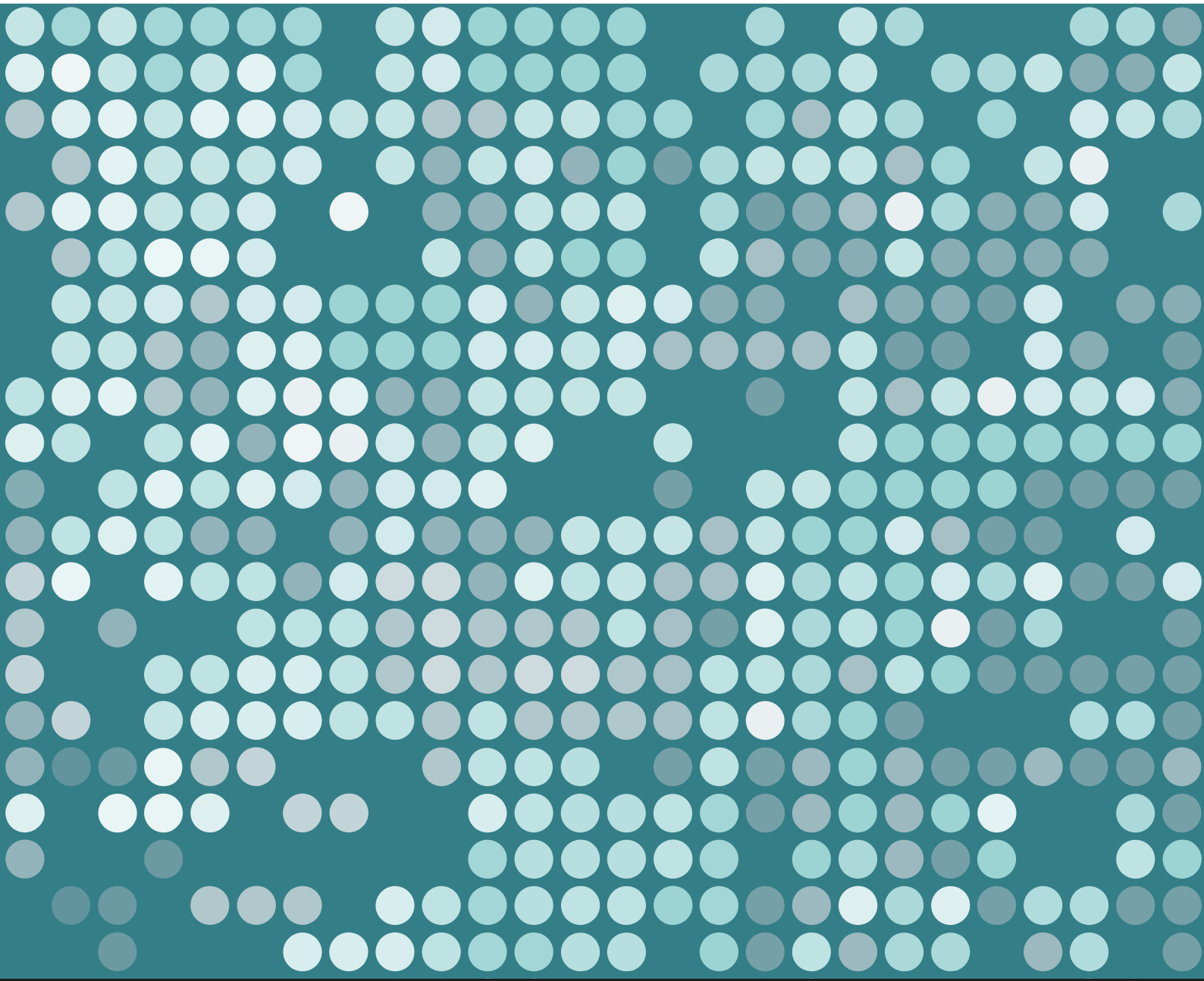
Rapport 2022:8



Polisanmälda dataintrång

Karaktär, utmaningar, utvecklingsområden

Brå – kunskapscentrum för rättsväsendet
Myndigheten Brå verkar för att brottsligheten minskar och tryggheten ökar i samhället. Det gör vi genom att ta fram fakta och sprida kunskap om brottslighet, brottsbekämpning och brottsförebyggande arbete, till i första hand regeringen och myndigheter inom rättsväsendet.

Publikationen finns som pdf på www.bra.se. På begäran kan Brå ta fram ett alternativt format. Frågor om alternativa format skickas till tillgangligt@bra.se

Författare: Elina Lindskog, Lou Huuva, Sarah Lehtinen, David Shannon

urn:nbn:se:bra-1074

Brottsförebyggande rådet, Box 1386, 111 93 Stockholm
Telefon 08-527 58 400, e-post info@bra.se, www.bra.se

Polisanmälda dataintrångsbrott

Karaktär, utmaningar, utvecklingsområden

Rapport 2022:8

Förord

Samhällets digitalisering innebära stora möjligheter, men skapar också sårbarheter som kan utnyttjas av kriminella aktörer. En central brottstyp i detta sammanhang är dataintrång, som handlar om allt från att kapa någons sociala mediakonto till att olagligen få tillgång till myndigheters eller företags datorsystem i syfte att exempelvis stjäla kundinformation eller kryptera information i utpressningssyfte.

I den här rapporten presenterar Brå en samlad överblick över karaktären på de dataintrång som anmäls till polisen och en beskrivning av de utmaningar som rättsväsendets aktörer står inför i sitt arbete med att utreda och lagföra brotten. Brå beskriver även utvecklingsområden för polisens arbete mot dataintrång. Rapporten vänder sig i första hand till Polismyndigheten, Åklagarmyndigheten och regeringen.

Författare till rapporten är Elina Lindskog (projektledare), Lou Huuva, Sarah Lehtinen och David Shannon, samtliga verksamma vid Brå. Brå vill särskilt tacka professor emeritus Sven-Åke Lindgren (Göteborgs universitet) och tekn.dr Ulrik Franke, senior forskare vid Research Institutes of Sweden (RISE), som har vetenskapligt granskat ett utkast till rapporten och lämnat mycket värdefulla synpunkter. Det är dock Brå som i alla avseenden är ansvarigt för innehållet i rapporten. Avslutningsvis vill Brå rikta ett varmt tack till de intervjupersoner som deltagit i studien och de experter som ingått i projektets olika referensgrupper.

Stockholm i oktober 2022

Mattias Larsson
Generaldirektör

David Shannon
Enhetschef

Innehållsförteckning

Sammanfattning

Dataintrång är att olovligen bereda sig tillgång till en uppgift som är avsedd för automatiserad behandling eller att olovligen ändra, utplåna, blockera eller i register föra in en sådan uppgift. Begreppet dataintrång samlar därmed brott som sker inom ramen för flera olika typer av brottsupplägg. Det är allt från dataintrång av enklare karaktär som att i sitt arbete göra otillåtna slagningar i olika register eller att kapa konton på sociala medier, till mer komplexa dataintrång där någon försöker att olagligen få tillgång till en dator eller ett datorsystem i syfte att orsaka skada genom att blockera tjänster, stjäla eller förstöra information, eller kryptera information i utpressningssyfte.

Även om dataintrång kan se väldigt olika ut i sina upplägg karaktäriseras de av att de sker i en digital och många gånger internationell kontext, vilket försvårar polisens och åklagarnas utredningsarbete. Denna rapport har som syfte att beskriva de dataintrång som anmäls i dag samt de svårigheter som polis och åklagare möter i arbetet med att utreda och lagföra i synnerhet de mer komplexa dataintrångsbrotten. För att uppnå syftet utgår studien från följande frågeställningar:

1. Vilka typer av dataintrång och tillhörande brottsupplägg anmäls till polisen, och vilka är det som utsätts respektive misstänks för dessa dataintrång?
2. Vilka typer av dataintrång leder till, respektive leder inte till, personuppklaring?
3. Vilka svårigheter upplever polis och åklagare i arbetet med att utreda och lagföra komplexa dataintrång?

Rapporten lyfter även förslag på utvecklingsområden för rättsväsendets utredningsarbete samt vikten av att nå ut med information för att förebygga och därmed minska antalet dataintrång i samhället.

Fokus på de mer komplexa dataintrångsbrotten

I Sverige polisanmäldes närmare 9 000 dataintrång 2020 med en ökning till drygt 11 000 dataintrång 2021, vilket troligtvis bara är en bråkdel av de dataintrång som begås eftersom mörkertalet anses vara stort (Europol 2020).

Polisen tillämpar fem olika brottskoder för att skilja mellan olika typer av dataintrång

- dataintrång genom överbelastningsattack
- dataintrång med hjälp av skadlig kod i utpressningssyfte
- dataintrång genom olovlig registerslagning
- dataintrång i sociala medier eller e-tjänster
- övrigt dataintrång.

Polismyndigheten skiljer sådana dataintrång som faller inom ramen för det som betraktas som komplex cyberbrottslighet, såsom dataintrång genom överbelastningsattack och dataintrång med hjälp av skadlig kod i utpressningssyfte, från dataintrång av enklare karaktär såsom dataintrång i sociala medier eller e-tjänster och dataintrång genom olovlig registerslagning. Denna rapport har ett särskilt fokus på utredningsarbetet kopplat till de mer komplexa dataintrången, som utreds vid polisens expertfunktioner för utredning av komplexa cyberbrott vid Polismyndighetens olika it-brottscentrum.

Rapporten bygger på en granskning av polisanmälningar och förundersökningsmaterial samt intervjuer

Två datamaterial har använts för att belysa studiens frågeställningar. Frågeställning 1 och 2 om vilka typer av dataintrång som anmäls till polisen respektive vilka typer som leder till personuppklaring besvaras genom en granskning av ett urval av 641 polisanmälningar som gjordes under perioden juli till december 2020 och i förekommande fall förundersökningsmaterial kopplat till dessa anmälningar.

För att besvara frågeställning 3 om vilka svårigheter poliser och åklagare upplever i utredningsarbetet har 30 intervjuer genomförts med polisanställda och åklagare samt även andra aktörer inom både privat och offentlig sektor som bevakar olika aspekter av dataintrångsbrottslighet som en del av sitt arbete. Dessa intervjuer är också ett underlag för de utvecklingsområden som beskrivs i rapporten.

Övergripande resultat

De polisanmälda dataintrångens karaktär

Dataintrång som en del av annan brottslighet

Dataintrång kan vara en enskild händelse eller ingå som ett initialt steg för att i ett senare skede begå ytterligare brott. Studiens resultat visar att när andra brott förekommer i de granskade ärendena är det vanligt att dataintrånget använts som ett steg i att begå bedrägeri- eller utpressningsbrott. Med undantag för dataintrång genom olovliga registerslagningar, förekommer bedrägeribrott eller utpressningsbrott tillsammans med dataintrång i mellan 20 och närmare 27 procent av de granskade dataintrångsanmälningarna.

Vid anmälningar om dataintrång i sociala medier och e-tjänster är det dock vanligare att dataintrånget skett i kombination med brott mot frihet och frid, särskilt olovlig identitetsanvändning, än att dataintrånget använts för att begå bedrägeri- och utpressningsbrott. Vid anmälningar om dataintrång genom olovliga registerslagningar är det vanligt att anmälan också avser tjänstefel eller brott mot tystnadsplikt.

Dataintrång drabbar både juridiska personer och privatpersoner

Studien visar att företag och verksamheter inom offentlig och ideell sektor i något större utsträckning anmäler mer komplexa dataintrång (överbelastningsattacker och dataintrång genom skadlig kod i utpressningssyfte) jämfört med privatpersoner, medan privatpersoner i större utsträckning är målsägare i de andra typerna av ärenden.

De företag som drabbas av dataintrång varierar från små firmor och egenföretagare till stora företag, som exempelvis har beskrivit att en förlorad åtkomst till sina servrar som resultat av skadlig kod kan kosta dem miljontals kronor om dagen. Förutom överbelastningsattacker och utpressning med hjälp av skadlig kod visar anmälningarna att dataintrång också används för att utsätta företag för bland annat informationsstöld och bedrägerier.

De privatpersoner som utsätts för dataintrång är män och kvinnor i många olika åldersgrupper, från skolbarn till personer i 80-årsåldern. Samtidigt förekommer vissa köns- och åldersskillnader. Till exempel förekommer kvinnor oftare än män som målsägare i anmälningarna om dataintrång i sociala medier och e-tjänster.

Bland privatpersonerna finns ingen åldersgrupp som verkar vara särskilt utsatt för en viss typ av dataintrång, men jämfört med de övriga typer av dataintrång som studerats är det vanligare att målsägaren är under 18 år i anmälningar där dataintrång i sociala medier använts för att utsätta målsägaren för mobbning, förnedring eller för att utöva kontroll över målsägaren. Det är framför allt kvinnor som anmäler den här typen av dataintrång. Det är även något fler kvinnor än män som anmäler dataintrång i sociala medier och e-tjänster som är kopplade till bedrägeribrott.

De personuppklarade och nedlagda dataintrångsbrotten

Personuppklaringen låg för dataintrång

Studiens resultat visar att personuppklaringen för dataintrång är låg i de ärenden som Brå har granskat. Det finns ändå en variation i uppklaringen mellan de olika brottskoderna. De allra flesta brott som personuppklaras är olovliga registerslagningar, där en femtedel av de studerade anmälningarna har lett till åtal och fem procent resulterat i ett strafföreläggande.

Åtal har väckts i endast ett överbelastningsärende och i två ärenden om övrigt dataintrång. För dataintrång genom skadlig kod i utpressningssyfte och dataintrång i sociala medier och e-tjänster har inget av de granskade ärendena lett till personuppklaring.

Resultaten visar alltså att de allra flesta av de anmälda dataintrången som Brå granskat inte personuppklaras. De flesta anmälningarna har antingen resulterat i en direktavskrivning, till exempel för att spaningsuppslag saknas, eller en nedlagd förundersökning, bland annat på grund av att det saknats spaningsresultat eller svårigheter med att säkra bevisning.

Vanligare att en misstänkt person knyts till brottet vid olovliga registerslagningar

Vid de flesta anmälda dataintrången finns det ingen skäligen misstänkt gärningsperson. Den enda typ av dataintrång där en skäligen misstänkt knyts till brottet i en majoritet av ärendena är dataintrång genom olovlig registerslagning. Dessa brott skiljer sig från de övriga typerna av dataintrång genom att slagningarna ofta sker på gärningspersonens arbetsplats och loggas i organisationens it-system, vilket underlättar identifieringen av en misstänkt gärningsperson.

Dock finns även en del dataintrång, som framför allt rör anmälningar som registrerats som övrigt dataintrång eller dataintrång i sociala medier eller e-tjänster av mer personlig karaktär, där målsägare redan vid anmälningstillfället beskrivit för polisen att de misstänker att brottet begåtts av en specifik person. I dessa fall är den misstänkte i de allra flesta fall antingen en bekant eller en partner eller före detta partner till målsägaren.

Utredningssvårigheter och utmaningar

Svårigheter i flera led av utredningsarbetet

Intervjupersonerna beskriver svårigheter i flera led i utredningsarbetet, i synnerhet när det gäller de mer komplexa dataintrångsbrotten. Det handlar om allt från att det finns ett bristande engagemang hos målsägare att delta i utredningen, särskilt hos utsatta företag, till svårigheter med att få tillgång till data från operatörer och från molntjänster.

Ett återkommande tema i Brås intervjuer med de rättsliga aktörerna är att en överbelastad it-forensisk verksamhet medför långa ledtider. Detta äventyrar utredningsarbetet eftersom digital bevisning är en färskvara och ju längre tid man får vänta på resultat från it-forensiska analyser desto större är risken att den information som behövs för att föra utredningen vidare inte finns kvar när man väl får de it-forensiska resultat som ger möjlighet att inhämta den.

Intervjupersonerna lyfter även andra utmaningar. Anmälningsbenägenheten är låg, och i kombination med att polisens kontaktcenter (PKC) ibland direktavskriver ärenden som borde ha skickats vidare till de specialiserade enheterna för utredning, samt en bristande samordning av dataintrångs-ärenden, medför detta att den utredande verksamheten inte har en bra bild av de brott som begås, vilket ytterligare försvårar utredningsarbetet.

Särskilda svårigheter kopplade till dataintrångsbrottslighetens internationella karaktär

Många dataintrångsbrott sker över nationella gränser, i synnerhet de komplexa dataintrången som överbelastningsattacker och utpressning genom skadlig kod. Kriminella grupperingar i andra länder genomför organiserade attacker mot bland annat svenska företag. Utredningar med fokus på dessa brott kräver ett fungerade och effektivt samarbete mellan rättsväsenden i olika länder, till exempel när det gäller att begära hjälp med utredningsåtgärder genom rättslig hjälp eller en europeisk utredningsorder

(EIO). Intervjupersonerna uppger dock att denna process är tidsödande, samtidigt som det är viktigt att snabbt få tillgång till digital bevisning.

En underutvecklad polisiär organisation för utredning av komplexa cyberbrott

Brås intervjuer visar att den svenska polisen i dag i mångt och mycket fortfarande arbetar på ett relativt traditionellt sätt mot dataintrångsbrottsligheten. Till exempel utreds de komplexa dataintrångsbrotten framför allt vid it-brottscentrum i respektive region. En slutsats från Brås intervjuer med både privata aktörer och anställda inom rättsväsendet är att polisens arbetssätt behöver utvecklas för att förbättra möjligheterna att komma längre med utredningar och bidra mer till det internationella samarbetet mot den växande cyberbrottsligheten.

Brås bedömning

En mer utvecklad och ändamålsenlig polisiär cyberbrottsinfrastruktur

Brås intervjuer med personer i olika positioner inom polisorganisationen ger en samlad bild av en polisiär infrastruktur för utredning av komplexa cyberbrott som fortfarande är under uppbyggnad, och som också är sårbar. Organisationen med regionala it-brottscentrum är relativt ny, och det saknas en tydlig samordningsfunktion på nationell nivå. Utifrån Brås granskning framstår ett behov av ett mer uthålligt utredningsarbete, där enskilda ärenden inte läggs ner för fort, och där man får bättre möjligheter att identifiera och samordna ärenden som härrör från samma kriminella aktör, både regionalt och nationellt, till exempel genom att arbeta i team där det ingår representanter från såväl regionerna som det nationella it-brottscentrumet. Ett mer uthålligt arbete skulle också ge bättre möjligheter att arbeta fram utredningsunderlag som kan vara till nytta i internationella polisoperationer mot den organiserade cyberbrottsligheten.

En viktig förutsättning för arbetet är också att det finns en dedikerad it-forensisk kompetens kopplad till utredningarna. Enligt Brås intervjupersoner finns i dag en dedikerad it-forensisk kompetens kopplad till utredningsarbetet i vissa regioner men inte i andra. I de fall där det saknas en dedikerad it-forensisk resurs måste cyberbrottsutredningar konkurrera med andra typer av brottsutredningar, bland annat sådana där en person har häktats. Vikten av att snabbt kunna inhämta och analysera it-forensiskt material innebär att avsaknaden av en dedikerad resurs är en stoppkloss i utredningsarbetet som riskerar hela utredningen. Det finns också behov av

att utveckla en bättre samverkan mellan polisen och privata aktörer inom it-säkerhetsområdet, bland annat för att ge polisen en förbättrad insyn i cyberbrottslighetens utveckling, aktiva kriminella grupperingar, skadlig digital infrastruktur och nya brottsupplägg.

Det är dock viktigt att inse att förbättrade utredningsförutsättningar sannolikt inte kommer att medföra någon markant ökning av antalet lagföringar för dataintrång just i Sverige, eftersom de komplexa brotten ofta begås av aktörer utanför Sveriges gränser. Ett utvecklat polisiärt utredningsarbete med fokus på det internationella samarbetet med rättsväsenden i andra länder skulle ge den svenska polisen bättre möjligheter att bidra till brottsbekämpningsarbetet, men för att uppnå detta finns ett behov av nya prestationsmått för polisens cyberbrottsbekämpning, som inte baseras på personuppklaring.

En fortsatt modernisering av relevant lagstiftning

Polisens möjligheter att utreda komplexa cyberbrott, inklusive dataintrång, är beroende av en ändamålsenlig lagstiftning. En utmaning som lyfts både i tidigare Brårapporter (t.ex. Brå 2015, Brå 2016a) och i intervjuerna med polis och åklagare i den här studien är att lagstiftningen inte har hängt med i den digitala brottsutvecklingen. Under de senaste åren har regeringen tillsatt ett flertal utredningar i syfte att se över olika delar av lagstiftningen kopplat till rättsväsendets möjligheter att få tillgång till elektroniska uppgifter, och dessa har resulterat i en lagstiftning som bland annat förbättrat möjligheterna att få tillgång till information som finns lagrad i molnet. Ett fortsatt arbete med att modernisera lagstiftningen och anpassa den efter den föränderliga digitala verkligheten är också en förutsättning för att de brottsbekämpande myndigheterna ska kunna arbeta effektivt mot dataintrång och andra typer av cyberbrott.

Uppmaningar och stöd för att skydda sig mot dataintrång

Dataintrångsbrott är en viktig del av den cyberbrottslighet som har ökat i takt med teknikutvecklingen och den tilltagande digitaliseringen av samhället. Brottsligheten omsätter stora värden, sker i organiserad form och kommer sannolikt att fortsätta att öka. Överlag behöver brottsligheten betraktas som ett betydande nuvarande och framtida hot mot såväl svenska företag och medborgare som landets digitala infrastruktur.

Mot bakgrund av denna hotbild och de svårigheter som kännetecknar utrednings- och lagföringsarbetet är det viktigt med uppmaningar och stöd till företag, andra organisationer och privatpersoner för att de ska kunna skydda sig mot dataintrång.

En viktig slutsats från Brås diskussioner med experter inom cybersäkerhet är att ett centralt mål för det förebyggande arbetet bör vara att få flera internetanvändare att ta till sig de möjligheter som finns för att skydda sig mot dataintrång. De flesta dataintrång sker med hjälp av enkla metoder och skulle kunna förhindras. Det finns redan i dag välutvecklade säkerhetslösningar och rekommendationer för att skydda sig mot dataintrång, och information om dessa lösningar finns samlad hos olika aktörer, bland annat Myndigheten för samhällsskydd och beredskap (MSB).

Utmaningen för det brottsförebyggande arbetet är att nå ut med dessa rekommendationer och få fler att tillämpa dem. Redan i dag sker generella informationskampanjer i detta syfte, men enligt forskningen ökar sannolikheten att åstadkomma beteendeförändringar om informationsinsatser riktas på ett mer direkt och anpassat sätt till olika målgrupper. Därför är det viktigt att även andra aktörer tar den information som finns samlad och anpassar och sprider den till sina egna målgrupper, till exempel inom skolan och högskolesektorn, bransch- och intresseorganisationer samt enskilda företag och myndigheter.

Inledning

Digitaliseringen har på många sätt förenklat människors vardag. Allt mer information finns tillgänglig via nätet och vi blir mer och mer beroende av digitala kommunikationsvägar i våra dagliga liv. Samtidigt sparas allt mer känslig information i olika datasystem, och allt fler samhällsviktiga system är kopplade till internet. Digitalisering innebär stora möjligheter men även risker som kan drabba den enskilde individen såväl som centrala samhällsfunktioner och företag.

En central brottstyp i detta sammanhang är dataintrång. Dataintrångsbestämmelsen samlar brott som sker inom ramen för flera olika typer av brottsupplägg, allt från enklare dataintrång som att i sitt arbete göra otillåtna slagningar i olika register eller att kapa konton på sociala medier, till komplexa dataintrång där någon försöker att olagligen få tillgång till en dator eller ett datorsystem i syfte att orsaka skada genom att blockera tjänster, stjäla eller förstöra information, eller kryptera information i utpressningssyfte. I Sverige polisanmäldes närmare 9 000 dataintrång 2020 med en ökning till drygt 11 000 dataintrång 2021. Dessa är troligtvis bara en bråkdel av de dataintrång som begås eftersom mörkertalet anses vara stort (Europol 2020).

Även om dataintrång kan se väldigt olika ut till sitt upplägg karaktäriseras de av att de sker i en digital och många gånger internationell kontext, vilket försvårar polisens och åklagarnas utredningsarbete. Polismyndigheten har uppmärksammat Brå på att det finns ett behov av ett kunskapsunderlag om dataintrång, dels för att få en mer samlad överblick över karaktären på de dataintrång som anmäls, dels för att kunna förbättra utredningsförutsättningarna.

Studiens syfte och frågeställningar

Syftet med studien är att ge en beskrivning av de dataintrång som anmäls i dag samt de svårigheter som polis och åklagare stöter på i arbetet med att utreda och lagföra i synnerhet de mer komplexa dataintrångsbrotten. För att uppnå syftet utgår studien från följande frågeställningar:

1. Vilka typer av dataintrång och tillhörande brottsupplägg anmäls till polisen, och vilka är det som utsätts respektive misstänks för dessa

dataintrång?
2. Vilka typer av dataintrång leder till, respektive leder inte till, personuppklaring?
3. Vilka svårigheter upplever polis och åklagare i arbetet med att utreda och lagföra komplexa dataintrång?

Rapporten lyfter även förslag på utvecklingsområden för rättsväsendets utredningsarbete och vikten av att sprida information om hur man kan skydda sig mot dataintrång.

Rapportens disposition

Detta kapitel fortsätter med en övergripande beskrivning av lagbestämmelsen om dataintrång, liksom olika tillvägagångssätt vid de mer komplexa dataintrångsbrotten. Därefter följer en kort beskrivning av viktiga aktörer inom cybersäkerhetsområdet. Kapitlet avslutas med en beskrivning av rättsväsendets hantering av dataintrång, och en övergripande genomgång av de utmaningar i rättsväsendets hantering av it-relaterad brottslighet som uppmärksammats av tidigare studier. I nästa kapitel presenteras de olika datamaterial som har använts för att besvara rapportens frågeställningar. Därefter presenteras rapportens resultat. Det första resultatkapitlet redogör för de polisanmälda dataintrångens karaktär, vilket följs av ett kapitel som redovisar hur många av de granskade dataintrångsärendena som lett till personuppklaring. Därefter beskrivs de utredningssvårigheter som rättsväsendets aktörer upplever med att utreda och lagföra framför allt komplexa dataintrång, liksom utmaningar som påverkar möjligheterna att arbeta med dataintrångsärenden på ett effektivt sätt. Det sista kapitlet lyfter utvecklingsområden för utredningsarbete med dataintrångsbrottsligheten samt vikten av att nå ut med information för att förebygga och därmed minska antalet dataintrång i samhället.

Bestämmelsen om dataintrång

I Datastraffrättsutredningens slutbetänkande från 1992 uppges att Sverige var det första landet i världen som kriminaliserade hacking[1] när bestämmelsen om dataintrång infördes i datalagen 1973 (1973:289) (SOU 1992:110). Dataintrång flyttades till sin nuvarande plats i brottsbalken (4

[1] Hacking definieras i SOU 1992:110 som att ”någon olovligen bereder sig tillgång till upptagning för automatisk behandling” (s. 62).

kap. 9 c §) år 1998 när datalagen ersattes med personuppgiftslagen (1998:204). Dataintrångsbestämmelsen lyder i dag enligt följande:

> Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.
>
> Är brottet grovt, döms för grovt dataintrång till fängelse i lägst sex månader och högst sex år. Vid bedömande av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art.

Att bereda sig tillgång till uppgifter innebär att man kan begå dataintrång utan att ha tagit del av informationen i uppgiften. Det innebär att själva handlingen att olovligen ta sig in i ett datasystem är olaglig (prop. 2006/07:66). Det bör betonas att det inte enbart är själva intrånget som är kriminaliserat i bestämmelsen. Det är även olagligt att utan tillstånd göra ändringar, radera, blockera eller att föra in ny information i ett sådant system. I propositionen anges ”inmatning eller spridning av olika typer av sabotageprogram (t.ex. datavirus, trojaner eller logiska bomber)” som exempel på vad som omfattas av lagen (prop. 2006/07:66 s. 50).

Ändringar i bestämmelsen om dataintrång

Sedan 1998 har bestämmelsen om dataintrång ändrats två gånger. Den första ändringen infördes 2007, då det gjordes ett tillägg för att kriminalisera att olovligen blockera, störa eller hindra en uppgift som är avsedd för automatisk behandling. Syftet var att genomföra EU:s rambeslut om angrepp mot informationssystem (prop. 2006/07:66). I praktiken innebar detta att även så kallade överbelastningsattacker (på engelska kallat Distributed denial of service, DDoS, attack) inkluderades i bestämmelsen. I samband med denna förändring kriminaliserades även försök och förberedelse till dataintrång.

Bestämmelsen ändrades igen 2014, då grovt dataintrång infördes för att särskilt kunna bestraffa allvarliga dataintrång (prop. 2013/14:92). I och med införandet av denna bestämmelse uppfyllde Sverige kraven i Europaparlamentets och rådets direktiv 2013/40/EU, direktiv om angrepp mot informationssystem.

Beskrivning av dataintrångsbrottsligheten

Dataintrångsbestämmelsen täcker in en mängd olika typer av brottsliga handlingar. Det kan handla om att en person kommer över inloggningsuppgifter och använder dem till att olovligen logga in på någons konto på sociala medier, eller att en person har tillgång till ett dataregister eller databas i tjänsten och gör olovliga slagningar på personer som de inte handlägger inom ramen för sitt arbete, till mer komplexa brott som överbelastnings- eller ransomwareattacker. Fokus för denna rapport riktas främst på de mer komplexa brotten. Nedan följer en övergripande redogörelse för: tillvägagångssätt vid dataintrång, skadlig programvara, hur dataintrång kan användas för att begå ytterligare brott, brottslighetens kopplingar till marknadsplatser för försäljning av olika kriminella tjänster, och till sist viktiga aktörer som på olika sätt arbetar mot dataintrångs-brottsligheten. Därefter redogörs för rättsväsendets hantering av dataintrång.

Tillvägagångssätt vid dataintrång

Det finns olika sätt att begå dataintrång. Hacking eller cracking kan enligt Yar and Steinmetz (2019) definieras som kriminella aktiviteter förknippade med obehörig åtkomst eller störning av datorsystem. En hacker letar efter sårbarheter i både hård- och mjukvara och använder sig ofta av skadlig programvara (se beskrivning nedan) för att ta sig in i ett system. När hackern väl är inne i ett system kan denne skapa, manipulera, flytta, kopiera eller ta bort innehåll i systemet och kan bereda sig möjlighet att fjärrstyra system samt neka brottsoffret åtkomst till filer i systemet (Maimon och Louderback 2019).

Angriparen får ofta initial åtkomst till systemet genom att helt enkelt logga in med inloggningsuppgifter som angriparen kan ha fått tag på genom exempelvis använda lösenord från läkta databaser. Ett annat vanligt sätt är att angriparen får åtkomst till system genom att använda sig av någon form av social engineering (Europol 2021). Social engineering innebär att en person som har tillgång till ett datasystem ovetandes kan luras till att vidta åtgärder som möjliggör för angriparens olagliga aktivitet (Salahdine och Kaabouch 2019). Vid dataintrång sker social engineering ofta genom phishing (nätfiske på svenska), vilket innebär att angriparen skickar ett mejl i ett försök att få mottagaren att lämna ifrån sig inloggningsuppgifter alternativt klicka på en länk eller bifogad fil som laddar ner skadlig kod (FRA m.fl. 2020). En trend är nätfiske som riktar in sig mot specifika personer inom en organisation, så kallad *spearphishing* (Europol 2020).

Skadlig programvara används ofta vid dataintrång

Skadlig kod (på engelska malware) används som ett samlingsbegrepp för olika typer av programkoder (exempelvis virus eller trojaner) som är utformade för att på olika sätt störa ett datasystems normala funktioner (Yar och Steinmetz 2019). *Ransomware* anses ofta vara den skadliga kod som orsakar mest problem online i dag (Europol 2021). Ransomware fungerar på så sätt att den krypterar filer så att användaren inte får tillgång till dem. Efter att datorn infekterats begärs en lösensumma för att få hjälp med att låsa upp datorn igen eller för att få tillgång till krypteringsnyckeln. Oftast ska lösensumman betalas i kryptovalutor såsom bitcoin då detta försvårar spårningen av gärningsaktören (Paquet-Clouston 2019).

En *trojan* är en annan vanlig typ av skadlig programvara som gömmer sig inuti andra program men ser ut som legitim programvara för att lura användaren att ladda ner programmet (ofta genom nätfiske) och på så sätt oavsiktligen släpper in skadlig kod på sin enhet (Yar och Steinmetz 2019). En trojan kan vara ett spionprogram som gör det möjligt för angriparen att få tillgång till exempelvis lösenord, registrering av tangenttryckningar (så kallade keyloggers) eller annan värdefull information. En vanlig funktion hos trojaner är att de kan fjärrstyras, så kallade *Remote Accsess Trojan* (RAT). Kriminella använder fjärrstyrningstrojaner bland annat för att skapa så kallade botnets (kort för robotnätverk). Dessa är nätverk av infekterade datorer (eller andra typer av enheter med uppkoppling mot internet) som kan fjärrstyras av en och samma individ (se t.ex. Hoque m.fl. 2015). Storleken på ett botnet kan variera; en känd botnet som stängdes ned under 2017 är det så kallade Andromeda-botnätet som hade över 2 miljoner datorer knutna till sig (Europol 2018). Ett botnet kan användas till att skicka stora mängder skräppost, sprida skadlig kod eller till att utföra överbelastningsattacker.

Dataintrång i syfte att störa tillgång till nätverk

Ett vanligt syfte med dataintrång är att störa tillgången till nätverk, vilket kan göras genom överbelastningsattacker (ENISA 2021). En överbelastningsattack är ett angrepp som är riktat mot ett nätverk, ett datorsystem eller en webbplats, webbtjänst eller liknande med syftet att göra den otillgänglig genom att överbelasta den med trafik (Europol 2018). På senare tid har överbelastningsattacker också börjat användas i utpressningssyfte (Europol 2020, FBI IC3 12-10-2017).

Dataintrång i syfte att begå vidare brottslighet

Dataintrång kan ske för att till exempel komma åt personuppgifter, som sedan kan användas för att begå vidare brottslighet. Det kan röra sig om namn, adress och personnummer men även användarinformation såsom inloggningsuppgifter till banktjänster eller molntjänster[2], kontokortsuppgifter eller personfoto (från exempelvis sociala medieplattformar). Enligt Integritetsskyddsmyndigheten (IMY 2021) utgör personuppgifter ett centralt värde i dagens digitala ekonomi. De kan till exempel användas i marknadsföringssyfte för att analysera inköpsmönster för olika grupper och det finns många aktörer som specialiserar sig på handel med dessa typer av uppgifter (så kallade datamäklare). Handeln med personuppgifter kan även vara illegal och ske på darkweb[3] (ibid.). Informationen som stjäls genom dataintrång kan även bestå av immateriella rättigheter från företag, såsom patent, forskningsresultat eller annan värdefull information. Det förekommer också att angriparen använder den olovligt inhämtade informationen i utpressningssyfte genom att hota med att publicera eller sälja materialet vidare om de drabbade inte betalar en lösensumma (Europol 2020).

Dataintrång kan även användas som en metod för att blockera eller störa samhällsviktiga funktioner. Enligt den militära underrättelse- och säkerhetstjänsten (MUST) pågår det kontinuerliga försök till dataintrång och kartläggning av svenska nätverk med syfte att inhämta information eller förbereda för sabotage (MUST 2022). Försvarsberedningen, som analyserar den säkerhetspolitiska utvecklingen, skriver i sin slutrapport om *Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025* (Ds 2019:8) att de mest kvalificerade hoten inom cyberområdet utgörs av cyberangrepp utförda av stater eller statligt finansierade grupper. Effekterna av ett sådant cyberangrepp kan liknas vid ett konventionellt väpnat angrepp eftersom ett cyberangrepp kan slå ut samhällsviktiga funktioner som eldistributionen (ibid.). Vid ett omfattande elavbrott skulle alla it-system, betalsystem och all handel störas, liksom all digital kommunikation och alla

[2] Molntjänster är it-tjänster som låter användaren hantera program, processorkraft, datalagring och annat online i stället för lokalt på datorn eller mobilen.

[3] Darkweb är ett antal slutna nätverk, vars åtkomst kräver speciella programvaror som gör att användare inte går att spåra. Eftersom besöken där sker anonymt och betalningar sker via kryptovalutor såsom bitcoin, kan köpare och säljare på dessa platser hålla sig anonyma.

transporter som tåg och flyg, men även bilar eftersom det krävs el för att kunna tanka.

Dataintrång och organiserad brottslighet

Dataintrång har viktiga kopplingar till den organiserade brottsligheten. På marknadsplatser på *darkweb* pågår försäljning av tjänster och program som kan användas för att begå olika former av brott, bland annat dataintrång, vilket kallas C*rime-as-a-service (CaaS)*. Speciellt vanligt är det att kriminella använder sig av *Ransomware-as-a-Service (RaaS),* vilket innebär att man köper sig tillgång till en plattform varifrån angreppet sedan utförs. RaaS beskrivs som en affärsmodell som möjliggör för angriparen att enkelt genomföra ransomwareattacker utan att behöva ha teknisk kompetens om kodning eller hackning. Vidare innebär affärsmodellen att RaaS-grupperingen och angriparen som köper tjänsten kommer överens om en avgift per insamlad lösensumma (Europol 2021). För att få större spridning av skadlig kod kan dessa angripare rikta in sig på mjukvaruleverantörer, för att sedan sprida den vidare till mjukvaruleverantörens kunder, detta kallas *supply chain attack* (ibid., FRA m.fl. 2019). Det har även blivit allt enklare att köpa en överbelastningsattack online (Europol 2018). Dessa fungerar på så sätt att man betalar för att en överbelastningsattack ska utföras mot ett utvalt offer, och den kriminella använder sedan sitt botnet för att genomföra attacken (ibid.). Försäljningen av den här typen av tjänster och program har ökat under de senaste åren och innebär att de som begår dataintrång inte längre behöver vara tekniskt kunniga (Europol 2021).[4] Det är dessutom relativt enkelt att hålla sig anonym när betalningen sker med kryptovalutor, som bitcoin (Paquet-Clouston m.fl. 2019).

Den digitala organiserade brottsligheten underlättas av en möjliggörande infrastruktur (Europol 2020). Det handlar bland annat om så kallade skottsäkra hostingtjänster [5], som vägrar lämna ut information till rättsliga aktörer, och tveksamma kryptovalutaväxlare, som förenklar kriminellas möjligheter att hålla sig anonyma online (ibid.). I den möjliggörande infrastrukturen ingår även kriminella som säljer databaser med person-

[4] I slutbetänkandet från utredningen om it-brottskonventionen anges att det räknas som förberedelse till dataintrång att skapa eller sälja program som används till att begå dataintrång (SOU 2013:39).

[5] Företag som erbjuder hosting erbjuder helt enkelt möjlighet att vara värd för en webbplats genom att upplåta utrymme på sin server. Det enklaste och billigaste sättet att skapa en egen hemsida eller webbplats är att använda sig av ett så kallat webbhotell.

uppgifter (till exempel inloggningsuppgifter som kan användas för att begå dataintrång), och så kallade *initial access brokers* (som har berett sig tillgång till nätverk och sedan säljer vidare sin kunskap om tillvägagångssätten).

Viktiga aktörer inom cybersäkerhet

Rättsväsendets myndigheter är de enda aktörerna som äger mandat att lagföra dataintrång, men det finns många viktiga aktörer som på olika sätt arbetar med cybersäkerhet. På EU-nivå finns Europol och Enisa. Europol är den Europeiska unionens byrå för brottsbekämpning. Europol arbetar med att bistå EU:s medlemsstater i bekämpningen av grov organiserad brottslighet och terrorism. De samarbetar även med medlemsstater utanför EU. Enisa är den Europeiska unionens cybersäkerhetsbyrå vars uppgift är att säkerställa att medlemsstaterna uppnår en hög nivå av cybersäkerhet. Arbetet inom EU med att öka cybersäkerheten har bland annat resulterat i NIS-direktivet, en lagstiftning på EU-nivå som implementerades i NIS-lagen (2018:1174).[6] Lagen innebär krav på att företag som levererar samhällsviktiga tjänster och vissa digitala tjänster är säkra och tillförlitliga, exempelvis inom energi- och transportsektorn. Inom EU finns även CERT-EU, Incidenthanterings-organisationen för EU:s institutioner och byråer (Cert-EU) som rör it-infrastruktur.[7] Sverige har även en nationell CSERT, CERT-SE, som bedriver motsvarande arbete i Sverige. CERT-SE är i sin tur en del av Myndigheten för samhällsskydd och beredskap (MSB) med uppdrag kopplade till it- och cybersäkerhet.

Det finns även myndigheter som arbetar för att motverka cyberangrepp och bidra till Sveriges cyberförsvar. Försvarsmakten ansvarar för Sveriges offensiva cyberförsvar och tillsammans med Försvarets radioanstalt (FRA) och Säkerhetspolisen ansvarar de även för Sveriges defensiva cyberförsvar. Den militära säkerhets- och underrättelsetjänsten MUST genomför exempelvis omvärldsanalyser för att identifiera och analysera yttre hot mot Sverige inom cyberområdet, medan FRA har exempelvis olika tekniker för att identifiera skadlig kod i nätverk samt ger stöd och råd till skyddsvärda myndigheter och samhällsfunktioner.

---

[6] Hösten 2022 beräknas NIS2-direktivet träda i kraft, som ersätter NIS-direktivet och kommer omsättas i svensk lagstiftning.

[7] Se en av Europeiska unionens officiella webbplatser för information om incidenthanteringsorganisationen för EU:s institutioner och byråer (CERT-EU): https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/cert-eu_sv

Regeringen har därtill gett Försvarets radioanstalt (FRA), Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB) och Säkerhetspolisen i uppdrag att bygga upp ett nationellt cybersäkerhetscenter för att ”stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot” (regeringsbeslut Fö2019/01330 s. 2). Uppbyggnaden av cybersäkerhetscentret ska ske stegvis från 2021 fram till 2023 och i nära samverkan med Försvarets materielverk (FMV), Polismyndigheten och Post- och telestyrelsen (PTS). Det övergripande syftet med cybersäkerhetscentret är att möjliggöra för dessa myndigheter att agera mer samordnat, förbättra informations- och kunskapsdelning samt stärka förmågan att stödja offentlig verksamhet och näringsliv.

Utöver dessa statliga och överstatliga organisationer finns det många privata aktörer som arbetar med cybersäkerhet, exempelvis privata it-säkerhets-företag som erbjuder företag och privatpersoner säkerhetslösningar för att skydda sig mot bland annat dataintrång.

Rättsväsendets hantering av dataintrång

När brottsutredande myndigheter upptar en brottsanmälan, registreras brotten med hjälp av olika brottskoder. Syftet med brottskoderna är att kunna föra statistik över vilka brott som anmäls samt att vara till hjälp i polisens operativa verksamhet, resultatredovisning och resursfördelning (Brå 2022). Tidigare omfattades alla dataintrång av en enda brottskod (0415 Dataintrång) men sedan juli 2020 finns fem brottskoder för att skilja mellan olika typer av dataintrång. De nya koderna skapades bland annat i syfte att tillgodose de krav som ställdes i Europaparlamentets och rådets direktiv 2013/40/EU, om att statistiken ska kunna visa om anmälda brott kan klassas som angrepp mot informationssystem. De skapades även för att Polismyndigheten efterfrågade en kategorisering som kunde särskilja dataintrång som faller inom ramen för komplex cyberbrottslighet från de mer enkla dataintrången, i syfte att lättare kunna organisera arbetet med brotten. De nya brottskoderna är

- 9464 Dataintrång genom överbelastningsattack
- 9465 Dataintrång med hjälp av skadlig kod i utpressningssyfte
- 9466 Dataintrång genom olovlig registerslagning
- 9467 Dataintrång i sociala medier eller e-tjänster

- 9468 Övrigt dataintrång[8].

Polisens organisation vid hanteringen av dataintrång

Från Polismyndighetens sida var syftet med införandet av flera brottskoder även att förenkla och effektivisera hanteringen av dataintrångsärenden. Dataintrång i sociala medier eller e-tjänster och dataintrång genom olovlig registerslagning anses vara enklare i sin karaktär och utreds på lokalpolisområdesnivå. Om misstanke om olovliga registerslagningar riktas mot exempelvis en polisanställd, polisstudent, domare eller åklagare utreds ärendet dock vid avdelningen för särskilda utredningar (SU), som är en fristående och oberoende avdelning inom Polismyndigheten.

Dataintrång genom överbelastningsattack och dataintrång med hjälp av skadlig kod i utpressningssyfte betecknas som komplexa dataintrång, och lämnas i stället till polisens expertfunktioner för utredning av komplexa cyberbrott vid landets olika it-brottscentrum.[9] Även en del av det som registreras som ”övrigt dataintrång” utreds som komplexa cyberbrott, om det handlar om dataintrång med hjälp av exempelvis trojaner.

It-brottscentrum finns i dag både på regional och nationell nivå. Vid Polismyndighetens Nationella operativa avdelning (Noa) etablerades år 2015 ett nationellt it-brottscentrum – Swedish cybercrime center (SC3). På centret finns bland annat en grupp för utredning av komplexa cyberbrott (KCB-gruppen), inklusive dataintrång. Vidare tog Polismyndigheten ett beslut 2017 om att samtliga sju polisregioner skulle inrätta regionala it-brottscentrum (RC3) i syfte att samla kompetens för att bättre kunna utreda it-relaterade brott, såsom internetrelaterade sexuella övergrepp mot barn och komplexa cyberbrott. Förutom it-brottscentrumen arbetar även polisens underrättelsetjänst vid Noa med att upptäcka, identifiera och förebygga cyberbrott.

---

[8] Kategori övrigt inkluderar dataintrång som inte omfattas av ovanstående brottstyper.

[9] Inom polisen används begreppet komplexa cyberbrott (KCB) för brott där brottsverktyget eller målet för brottet är digital information eller den utrustning som hanterar den digitala informationen. Det som gör brottsligheten mer komplex kan vara att den riktas mot samhällsviktig verksamhet, är en del av organiserad brottslighet eller tekniskt avancerad (se till exempel Polismyndigheten m.fl. 2019). Enligt Nationellt underrättelsecentrum (Nuc) sker mycket av den komplexa cyberbrottsligheten (KCB) via dataintrång (ibid.). Dataintrång genom överbelastningsattack och dataintrång med hjälp av skadlig kod räknas till komplexa dataintrång.

Internationellt samarbete

Tanken med det nationella it-brottscentrumet (SC3) är att det ska återspegla *European cybercrime center (EC3),* som är det europeiska organ som på olika sätt arbetar för att stärka brottsbekämpande åtgärder mot it-relaterad brottslighet och en del av Europol. Vid EC3 finns även den internationella polisstyrkan J-CAT[10], där representanter från olika länders rättsväsenden medverkar för att dela information och samarbeta för att bekämpa it-relaterad brottslighet.

Åklagarmyndighetens organisation kring hantering av dataintrång

Hos Åklagarmyndigheten är det generellt sett inte särskilda åklagare som är utsedda att vara förundersökningsledare i dataintrångsärenden. Vid komplex cyberbrottslighet lottas dock ärendena ofta till förundersökningsledare som sitter på Riksenheten mot internationell och organiserad brottslighet (RIO). RIO bildades 2018 genom att Åklagarmyndighetens tre internationella åklagarkammare slogs samman till en organisatorisk enhet med specialistkompetens för att bekämpa den organiserade och gränsöverskridande brottsligheten, där komplexa dataintrångsbrott ingår som del.

Sedan 2015 finns det även ett nätverk för kontaktåklagare med särskild it-kompetens. Dit kan åklagare vända sig om de behöver hjälp med frågor kopplade till it-relaterade brott, exempelvis vid inhämtning av bevisning. Varje åklagarkammare har en utpekad kontaktåklagare för it-brott. Förutom nätverket med kontaktåklagare så finns det en utpekad åklagare som är ämnesspecialist för it-brott. Denne har ett nationellt ansvar för strategiska frågor och utvecklingsfrågor kring it-brott och samverkar med Åklagarmyndighetens utvecklingscentrum i Stockholm.

När det gäller dataintrång genom olovliga registerslagningar där brottsmisstanke riktas mot exempelvis en polisanställd, polisstudent, domare eller åklagare leds förundersökningen alltid av en åklagare vid Särskilda åklagarkammaren, SÅK.

[10] J-CAT (Joint Cybercrime Action Taskforce) har i uppdrag att koordinera internationella utredningar, bland annat med fokus på dataintrångsrelaterad brottslighet.

Internationellt samarbete

Utredningar om dataintrång kräver ofta ett internationellt samarbete och Åklagarmyndigheten har, liksom Polismyndigheten, internationella kontaktpunkter för till exempel utbyte av information inom området. Vid Eurojust[11] finns till exempel *European Juridical Cybercrime Network (EJCN),* där representanter från olika länders åklagarmyndigheter möts för att diskutera gemensamma problem inom området och ta fram information. Eurojust kan även hjälpa till vid koordineringsmöten mellan rättsväsenden inom olika länder som till exempel vill diskutera ett ärende med en gemensam gärningsperson. Det finns även möjligheter för åklagare att starta gemensamma bi- eller multilaterala utredningsgrupper genom att inleda ett Joint Investigation Team (JIT) (dessa kan även inkludera utomeuropeiska länder). Detta kan bland annat förenkla både delning av bevis mellan olika länder och koordinerade insatser, till exempel vid husrannsakan. Åklagarmyndigheten har även en kontaktperson vid European Juridical Network (EJN)[12], som bland annat behandlar frågor som rör it-relaterad brottslighet.

Utmaningar i rättsväsendets hantering av it-relaterad brottslighet enligt tidigare studier

Tidigare studier och myndighetsgranskningar har identifierat ett flertal utmaningar i rättsväsendets hantering av it-relaterad brottslighet, med relevans för frågan om möjligheterna att utreda och lagföra dataintrångsbrottsligheten.

Bristande kompetens och kapacitet att utreda it-relaterad brottslighet

Brå har i tidigare studier berört rättsväsendets förmåga att hantera it-inslag i brottsligheten,[13] särskilt i Brå 2016a var detta huvudfokuset. Studien visade att en stor andel av de åklagare, polisiära förundersökningsledare och it-forensiker som deltog i studiens enkäter eller intervjuer upplevde att de saknade den nödvändiga kompetensen i sitt arbete med it-relaterad

[11] Eurojust är Europeiska unionens byrå för straffrättsligt samarbete med huvudkontor i Haag i Nederländerna. Den bildades 2002 för att arbeta med samordningen av utredningar mellan rättsväsenden i EU vid bekämpningen av grov organiserad brottslighet.

[12] European Juridical Network (EJN) är ett nätverk inom EU (separat från Eurojust), med rättsliga kontaktpunkter i de olika medlemsstaterna genom vilka utbyte av information kan ske. Till exempel om vilka utredningsåtgärder som är möjliga att genomföra i olika länder, hur lagstiftningen ser ut inom olika områden, eller hur man rent administrativt ska gå tillväga vid kontakt eller begäran av EIO.

[13] Se till exempel Brå 2013, Brå 2015, Brå 2016a och Brå 2016b.

brottslighet. Utöver brister i kompetensen har både Brå (2016a) och Riksrevisionen (2015) uppmärksammat brister i Polismyndighetens *kapacitet* att hantera de it-relaterade brotten. Till exempel konstaterade Brå-rapporten att den it-forensiska verksamheten var underbemannad, vilket ledde till att den blev en flaskhals i utredningarna. År 2020 genomförde polisen en intern granskning av den it-forensiska processen inom myndigheten, som också drog slutsatsen att underbemanningen av it-forensiker var stor (Polismyndigheten 2020).

Svårigheter med att utreda brott över nationella gränser

Den it-relaterade brottsligheten sker ofta över nationella gränser och kräver därför ett fungerade och effektivt samarbete mellan rättsväsenden i olika länder, till exempel när det gäller att begära hjälp med att genomföra utredningsåtgärder. Det är vanligt att information som behövs inom ramen för en utredning finns på servrar i ett eller flera andra länder eller att man inte vet var informationen finns lagrad (Europol och Eurojust 2019, SOU 2017:100). En åklagare kan då begära internationell rättslig hjälp i landet där informationen finns lagrad[14] (i de fall man kan utröna detta). År 2017 infördes lagen (2017:1000) om en europeisk utredningsorder (EIO) i Sverige, enligt vilken den åklagare eller domstol som utfärdat utredningsordern skickar den direkt till en behörig myndighet i den medlemsstat där ordern ska verkställas. Enligt Europol och Eurojust (2020) anser dock många inom Europas rättsväsenden att båda dessa förfaranden är problematiska om mottagarlandet inte är samarbetsvilligt och att processen tar tid. Även i Brås rapporter (Brå 2015, Brå 2016a) har det konstaterats att rättslig hjälp är en tidsödande process.

En lagstiftning som inte hängt med i den digitala utvecklingen

Under de senaste åren har flera offentliga utredningar och uttalanden från utredande myndigheter berört problemet att lagstiftningen som reglerar rättsväsendets möjligheter att genomföra utredningsåtgärder skrevs innan dagens digitala verklighet (SOU 2017:89, SOU 2017:100). Samtidigt har det skett en del förändringar på detta område, till exempel genom införandet av

[14] Detta regleras i lagen (2000:562) om internationell rättslig hjälp i brottmål (LIRB).

det nya hemliga tvångsmedlet hemlig dataavläsning (HDA)[15] samt mer nyligen av det nya tvångsmedlet genomsökning på distans[16] som innebär att eftersökning av information kan göras även om informationen inte rent fysiskt finns på det beslagtagna föremålet, utan till exempel i det så kallade molnet. I Sverige tolkas dock den folkrättsliga principen om så kallad exekutiv jurisdiktion på så sätt att genomsökning på distans är möjligt om man kan säkerställa att informationen finns på en server i Sverige. Om man inte kan säkerställa att informationen finns inom Sveriges gränser kan åklagaren dock i vissa fall vända sig till domstol och argumentera för exekutiv jurisdiktion på andra grunder än var information finns lagrad och få saken prövad.

Svårigheter med utlämning av abonnemangsuppgifter

Vid utredningsarbetet av it-relaterade brott är polisen ofta intresserad av att ta reda på information kopplad till en IP-adress (Brå 2016a).[17] Detta förutsätter bland annat att svenska operatörer[18] lämnar ut uppgifter om vilken abonnent som tilldelats IP-adressen vid brottstillfället. Tidigare Bråapporter om it-relaterad brottslighet har lyft att de utredande myndigheterna haft problem med att få ut uppgifter om IP-adresser från internetoperatörer (t.ex. Brå 2013, Brå 2015, Brå 2016a). Vilka krav som ställs på svenska operatörer att spara och lämna ut sådana uppgifter i brottsbekämpande syfte regleras i lagen (2022:482) om elektronisk kommunikation (LEK) och även på detta område har det skett flera förändringar i lagstiftningen de senaste åren, bland annat när det gäller under hur lång tid operatörer är skyldiga att spara olika typer av information.

Ett relaterat problem som också lyfts i tidigare Bråapporter rör användningen av NAT-teknik (Brå 2016a, se även Europol och Eurojust

---

[15] Hemlig dataavläsning innebär i korthet att en mjuk- eller hårdvara installeras i en server, mobiltelefon eller dator och att myndigheterna sedan, utan den misstänktes vetskap, kan ta del av det som finns på en server eller en mobiltelefon såsom meddelanden som annars hade varit krypterade. Lagen trädde i kraft år 2020 och är tidsbegränsad i fem år. Den ska sedan utvärderas.

[16] Modernare regler för användningen av tvångsmedel regleras i lagen om ändring i lagen (2020:62) om hemlig dataavläsning.

[17] En IP-adress är ett nummer som identifierar en anslutning mot internet och som tilldelas av internetleverantören. IP-adressen kan registreras av de internetsajter eller internettjänster som man använder.

[18] I denna rapport används ordet operatör för att beskriva ett företag som tillhandahåller ett elektroniskt kommunikationsnät, ett begrepp som definieras i lagen (2022:482) om elektronisk kommunikation (LEK). Det handlar bland annat om mobiloperatörer och internetleverantörer.

2019). Detta är en teknik som möjliggör för flera enheter (såsom datorer eller telefoner) som är uppkopplade mot internet att dela samma IP-adress.[19] Användningen av NAT-teknik har inneburit att det blivit svårare för polisen att få ut information från operatörer om en specifik innehavare av en viss IP-adress. Tidigare var det så att operatörernas lagringsskyldighet inte omfattade de uppgifter som behövs för att knyta trafiken till specifika adresser vid användning av NAT-teknik. Sedan 1 april 2020 finns dock även regler som innebär att polisen ska få tillgång till de uppgifter som behövs för att identifiera abonnent eller registrerad användare även när NAT-teknik används (PTSFS 2019:2).

[19] I det internetprotokoll som har använts sedan internet slog igenom (IPv4) finns det inte möjlighet till tillräckligt många unika kombinationer av tecken för att varje enhet som är uppkopplad mot internet i dag ska kunna tilldelas en unik IP-adress. Den långsiktiga lösningen på detta är ett internetprotokoll som möjliggör betydligt fler unika teckenkombinationer (IPv6). NAT-tekniken är en lösning fram till att IPv6-används fullt ut.

Metod och material

Denna studie är både kvantitativ och kvalitativ i sin ansats. Frågeställning 1 och 2 (vilka typer av dataintrång som anmäls till polisen respektive vilka typer som leder till personuppklaring) besvaras med hjälp av registerdata från Brås anmälnings- och misstankeregister samt en granskning av polisanmälningar och förundersökningsmaterial från Polismyndigheten. För att besvara frågeställning 3 (vilka svårigheter poliser och åklagare upplever i utredningsarbetet) har intervjuer gjorts med personal vid rättsväsendets myndigheter som arbetar med dataintrång, samt andra aktörer i samhället som bevakar olika aspekter av dataintrångsbrottsligheten som en del i deras arbete.

Polisanmälningar och förundersökningar

Brå har gjort ett urval bland de polisanmälda dataintrången som registrerades i Sverige från juli till och med december 2020. Valet av tidsperiod baserades på att de nya brottskoderna för dataintrång togs i bruk i juli 2020 och för att få ett så aktuellt datamaterial som möjligt vid tiden för studiens datainsamling. Brå har erhållit kriminaldiarienummer för de aktuella anmälningarna och därefter begärt ut handlingar från Polismyndigheten i form av anmälan och i förekommande fall förundersökningar. I materialet ingår såväl ärenden som lagts ned direkt som ärenden där polisen valt att inleda förundersökning. Studiens polisanmälningar och förundersökningar kallas fortsättningsvis för ”förundersökningsmaterial” oavsett om en förundersökning har inletts i ärendet eller inte. Uppgifter från såväl de fritexter som kort beskriver innehållet i varje polisanmälan som uppgifter från förundersökningsmaterial har analyserats.

Urvalsförfarande

Urvalet av polisanmälningar består av 641 ärenden där det ingår minst ett polisanmält dataintrångsbrott (tabell 1).[20] Flera brott kan förekomma i samma ärende. För de brottskoder där antalet anmälda dataintrångsbrott var relativt få samt för de som betecknas som komplexa dataintrång (och därmed utreds vid polisens expertfunktioner för utredning av komplexa cyberbrott)

[20] Den officiella kriminalstatistiken för samma tidsperiod beskrivs inledningsvis i kapitlet De polisanmälda dataintrångens karaktär.

har samtliga polisanmälningar som gjordes under perioden juli till december 2020 inkluderats. Det handlar om *Dataintrång genom överbelastningsattack* och *Dataintrång med hjälp av skadlig kod i utpressningssyfte*, 27 respektive 155 ärenden (tabell 1). Resterande delen av urvalet valdes slumpmässigt med utgångspunkt i att urvalet för respektive brottskod skulle vara tillräckligt stort för att fånga upp variationen i de brottshändelser som registrerats under respektive brottskod. Urvalet för dessa tre brottskoder omfattar 99, 120 respektive 240 anmälningar.[21]

Tabell 1. Det totala antalet polisanmälda ärenden samt antalet ärenden i studiens urval inom respektive brottskod för perioden juli–december 2020.

Brottskod	Totala antalet ärenden som polisanmäldes	Antalet ärenden i studiens urval
Dataintrång genom överbelastningsattack (9464)	27	27
Dataintrång med hjälp av skadlig kod i utpressningssyfte (9465)	155	155
Dataintrång genom olovlig registerslagning (9466)	167	99
Dataintrång i sociala medier eller e-tjänster (9467)	1 757	120
Övrigt dataintrång (9468)	1 650	240
Totalt	3 756	641

Genomgången av ärendena

Information från ärendena i studiens urval har kodats efter ett kodschema, som utarbetades utifrån studiens frågeställningar och som har anpassats till de olika brottskoderna, då karaktären på brotten skiljer sig åt. Hela urvalet kodades för alla brottskoder förutom Övrigt dataintrång, där ett beslut togs om att inte koda sådana ärenden som enligt en första granskning bedömdes vara dataintrång i sociala medier och e-tjänster, och som därmed hade fått fel brottskod vid anmälningsupptagningen.[22] Varje ärende kodades utifrån den information som fanns tillgänglig. I de fall ärenden hade avskrivits direkt fanns oftast endast polisanmälan, men för de ärenden där en förundersökning hade inletts kodades även information från förundersökningen. Bland annat kodades

[21] Urvalet av ärenden som registrerades som ”Övrigt dataintrång” gjordes större än de övriga brottskoderna eftersom det var mer oklart vad denna brottskod skulle omfatta för typ av brottshändelser.

[22] En genomläsning av dessa ärenden visade att de brottshändelser som beskrevs var av samma typ som dem som hade registrerats korrekt, dvs. under brottskoden för dataintrång i sociala medier och e-tjänster.

- om anmälaren eller målsägaren är en privatperson eller juridisk person
- om juridisk person: företag, kommunala bolag/företag eller myndighet
- om privatperson: målsägarens kön och ålder
- eventuell relation eller kontakt mellan målsägaren och gärningsperson
- antal och typ av andra brottstyper som registrerats i ärendet.

Uttag från misstankeregistret

För att få information om hur ofta en skäligen misstänkt gärningsperson knutits till ett dataintrångsbrott samt för att kunna besvara frågan om vilka typer av dataintrång som leder till personuppklaring beställdes ett uttag från misstankeregistret. Detta uttag avser de brottsmisstankar[23] som registrerats mot personer som blivit skäligen misstänkta för de dataintrång som finns i urvalet av polisanmälningarna.

Tidpunkt för beslut

De åtals- respektive nedläggningsbeslut som finns i utdraget från misstankeregistret avser perioden fram till och med maj 2022. Detta innebär att det finns ett mindre antal ärenden med brottsmisstankar där det inte har fattats ett avslutande beslut vid tidpunkten för beställningen från misstankeregistret.

Datauttaget från Brås register över anmälda brott inkluderar information om det senaste beslutet för de polisanmälda dataintrången, det kan till exempel vara att brottet läggs ned eller att det inleds förundersökning. Då uttaget gjordes i september 2021 inkluderar studien information om det senaste beslutet som fanns vid denna tidpunkt.

Granskningens begränsningar

Granskningen ger en bild av de dataintrång som polisanmäls och hanteras av rättsväsendet. Samtidigt visar studier att en mycket liten andel privatpersoner (se t.ex. Domenie m.fl. 2013, van de Weijer m.fl. 2019) och företag (se t.ex. Svenskt Näringsliv 2021, Teknikföretagen 2019) väljer att polisanmäla när de utsätts för dataintrång. Vidare är det sannolikt att många dataintrång aldrig upptäcks, till exempel de som genomförs i syfte att spionera. Detta innebär begränsningar när det gäller möjligheten att utifrån de polisanmälda

[23] En brottsmisstanke kopplar ett brott till en misstänkt person. Flera personer kan vara misstänkta för samma brott, vilket innebär att ett brott kan ha flera brottsmisstankar knutna till sig.

dataintrången ge en heltäckande bild av dataintrångens omfattning och komplexitet. Samtidigt är det sannolikt att de polisanmälda dataintrången åtminstone i någon mån innehåller exempel på de vanligaste formerna av dataintrång.

De dataintrångshändelser som analyserats polisanmäldes under hösten 2020, då covid-19-pandemin rådde och det är därmed möjligt att det rådde speciella omständigheter under denna period som påverkat karaktären på de anmälda dataintrångsbrotten. Eventuella pandemieffekter har inte kunnat analyseras inom ramen för denna studie.

Intervjuer

Sammanlagt 30 personer har intervjuats, uppdelat på 19 enskilda intervjuer och tre gruppintervjuer. En stor del av intervjuerna genomfördes över videolänk eller telefon, för att följa Folkhälsomyndighetens rekommendationer till följd av pandemin. En intervjuguide utarbetades med frågor som anpassades efter intervjupersonernas yrkesroll och expertområde. Intervjuerna var semistrukturerade med övergripande frågeområden utifrån studiens syfte och frågeställningar. Intervjuguiderna gav även utrymme för följdfrågor.

Brå har intervjuat 18 polisanställda och sju åklagare för att få en förståelse för de problem och utmaningar som uppstår i arbetet med att utreda och lagföra olika former av dataintrång. Bräs intervjuer med polisen inkluderar främst polisanställda som arbetar med komplexa cyberbrott. Brå har intervjuat dels anställda vid Nationella operativa avdelningen (NOA), dels anställda vid Polismyndighetens nationella it-brottscentrum (SC3), NOA-underrättelsetjänst och J-CAT. Brå har även intervjuat polisanställda vid regionala it-brottscenter (RC3). Utöver de polisanställda som nämns ovan har intervjuer genomförts med lokalpolis samt polis som arbetar på avdelningen för särskilda utredningar (SU).

Alla åklagare som intervjuades är kontaktåklagare i det nationella nätverket för it-relaterad brottslighet. Polisutredningar av dataintrång av normalgraden är polisledda fram till dess att en skäligen misstänkt gärningsperson har knutits till brotten (eller till dess att en åklagare behöver kopplas in av annan anledning). Kontakter med relevanta intervjupersoner förmedlades av kontaktpersoner vid Polismyndigheten respektive Åklagarmyndigheten.

Representanter från andra samhällssektorer

För att få en ökad förståelse för de dataintrång som inte anmäls och för det brottsförebyggande arbetet i samhället intervjuades samhällsaktörer som bevakar olika aspekter av dataintrångsbrottsligheten som en del i deras arbete. Sammanlagt fem intervjuer har genomförts med experter inom it- och cybersäkerhet, från både privat och offentlig sektor.

Bearbetning av intervjumaterialet

Samtliga intervjuer utom två spelades in och transkriberades. Vid de två intervjuer som inte spelades in togs anteckningar. Intervjuerna pågick i regel en till två timmar, även om det förekom enstaka längre intervjuer.

De transkriberade intervjuerna kodades och strukturerades utifrån ett antal övergripande teman relaterade till studiens frågeställningar och analyserades därefter. Citat från intervjuerna återges i resultatredovisningen. Citaten har redigerats något för att göra dem mer lättlästa, men också för att omöjliggöra identifiering av enskilda individer.

Seminarier med experter inom området

Som ett led i studien har Brå vid två tillfällen bjudit in experter till seminarier där utvecklingsområden och brottsförebyggande frågor diskuterades. Det ena seminariet genomfördes med aktörer inom rättsväsendet. Fokus för mötet var att diskutera de utredningssvårigheter och utmaningar som identifierats utifrån intervjuerna och för att vidare diskutera utvecklingsområden för utredningsarbetet. Det andra seminariet genomfördes med experter som arbetar brottsförebyggande mot it-brott. Fokus vid detta möte var att diskutera mörkertal kopplat till den låga anmälningsbenägenheten och säkerhetsåtgärder för att förebygga eller minska antalet dataintrång i samhället.

De polisanmälda dataintrångens karaktär

Detta kapitel syftar till att ge en beskrivning av karaktären på de dataintrång som polisanmäldes från juli till och med december 2020. Först ges en översiktlig beskrivning av dataintrång enligt kriminalstatistiken, vilket följs av en redogörelse för dataintrångsbrotten separat för de fem brottskoder som används vid registrering av anmälda dataintrång.

Polisanmälda dataintrång i kriminalstatistiken

Under 2020 polisanmäldes närmare 9 000 dataintrång, vilket är ungefär lika många som polisanmäldes under 2018 och 2019. Däremot ökade antalet dataintrång under 2021 till drygt 11 500 anmälda brott.

Som beskrivits i inledningen infördes fem nya brottskoder för dataintrång i juli 2020. Under perioden juli till december det året polisanmäldes drygt 4 000 dataintrång. Tabell 2 visar att antalet dataintrång som anmäldes under perioden varierar stort mellan de olika brottskoderna. Flest anmälningar gjordes inom brottskoderna *Dataintrång i sociala medier eller e-tjänster* och *Övrigt dataintrång*, medan betydligt färre *Dataintrång genom överbelastningsattack* respektive *Dataintrång med hjälp av skadlig kod i utpressningssyfte* anmäldes.

Tabell 2. Antal polisanmälda dataintrång, juli–december 2020, fördelat på brottskoder.

Brottskoder	Antal anmälda brott
Dataintrång genom överbelastningsattack (9464)	27
Dataintrång med hjälp av skadlig kod i utpressningssyfte (9465)	164
Dataintrång genom olovliga registerslagningar (9466)	615
Dataintrång i sociala medier eller e-tjänster (9467)	1 818
Övrigt dataintrång (9468)	1 719
Totalt	4 048

Källa: Kriminalstatistiken.

De granskade dataintrångsärendena

Denna studie analyserar dataintrång på ärendenivå. Ett ärende motsvarar en upprättad polisanmälan i de allra flesta fall, men en polisanmälan, och därmed ett ärende, kan innehålla både flera brott av samma typ och flera olika typer av brott. Det beror på att den som anmäler kan ha blivit utsatt

för flera dataintrångsbrott innan den gör anmälan eller kan exempelvis ha blivit utsatt för ett dataintrång och samtidigt hotats eller utsatts för ett bedrägeriförsök.

Som nämnts i metodkapitlet har Brå gjort ett uttag på sammanlagt 641 ärenden, som innehåller åtminstone ett dataintrångsbrott, för att närmare studera de anmälda dataintrången. För dessa ärenden har tillhörande polisanmälningar och i förekommande fall även förundersökningar granskats. En utförligare resultatredovisning finns i bilaga 1.

Dataintrång genom överbelastningsattack

Som nämnts i inledningen innebär en överbelastningsattack ett angrepp där gärningspersonen, i syfte att störa ett system eller dess tillgänglighet, riktar digital trafik mot exempelvis den utsattes nätverk, dator eller server, så att enheten störs eller slås ut. Mellan juli och december 2020 registrerades totalt 27 polisanmälda dataintrång genom överbelastningsattack, som samtliga har granskats. I 8 av dessa ärenden har även andra brottstyper registrerats, framför allt utpressning eller bedrägeri (tabell 3). Alla ärenden rubricerades som fullbordade dataintrång utom ett, som rubricerades som försök till dataintrång.

Tabell 3. Brottstyper som förekommer i överbelastningsärenden (utöver själva dataintrånget). En brottstyp räknas en gång per ärende.

Andra brottstyper i ärendena	Antal ärenden
Utpressning	4
Bedrägeri	3
Övriga brottstyper[24]	1

Drygt hälften av överbelastningsattackerna har riktats mot företag eller kommunala verksamheter

I drygt hälften av ärendena om dataintrång genom överbelastningsattack är målsägaren en juridisk person, och i nästan alla dessa fall är målsägaren ett privat företag eller en kommunal verksamhet.

Flera av dessa polisanmälningar beskriver att företag blivit utsatta för utpressning, genom att gärningspersonen först mejlat företaget och hotat med att en överbelastningsattack skulle genomföras om företaget inte betalar en

[24] Kategorin *Övriga brottstyper* samlar brott som förekommer enskilda gånger inom den specifika brottskategorin för dataintrång.

viss summa i bitcoin. I de flesta fall framgår att företagen senare också blivit utsatta för överbelastningsattacker, som slagit ut företagens webbplatser eller servrar.

Ingen av de anmälningar som avser överbelastningsattacker mot kommunala verksamheter beskriver att det skett någon form av utpressning. I dessa fall är det oftast kommunförvaltningen som blivit utsatt för en attack som antingen gjort deras webbplats otillgänglig för allmänheten eller stört förvaltningens nätverk så att kommunanställda inte kunde komma åt internet. Det finns också enstaka anmälningar från skolor, där elever har angett sig själva till skolpersonal efter att skolornas lärarplattformer har utsatts för överbelastningsattacker.

Överbelastningsattacker mot privatpersoner är ofta riktade mot den utsattes router

Anmälningar om överbelastningsattacker mot privatpersoner beskriver ofta att en okänd gärningsperson, ibland upprepade gånger över en längre period, riktat attacker mot målsägarens router, vilket bland annat gjort att målsägaren inte kan komma åt internet. I några fall har routern slutat fungera helt.

Det finns också några anmälningar som beskriver ett tillvägagångssätt som inte liknar en så kallad överbelastningsattack, utan som i stället handlar om att gärningspersonen olovligen fått tillgång till målsägarens mobiltelefonkonto och därefter använt abonnemanget för att skicka ett stort antal sms till framför allt utländska telefonnummer, vilket också lett till att målsägaren fått ta emot ibland flera hundra inkommande sms under en kort period. Enstaka anmälningar av den här typen har också rubricerats som bedrägeri, då det framgår av vissa sms att någon försökt göra onlineköp med målsägarens mobilabonnemang.[25]

Därtill förekommer också anmälningar där det inte framgår att det skett någon form av överbelastningsattack utan där det snarare handlar om att någon berett sig tillgång till målsägarens dator eller mobil och raderat allt innehåll eller gjort den obrukbar.

---

[25] Anmälningar av den här typen har också registrerats som *dataintrång genom skadlig kod i utpressningssyfte* och som *övrigt dataintrång*.

Dataintrång med hjälp av skadlig kod i utpressningssyfte

Brottskoden kännetecknas av att brottsoffret blir ombedd att betala en lösensumma för att få tillgång till filer som gärningspersonen gjort otillgängliga, ofta genom att använda en typ av skadlig kod som krypterat filerna. Andra namn för de typer av angrepp som samlas under brottskoden skadlig kod i utpressningssyfte är ransomware, gisslanprogram eller utpressningsvirus (Brå 2022). Under perioden juli–december 2020 registrerades totalt 164 polisanmälda *dataintrångsbrott med hjälp av skadlig kod i utpressningssyfte,* fördelat på 155 ärenden. Samtliga dessa ärenden har granskats.

Det förekommer andra brottstyper än dataintrång med hjälp av skadlig kod och dessa utgörs nästan uteslutande av *utpressningsbrott* (se tabell 4). Eftersom polisen uppmanas att även registrera utpressningsbrottet som förekommer tillsammans med denna typ av dataintrång, är det förväntat. Sex av ärendena är rubricerade som försök till dataintrång, resterande som fullbordade dataintrång.

Tabell 4. Brottstyper som förekommer i ärenden med skadlig kod i utpressningssyfte (utöver själva dataintrånget). En brottstyp räknas en gång per ärende.

Andra brottstyper i ärendena	Antal ärenden
Utpressning	30
Övriga brottstyper	5

Målsägare en juridisk person i en stor del av ärendena om dataintrång genom skadlig kod

När det gäller dataintrång genom skadlig kod är det betydligt vanligare att målsägaren är en juridisk person, jämfört med en privatperson, och det är framför allt företag som blivit utsatta. Två tredjedelar av dessa brott har inte anmälts av det utsatta företaget utan anmälningarna har upprättats efter att Europol genom J-CAT[26] informerat den svenska polisen om att den ryskbaserade gruppen REvil (Ransomware Evil) [27] hade lyckats infektera ett flertal svenska företag med skadlig kod i syfte att kunna utöva utpressning.

[26] Som nämndes i inledningen är J-CAT (Joint Cybercrime Action Taskforce) en polisstyrka vid Europols cyberbrottscenter, EC3.

[27] REvil utförde exempelvis en utpressningsattack i juli 2021 mot mjukvarubolaget Kaseya, som förser tiotusentals kunder över hela världen med kassasystem. En av kunderna var den svenska matvarubutiken COOP, vars system spärrades med krav om betalning.

Utöver att upprätta anmälningarna hade polisen sedan också kontaktat och informerat de berörda företagen.

I alla dessa anmälningar (förutom en) har polisen inte registrerat ett utpressningsbrott i anmälan, då den information de fått från J-Cat avser att företagen infekterats av den skadliga koden, inte att de blivit utsatta för utpressning. Av polisens dokumentation framgår att företagen själva inte alltid har märkt att deras system blivit infekterat, vilket också tyder på att de fått information från polisen innan gärningspersonerna aktiverat den skadliga koden och utsatt företagen för utpressning.

Utöver dessa anmälningar som upprättades utifrån information från J-Cat finns ytterligare 36 anmälningar om dataintrång med hjälp av skadlig kod där en juridisk person blivit utsatt. De flesta av dessa målsägare är också företag, men det förekommer också enstaka anmälningar om brott mot verksamheter i den offentliga sektorn. I dessa fall har det utsatta företagets eller verksamhetens servrar eller datorer blivit infekterade med skadlig kod, som sedan har krypterat delar av eller hela innehållet så att målsägarna inte kunde komma åt sina filer. Ett meddelande med krav om betalning för att låsa upp krypteringen har i de flesta fall lämnats på datorn eller servern, tillsammans med instruktioner om att kontakta gärningspersonen, antingen via mejl eller genom att ladda ner ett program från en darknetserver.

I några få fall framgår att företaget har betalat lösensumman för att återfå tillgång till de krypterade filerna. I ett fall framgår av det granskade materialet att företaget tillsammans med en intern eller extern it-konsult kommit fram till att det är mindre kostsamt för företaget att betala gärningspersonen än att återställa sina system på egen hand.

Bland de brott mot juridiska personer som registrerats som dataintrång med hjälp av skadlig kod finns också några stycken där en okänd gärningsperson använt dataintrång för att komma åt känslig information, exempelvis kund- eller medlemslistor, och därefter krävt pengar för att inte offentliggöra uppgifterna. Det finns också enstaka anmälningar som registrerats som skadlig kod men som i stället avser utpressning kopplad till hot om överbelastningsattacker.

Privatpersoner utsätts oftast för utpressningsmejl kopplade till påstådda dataintrång

I de anmälningar om dataintrång genom skadlig kod där målsägaren är en privatperson är det sällan som det framgår att målsägarens dator blivit utsatt för en skadlig kod som krypterat datafilerna, även om detta förekommer i några ärenden, och det finns enstaka fall som avser privatpersoner där anmälan upprättats av polisen efter att ha fått information från J-Cat (som ovan).

Det vanligaste tillvägagångssättet i anmälningarna om skadlig kod mot privatpersoner är att målsägaren fått ett utpressningsmejl från en okänd gärningsperson där det påstås att gärningspersonen tagit sig in på målsägarens server eller dator och installerat skadlig kod för att kunna bevaka och filma både målsägaren och målsägarens aktivitet på nätet. Typiskt sett innehåller mejlen också ett hot om att gärningspersonen kommer sprida filmer på målsägaren när denna tittat på porrsidor, om hen inte betalar, oftast i bitcoin. I de allra flesta av dessa anmälningar finns ingen information om att målsägarens dator faktiskt blivit infekterad med någon form av skadlig kod, och i enstaka fall framgår att målsägaren inte har en webbkamera och har därför insett att det måste vara en bluff.

Bland anmälningarna om skadlig kod i utpressningssyfte mot privatpersoner förkommer även ett antal anmälningar som handlar om en annan typ av utpressning, där en okänd gärningsperson fått tillgång till målsägarens mejl-, spel- eller sociala mediekonto, bytt lösenord och krävt målsägaren på pengar för att återfå tillgång till kontot.

Dataintrång genom olovlig registerslagning

Olovlig registerslagning inkluderar dataintrång där gärningspersonen olovligen berett sig tillgång till information i register hen har tillgång till inom ramen för sitt arbete. Det kan till exempel handla om sjukvårdspersonal som kollar upp patienter, eller polisanställda som söker på ärenden de själva inte handlägger (Brå 2022). Under perioden juli–december 2020 registrerades totalt 615 brott som *dataintrång genom olovlig registerslagning*. Dessa brott har studerats närmare med hjälp av ett urval av 99 ärenden.

En femtedel av dessa ärenden inkluderade några enstaka extra dataintrång genom olovlig registerslagning, men två ärenden innehåller runt 60 olovliga registerslagningar och ett ärende innehåller över 250 olovliga

registerslagningar. Det förekommer även andra brottstyper, oftast *brott mot tystnadsplikt* eller *tjänstefel* (tabell 5).

I ärenden om dataintrång genom olovlig registerslagning är det vanligt att den person som anmälaren misstänker för intrånget har gjort dataintrånget på sin arbetsplats, exempelvis inom polisen eller sjukvården. Det kan även handla om slagningar inom till exempel kriminalvården eller socialtjänsten.

Tabell 5. Brottstyper som förekommer i ärenden om dataintrång genom olovlig registerslagning (utöver själva dataintrånget). En brottstyp räknas en gång per ärende.

Andra brottstyper i ärendena	Antal ärenden
Tjänstefel/brott mot tystnadsplikt	16
Övriga brottstyper	6

En tredjedel av de olovliga registerslagningarna har begåtts inom polisen

Som nämnts i inledningskapitlet utreds olovliga registerslagningar som gjorts av en anställd inom polisen av en särskild avdelning, avdelningen för särskilda utredningar (SU). Avdelningen för särskilda utredningar är en fristående och oberoende avdelning inom Polismyndigheten som utreder misstänkta brott som bland annat polisanställda, polisstudenter, domare och åklagare kan ha gjort sig skyldiga till. Av samtliga granskade ärenden om dataintrång genom olovlig registerslagning är närmare en tredjedel av den här typen. Några få anmälningar om dataintrångsbrott genom olovlig registerslagning av polisanställd avser ett större antal brott (upp till ett 60-tal).

Framför allt privatpersoner som är målsägare i SU-ärendena

Informationen i förundersökningsmaterialet i de ärenden som levererats till Brå av SU är många gånger maskerad, vilket innebär att det är svårt att utläsa olika aspekter av brottshändelsen. Ett exempel på den här typen av ärenden är dock att polisanställda misstänks dels för olovliga registerslagningar, dels för att sedan ha spridit informationen vidare till tredje part. Ett annat exempel är att polisanställda misstänks ha gjort slagningar på grannar eller bekanta. Granskningen visar att det framför allt är privatpersoner som är målsägare i de dataintrång genom olovlig registerslagning som utreds av SU.

Olovliga registerlagningarna inom sjukvården

I en stor del av de övriga granskade ärendena om olovliga registerslagningar arbetade den misstänkta gärningspersonen inom vården. Det handlar exempelvis om sjuksköterskor och i något enstaka fall om någon inom

tandläkarvården, som har gjort slagningar på målsägaren i journaler som de har tillgång till i sitt arbete.

Anmälaren känner ofta den som misstänks för brottet

Dataintrång genom olovlig registerslagning skiljer sig från de övriga typerna av dataintrång eftersom det vanliga är att anmälaren eller målsägaren har en uppfattning om vem gärningspersonen är. I en majoritet av de kodade ärendena framkommer att målsägaren eller anmälaren har uppgett information om en misstänkt person. I nästan en femtedel av ärendena har den misstänkte en relation till målsägaren, eller har haft det, eller ingår i målsägarens familj eller släkt, medan det i en tredjedel av ärendena framkommer att målsägaren och den misstänkte är bekanta eller ytligt bekanta.

Dataintrång i sociala medier och e-tjänster

Denna brottskod innebär att gärningspersonen utan tillstånd bereder sig tillgång till en annan persons konto på sociala medier eller i en e-tjänst. Sociala medier syftar på digitala tjänster eller plattformar där människor kommunicerar eller uttrycker sig (såsom Facebook eller Instagram), medan e-tjänster är digitala tjänster där man genom att logga in kan utföra olika handlingar som att betala, kolla på tv eller betala räkningar (till exempel e-post, bank-id eller Internetbanken) (Brå 2022). Under perioden juli–december 2020 registrerades totalt 1 818 anmälda brott som *dataintrång i sociala medier och e-tjänster*. Följande redovisning bygger på ett urval av 120 ärenden.

Nästan hälften av dessa anmälningar avser endast dataintrång i sociala medier och e-tjänster. I de övriga har även någon annan brottskod registrerats (tabell 6), där den vanligaste är *olovlig identitetsanvändning*.

Tabell 6. Brottstyper som förekommer i ärenden om dataintrång i sociala medier och e-tjänster (utöver själva dataintrånget). En brottstyp räknas en gång per ärende.

Andra brottstyper i ärendena	Antal ärenden
Olovlig identitetsanvändning	27
Bedrägeri	20
Olaga hot	5
Ofredande	4
Utpressning	4
Stöld/rån	3
Olaga integritetstrång	3
Övriga brottstyper	12

Dataintrång i sociala medier och e-tjänster anmäls sällan av juridiska personer

I de allra flesta anmälningar som avser dataintrång i sociala medier och e-tjänster är det en privatperson som blivit utsatt för det anmälda brottet. I de få fall där målsägaren är en juridisk person handlar anmälan om att gärningspersonen berett sig tillgång till ett företags Facebook- eller mejlkonto och bytt lösenord, så att företaget inte kan komma åt sitt konto, dock utan att det framgår att företaget också blivit utsatt för utpressning. I ett fall framgår däremot att gärningspersonen använt kontot för att lägga ut Facebook-annonser, som det utsatta företaget sedan fakturerats för.

Privatpersoners Facebook- och/eller Messengerkonton utsatta för dataintrång i större utsträckning än andra sociala medier eller e-tjänster

I nästan hälften av de anmälningar som avser privatpersoner är det vanligt att det är målsägarens Facebook- eller Messengerkonto som blivit utsatt, men det är också vanligt med intrång i exempelvis mejl-, snapchat-, spel- och Instagramkonton. I enstaka fall beskrivs intrång i ett streamingtjänst-, bank- eller e-baykonto tillhörande målsägaren. I 30 procent av anmälningarna har målsägaren uppgett att intrång skett i flera olika sociala medier eller e-tjänster. I drygt hälften av dessa ärenden har målsägaren en uppfattning[28] om vem gärningspersonen kan vara och i resterande ärenden är gärningspersonen helt okänd.

Kapade konton har använts till bland annat bedrägerier och nätfiske samt i utpressningssyfte

Det finns en relativt stor variation bland anmälningarna när det gäller syftet med intrånget i de utsattas sociala medie- och e-tjänstkonton. I en del fall framgår bara att målsägaren blivit utelåst från sitt konto, men i de flesta fall beskrivs att kontot, och därmed även målsägarens identitet, sedan har använts av gärningspersonen på olika sätt.

I en del anmälningar framgår att gärningspersonen använt målsägarens konto till olika typer av bedrägerier. I flera anmälningar har exempelvis kontot använts för att skicka meddelanden till målsägarens vänner, där de ombes swisha pengar till ett telefonnummer som inte tillhör målsägaren, medan i andra fall har konton kopplade till Facebook eller till försäljnings-, mobil- och speltjänster använts för att genomföra onlineköp i målsägarens namn, eller för att bjuda ut varor till försäljning, som sedan inte levererats. I enstaka

[28] För en del av dessa ärenden har målsägaren endast kännedom om vem gärningspersonen är genom att det exempelvis finns en mejladress.

fall har lån tagits i målsägarens namn eller överföringar gjorts från målsägarens bankkonto. I dessa typer av ärenden har polisen ibland, men långt ifrån alltid, även registrerat ett olovligt identitetsintrång i polisanmälan.

Ett annan relativt vanlig typ av anmälan avser fall där målsägarens konto använts till nätfiske.[29] Det vanligaste tillvägagångssättet i de granskade polisanmälningarna är att en okänd gärningsperson använt målsägarens konto för att skicka meddelanden till vänner eller kontakter, med en uppmaning om att delta i en onlinetävling. Det framgår också i flera fall att målsägaren först själv hade fått ett liknande meddelande från en av sina kontakter (som sannolikt också varit utsatt för samma typ av dataintrång). I de fall det framgår att någon har deltagit i en tävling av den här typen beskrivs att målsägaren hade vunnit pengar i tävlingen och sedan tillfrågats om att lämna ifrån sig konto- eller kortuppgifter med förespegling om att dessa uppgifter behövdes för att föra över vinsten.[30] Det finns också beskrivningar i materialet där målsägarens vänner blivit lurade till att tro att målsägaren själv har kontaktat dem och frågat om deras kontouppgifter eller telefonnummer med mera.

I en del anmälningar beskrivs att en okänd gärningsperson först gjort intrång i målsägarens konto på exempelvis Instagram eller Snapchat, låst ut målsägaren, och därefter tagit kontakt med målsägaren i utpressningssyfte, och hotat att spridda nakenbilder som funnits på kontot till målsägarens familj och vänner, om målsägaren inte skickar antingen pengar eller fler nakenbilder.

En del dataintrång är av mer personlig karaktär

I en femtedel av anmälningarna framstår det som att dataintrånget har en mer personlig karaktär, där motivet snarare har varit mobbning, förnedring eller att utöva kontroll över målsägaren. Ibland har gärningspersonen publicerat provocerande inlägg på målsägarens konto i form av text eller bilder, som målsägaren sedan inte har möjlighet att ta bort, eller använt kontot för att exempelvis hota kontakter till målsägaren. Om det förekommer någon annan brottstyp i dessa ärenden handlar det bland annat om olaga hot, ofredande och ärekränkningsbrott snarare än om olovlig

---

[29] Som nämnts i inledningen används nätfiske som en gemensam beteckning för en rad olika metoder som används för att lura människor till att lämna ifrån sig känslig information. Se till exempel Brå 2016b.

[30] Att påstå att någon vunnit en tävling eller lotteri för att lura personen att lämna ut sina kontouppgifter är en väletablerad form av nätfiske (se t.ex. Ojha och Tak 2012, Brå 2016b).

identitetsanvändning eller bedrägeri. I dessa anmälningar är det också mycket vanligare, jämfört med de övriga typerna av dataintrång, att målsägaren redan vid tiden för anmälan har en stark misstanke om vem gärningspersonen är. I hälften av ärendena är det en partner eller tidigare partner som målsägaren misstänker.

Övrigt dataintrång

Brottskoden Övrigt dataintrång ska ges till alla de dataintrång som regleras i brottsbalken, men som inte faller in under beskrivningarna av de fyra brottskoder för dataintrång som beskrivits ovan (det vill säga överbelastningsattacker, skadlig kod i utpressningssyfte, olovlig registerslagning eller intrång i sociala medier eller e-tjänster (Brå 2022)). Under perioden juli–december 2020 registrerades totalt 1 719 brott som *övrigt dataintrång*. Ett urval om 240 ärenden har gjorts för den aktuella granskningen. [31] Drygt fyra av tio ärenden inkluderar minst en annan brottstyp än dataintrånget. De övriga brottstyper som förekommer i dessa ärenden är mycket fler än vid de andra typerna av dataintrång, men vanligast är någon form av bedrägeri och näst vanligast är olovlig identitetsanvändning (tabell 7).

Tabell 7. Brottstyper som förekommer i ärenden om övrigt dataintrång (utöver själva dataintrånget). En brottstyp räknas en gång per ärende.

Andra brottstyper i ärendena	Antal ärenden
Bedrägeri	62
Olovlig identitetsanvändning	16
Ärekränkning: förtal & förolämpning	7
Olaga hot	6
Olaga integritetsintrång	5
Ofredande	3
Olovlig avlyssning m.m.	3
Misshandel	3
Utpressning	2
Övriga brottstyper	16

Av de granskade ärendena består hälften av sådana brott som Brå bedömer handlar om dataintrång i sociala medier och e-tjänster, och som borde ha registrerats av polisen som sådana. Dessa liknar de olika typer av

[31] Urvalet av ärenden som registrerades som ”Övrigt dataintrång” gjordes större än de övriga brottskoderna eftersom det var mer oklart vad denna brottskod skulle omfatta för typ av brottshändelser.

brottshändelser som beskrivits ovan i avsnittet om dataintrång i sociala medier och e-tjänster. Det kan till exempel handla om målsägare vars mejl- eller sociala mediekonton använts för att skicka meddelanden till deras kontakter, och som ber mottagaren att skicka pengar, och målsägare vars kundkonton på exempelvis speltjänster eller butikskedjor använts av okända gärningspersoner för att beställa tjänster eller varor, i det senare fallet efter att ha bytt ut leveransadressen. Det finns också anmälningar där gärningspersonen berett sig tillgång till målsägarens sociala mediekonto och läst privata meddelanden eller gjort provocerande inlägg.

Det är även vanligt med så kallade VD-bedrägerier.[32] VD-bedrägerier handlar om att gärningspersonen först får tillgång till ett mejlkonto som tillhör en nyckelperson inom ett företag eller organisation, exempelvis VD:n, och sedan använder detta konto för att mejla andra inom organisationen med instruktioner om att betala en faktura eller föra över pengar till ett externt bankkonto. Samtliga ärenden som Brå bedömt vara dataintrång i sociala medier och e-tjänster har exkluderats från den fortsatta resultatredovisningen i detta avsnitt.

Privatpersoner utsatta för övrigt dataintrång

I fyra av fem av de granskade ärendena om Övrigt dataintrång är målsägaren en privatperson. Vanligt är fall där målsägaren beskriver att en okänd person gjort intrång i målsägarens dator eller mobil, ofta utan att målsägaren har förstått syftet med intrånget. Som tecken på att det skett ett intrång menar målsägare exempelvis att bilder eller filer har försvunnit från datorn eller mobilen, men det finns även fall där någon har börjat fjärrstyra enheten eller där gärningspersonen ändrat målsägarens bakgrundsbild. I vissa ärenden av den här typen framgår att målsägaren har en misstanke om vem gärningspersonen är, till exempel för att denna person sedan spridit bilder som bara funnits på målsägarens telefon eller skärmdumpar av målsägarens textkonversationer.

Företag utsatta för bedrägerier och informationsstöld

I en femtedel av ärendena är målsägaren en juridisk person och dessa består främst av företag. Exempelvis finns anmälningar där gärningspersonen skickat fakturor till företagskunder från en påhittad mejladress som är tillräckligt lik företagets för att lura mottagarna, eller skickat ett mejl från en

[32] Från engelskans CEO Fraud, också kallad business e-mail compromise (BEC)-bedrägerier, se till exempel Al-Musib m.fl. (2021). Se även MSB och CERT-SE 2019.

sådan mejladress med uppgift om att företaget bytt bankkonto och att kunderna framöver skulle skicka betalningar till det nya kontot.

Det finns också flera anmälningar som avser dataintrång hos företag eller ideella organisationer, som beskriver att företaget eller organisationen vet eller misstänker att uppgifter om kunder eller medlemmar, eller annan känslig information, har stulits. I enstaka anmälningar beskrivs också fall där en anställd eller konsult olovligen bytt lösenord till olika system, eller fört över pengar till ett eget konto.

De utsatta juridiska och privatpersonerna

Genomgången av det insamlade materialet visar att i stort sett vem som helst kan drabbas av dataintrång. De företag som drabbas av dataintrång varierar från små firmor och egenföretagare till stora företag, som exempelvis har beskrivit att förlorad åtkomst till sina servrar som resultat av skadlig kod kan kosta dem miljontals kronor om dagen. Som framgått ovan finns också anmälningar om brott mot verksamheter inom olika delar av de offentliga och ideella sektorerna.

De privatpersoner som utsätts för dataintrång utgörs av män och kvinnor i många olika åldersgrupper, från skolbarn till personer i 80-årsåldern. Samtidigt förekommer vissa köns- och åldersskillnader i materialet mellan de olika typerna av dataintrångsbrott. Kvinnor förekommer som målsägare oftare än män i anmälningarna om dataintrång i sociala medier och e-tjänster samt även i de anmälningar som avser olovliga registerslagningar som inte skett inom polisen.[33] Könsfördelningen är relativt jämn bland målsägarna i de anmälningar som registrerats som övrigt dataintrång (53 kvinnor och 41 män).

I samtliga typer av dataintrångsanmälningar finns både målsägare som är barn och målsägare från olika åldersgrupper av vuxna. Det finns ingen åldersgrupp som verkar vara särskilt utsatt för en viss typ av dataintrång, men jämfört med de övriga typer av dataintrång som studerats är det vanligare att målsägaren är under 18 år i de anmälningar som avser den undergrupp av dataintrång i sociala medier där det framgår att intrånget

[33] Som nämnts saknas mycket information om de utsatta personerna kopplade till de anmälningar som utretts av polisens avdelning för särskilda utredningar (SU), eftersom denna information hade maskerats i det material som skickades till Brå. I de fall kön på målsägaren framgår är det något fler män än kvinnor som varit utsatta. Det granskade materialet från SU innehåller ingen information om målsägarnas ålder.

handlat om att mobba, förnedra eller utöva kontroll över målsägaren. Det är framför allt kvinnor som anmäler dataintrång i sociala medier som är av mer personlig karaktär. Det är även något fler kvinnor än män som anmäler dataintrång i sociala medier och e-tjänster som är kopplade till bedrägeribrott.

Som nämnts är det också vanligare i anmälningarna om brott av mer personlig karaktär än vid de övriga typerna av dataintrång (med undantag för olovlig registerlagning) att anmälaren har en misstanke om vem gärningspersonen är redan vid anmälningstillfället. För de dataintrång i sociala medier som är av mer personlig karaktär där målsägaren har en misstanke om vem som ligger bakom brottet är det betydligt vanligare att den kvinnliga målsägaren misstänker en man som hon är eller har varit tillsammans med, än att en man misstänker en nuvarande eller tidigare fru, sambo eller flickvän.

De personuppklarade och nedlagda dataintrången

I denna del av rapporten beskrivs vilka typer av dataintrång som leder till personuppklaring och vilka som inte gör det. Det görs genom att redovisa dels om rättsväsendet lyckats knyta en misstänkt gärningsperson till brottet, dels om det finns ett uppklaringsbeslut i ärendet. Den information som redovisas om misstänkta avser misstänkta personer som förekom i ärendena fram till och med maj 2022.

Att ett brott är personuppklarat innebär att en åklagare fattat ett lagföringsbeslut om att väcka åtal, utfärda strafföreläggande eller meddela åtalsunderlåtelse i ärendet (Brå 2018). Så kallade offerbrott, där det finns en interaktion mellan gärningspersonen och offret, innebär att det oftare finns information om vem den misstänkte kan vara, eller åtminstone spår att jobba vidare med för att kunna klara upp brottet (ibid.). Vid brott med låg eller ingen interaktion mellan gärningsperson och offer finns däremot mer sällan information om en möjlig misstänkt person, vilket också försvårar personuppklaring. Dataintrång är inte bundna till en specifik brottsplats utan äger rum i en digital miljö, där offret och gärningspersonen oftast har en begränsad interaktion med varandra. Personuppklaringen kan därför förväntas vara låg för denna brottstyp.

Tabell 8 redogör först för antal och andel ärenden inom respektive brottskod där åklagare har fattat ett personuppklaringsbeslut för minst ett dataintrång, antingen genom att väcka åtal eller att utfärda ett strafföreläggande. Därefter redogörs för de ärenden som saknar personuppklaringsbeslut för dataintrång, antingen genom att ärenden direktavskrivs eller att förundersökningen läggs ned. Sist i tabellen redogörs för de ärenden där det saknas ett avslutande beslut.

Tabell 8. Antal och andel ärenden inom respektive brottskod som resulterat i personuppklarade dataintrång eller nedlagda dataintrång samt antal och andel där det saknas ett avslutande beslut.

	Överbelastning		Skadlig kod		Registerslag.		Sociala med.		Övrigt		Totalt
	Antal	Andel	Antal	Andel	Antal	Andel	Antal	Andel	Antal	Andel	Antal
Personuppklarade ärenden	**1**	**4 %**	**0**	**0 %**	**24**	**24 %**	**0**	**0 %**	**2**	**1 %**	**27**
… varav åtal väcks	1	4 %	0	0 %	19	19 %	0	0 %	2	1 %	22
… varav strafföreläggande	0	0 %	0	0 %	5	5 %	0	0 %	0	0 %	5
Avskrivning/nedläggning	**23**	**85 %**	**125**	**81 %**	**62**	**63 %**	**119**	**99 %**	**232**	**96 %**	**561**
… varav direktavskrivning	10	37 %	49	32 %	20	20 %	76	63 %	167	70 %	322
… varav FU läggs ned	13	48 %	76	49 %	42	42 %	43	36 %	65	27 %	239
Saknas avslutande beslut	**3**	**11 %**	**30**	**19 %**	**13**	**13 %**	**1**	**1 %**	**6**	**3 %**	**53**
Totalt	**27**	**100 %**	**155**	**100 %**	**99**	**100 %**	**120**	**100 %**	**240**	**100 %**	**641**

Personuppklarade dataintrång

Det är ovanligt att det förekommer personuppklaringsbeslut för dataintrång i de granskade ärendena.[34] Både antalet och andelen ärenden som lett till personuppklaring är högst för olovliga registerslagningar, där ett beslut om att väcka åtal eller utfärda ett strafföreläggande registrerats vid 24 procent av samtliga olovliga registerslagningar. Som beskrevs i förra kapitlet sker dessa dataintrång oftast på den misstänktes arbetsplats, där slagningarna även loggas i det system där slagningarna gjorts. Det gör det naturligtvis enklare att identifiera vem som gjort dataintrånget, men även att säkerställa bevisning. Att personuppklaringen är högre i dessa ärenden kan därmed ses som väntat.

När det gäller de övriga typerna av dataintrång har bara ett av ärendena om överbelastningsattacker personuppklarats, och två av ärendena om övrigt dataintrång. Inget av ärendena om dataintrång med hjälp av skadlig kod eller dataintrång i sociala medier och e-tjänster hade personuppklarats fram till maj 2022.

[34] Enbart fyra ärenden innehåller personuppklarade brottsmisstankar gällande andra brott än dataintrång.

Att väcka åtal det vanligaste personuppklaringsbeslutet

De flesta personuppklaringsbeslut avser beslut att väcka åtal. De övriga personuppklarade ärendena, som samtliga avser olovlig registerslagning, personuppklarades genom ett beslut om strafföreläggande.

Könsfördelningen är jämn bland de gärningspersoner mot vilka åtal väckts eller som meddelats ett strafföreläggande (15 kvinnor, 12 män), och åldersmässigt varierar de från femtonåringar till personer i 60-årsåldern.

Direktavskrivna och nedlagda dataintrångsärenden

Som framgått ovan är det väldigt få av de granskade dataintrångsärendena som lett till personuppklaring. De flesta ärenden har avslutats antingen genom beslut om att en förundersökning inte ska inledas (direktavskrivning), eller genom beslut att lägga ned förundersökningen (nedläggning).

Många dataintrångsärenden direktavskrivs

Tabell 8 visar att det är vanligare med direktavskrivningar vid ärenden om dataintrång i sociala medier och e-tjänster (63 procent av samtliga) respektive ärenden om övrigt dataintrång (70 procent). Direktavskrivning förekommer mindre ofta vid överbelastningsattacker respektive skadlig kod (37 respektive 32 procent av ärendena). Andelen direktavskrivningar är lägst för dataintrång genom olovlig registerslagning (20 procent).

Anledning till direktavskrivning är oftast att brottet inte går att utreda

Enligt 23 kap. rättegångsbalken (1942:740) ska en förundersökning inledas om det finns skäl att anta att ett brott som hör under allmänt åtal har begåtts. En förundersökning behöver dock inte inledas om det är uppenbart att brottet inte går att utreda (till exempel om spaningsuppslag saknas), eller om kostnaderna för utredningen inte står i rimligt förhållande till sakens betydelse och brottets straffvärde understiger fängelse i tre månader.

I en stor majoritet av de direktavskrivna dataintrångsärendena (90 procent) framgår att skälet till direktavskrivningen är att brottet *uppenbart inte går att utreda*. Beslutskoderna om direktavskrivning omfattar inte någon detaljerad information om varför ärendena inte går att utreda, men ibland framgår ytterligare motiveringar av polisens dokumentation. Det handlar framför allt om att spaningsuppslag saknas. I enstaka ärenden framgår att en förundersökning inte inletts för att gärningspersonen är under 15 år eller att brottet skett utomlands.

Olovliga registerslagningar bedöms ofta inte vara brott

Även när det gäller anledningarna för direktavskrivning avviker olovlig registerslagning till viss del från de andra dataintrångsbrotten. I en majoritet av de direktavskrivna ärendena om olovlig registerslagning anges att uppgifterna i ärendet inte ger anledning att anta att brott som hör under allmänt åtal har förövats.

Nästan alla inledda förundersökningar läggs ned

En granskning av de ärenden där en förundersökning inletts visar att de allra flesta läggs ned, med undantag för de olovliga registerslagningarna (tabell 8).

Under förundersökningen utreds vem som kan skäligen misstänkas för brottet och om tillräckliga skäl föreligger för att väcka åtal mot den misstänkte personen. I de ärenden som granskades i denna rapport är det vanligaste angivna skälet för nedläggning att *det inte längre finns anledning att fullfölja förundersökningen*, vilket ofta motiveras ytterligare av att det inte finns några spaningsresultat och därför inte några vidare utredningsåtgärder som kan vidtas, eller att det saknas tillräckligt med information för att bevisa att den misstänkta gjort sig skyldig till brottet, och att ytterligare åtgärder sannolikt inte kommer förändra bevisläget. Granskningen visar vidare att de flesta förundersökningar läggs ner utan att utredningen lyckats knyta en skäligen misstänkt person till brottet. Samtidigt finns en variation mellan de olika typerna av dataintrång i detta avseende (tabell 9).

Tabell 9. Antal och andel inledda förundersökningar om dataintrångsbrott där man lyckats knyta en skäligen misstänkt person till ett dataintrångsbrott i ärendet.[35]

	Totalt antal ärenden med skäligen misstänkt	Andel av inledda förundersökningar där en skäligen misstänkt identifierats (%)
Dataintrång genom överbelastningsattack	2	12
Dataintrång med hjälp av skadlig kod	2	2
Dataintrång genom olovliga registerslagningar	54	68
Dataintrång i sociala medier eller e-tjänster	7	16
Övrigt dataintrång	17	23
Totalt	82	

[35] Sista kolumnen i tabellen beskriver andelen ärenden där det finns minst en brottsmisstanke som gäller dataintrångsbrottet. Utöver dessa ärenden finns det fem ärenden där det förekommer brottsmisstankar för andra brott, men inte för dataintrångsbrottet. Det gäller två ärenden rörande dataintrång i sociala medier och e-tjänster (en brottsmisstanke om bedrägeri och en om penningtvättsbrott) samt tre ärenden i kategorin övrigt dataintrång (två brottsmisstankar om bedrägeri och en om olaga hot).

Misstänkt person identifierad i en majoritet av förundersökningarna om olovliga registerslagningar

Som framgår av tabell 9 är det först och främst vid olovliga register-slagningar som utredningen lyckats knyta en skäligen misstänkt person till ärendet. En misstänkt person har kopplats till brottet i 68 procent av de inledda förundersökningarna om olovlig registerslagning. Något som också skiljer de misstänkta för denna brottskod, jämfört med de övriga brottskoderna om dataintrång, vilket framgår nedan, är att majoriteten (66 procent) av de misstänkta är kvinnor. Åldersspridningen bland de misstänkta i brottskategorin olovliga registerslagningar är stor, från 19 till 67 år.

Få misstänkta kopplade till övriga typer av dataintrångsbrott

Andelen inledda förundersökningar där man lyckats knyta en skäligen misstänkt till brottet är liten för samtliga andra typer av dataintrång (mellan 2 och 23 procent).

Åldern på dessa misstänkta personer varierar stort, från grundskolelever till personer i 60-års åldern, och majoriteten är män. I de två kategorier av anmälningar där en skäligen misstänkt person har identifierats i mer än tio procent av ärendena (dataintrång i sociala medier respektive övrigt dataintrång), har anmälarna i de allra flesta fall beskrivit för polisen vem de misstänker för brottet redan vid anmälningstillfället. I de få fall där en skäligen misstänkt registrerats i ärenden som avser brott mot juridiska personer är den skäligen misstänkta antingen en anställd på företaget eller en person som företaget anger har spridit uppgifter som stulits genom dataintrång. I majoriteten av de ärenden där en skäligen misstänkt registrerats för brott mot privatpersoner är den skäligen misstänkte antingen en nuvarande eller före detta partner (drygt hälften av ärendena) eller en bekant till målsägaren.

Utredningssvårigheter

Brås intervjuer med rättsväsendets aktörer ger en bild av att utredningsarbetet av dataintrång kantas av olika svårigheter. Detta framgår även av resultaten om direktavskrivna och nedlagda ärenden i förra kapitlet. Som nämnts där finns en del anmälda dataintrång som direktavskrivs med anledning av att brottet inte går att utreda, vilket ofta motiveras med att spaningsuppslag saknas. Det vanligaste skälet till att lägga ned förundersökningar är att det inte längre finns anledning att fullfölja undersökningen som motiveras med att spaningsresultat saknas liksom svårigheter med att säkra bevisning. De intervjuer med polisanställda och åklagare som gjorts inom ramen för studien har framför allt handlat om de svårigheter som de upplever finns i utredningsarbetet, med ett särskilt fokus på de mer komplexa dataintrångsbrotten.

Det saknas ofta tillräckligt med information för att identifiera en misstänkt person

Rättsväsendets aktörer lyfter under intervjuerna ett flertal aspekter kopplade till att det är svårt att få tillgång till tillräckligt med information för att kunna identifiera vem som har begått brottet.

Spaningsuppslag från målsägaren inte alltid tillgängligt

För att kunna bedöma om brottet har förutsättningar att utredas behöver polisen inledningsvis få ta del av information från målsägaren. En av de första utredningsåtgärderna är därför att kontakta målsägaren för att få mer information. En polisanställd vid ett av it-brottscentren berättar:

> När jag får in ett ärende gör jag oftast målsägandeförhör, och hämtar in information från målsäganden. Det kan vara loggar, skärmavbilder, saker från brottstillfället. Det samlar man in i ärendet, kollar på den informationen för att se om det sen finns till exempel IP-adress att spåra. Om det inte finns det så är det ganska svårt att ta reda på vem som ligger bakom det. (Polisanställd)

Om målsäganden inte har kvar tillräckligt med spår som leder utredningen vidare kan ärendet läggas ned, berättar polisen vidare.

Utsatta företags hantering av dataintrång och bristande engagemang problematiskt för utredningsarbetet

Vid brott mot företag berättar de intervjuade polisanställda att företagens fokus ofta riktas främst mot att stoppa själva dataintrånget och rädda informationen i företagets system för att sedan återställa sina it-miljöer. Vid exempelvis ransomwareattacker är det vanligt att man försöker få bort den skadliga koden och att snabbt återställa sin it-miljö för att minimera kostnader kopplade till dataintrånget. Detsamma gäller vid överbelastningsattacker, där företag snabbt vill bli av med den överbelastande trafiken och återställa företagets tjänster eller produktion. Genom att exempelvis installera om de utsatta servrarna kan målsägaren ha förstört bevisning, och spår som polisen annars skulle ha kunnat använda. Om det är ett större företag som blivit utsatt är det större sannolikhet att företaget har kunnig it-personal som känner systemen, eller att de har knutit till sig ett it-säkerhetsföretag som skrivit en incidentrapport. Mindre företag har dock inte alltid personal som kan sammanställa information om händelsen för att delge denna till polisen.

Ett annat problem är att företagen kan vara mindre engagerade i att brottet ska utredas. Det kan handla om företagssekretess eller att företaget kan ha sin verksamhet eller sitt huvudkontor eller it-avdelning i ett annat land, där det finns en annan företagskultur eller lagstiftning, som innebär svårigheter att få ut relevanta uppgifter för utredningen av ärendet.

Det saknas information när den utsatta inte har kännedom om dataintrånget

Som nämnts tidigare i rapporten har en del av de studerade polisanmälningarna om ransomwareattacker upprättats av polisen mot bakgrund av underrättelser från Europol utan att det utsatta företaget ens varit medvetet om att de blivit infekterade med den skadliga koden. I fall där företagen inte är medvetna om sin utsatthet har de sällan någon information att delge polisen om hur intrånget gått till eller hur det kan ha påverkat företagets tjänster eller it-miljö. En polisanställd vid ett it-brottscentrum lyfter det som en svårighet:

> Om det är så att de inte har en aning om vad som har hänt och vi har inget att gå på. Det finns inget självändamål i att låta ett ärende vara öppet om det inte finns någonting att gå vidare med. (Polisanställd)

Vid de komplexa dataintrången menar intervjupersonerna att det ofta tar stopp här, redan i det inledande skedet av utredningsarbetet. Efter kontakt

med målsägaren är upplevelsen att det inte finns så mycket mer som kan göras och ärendet läggs ned.

Svårt att få information från företag som tillhandahåller internettjänster

För att kunna driva förundersökningen vidare krävs ofta information från företag som tillhandahåller de internettjänster som använts vid dataintrånget, menar intervjuade polisanställda och åklagare. Det kan exempelvis handla om användarinformation kopplad till IP-adresser eller mobilnummer från operatörer. IP-adresser kan bidra till att ge viktiga utredningsuppslag om angriparen och dennes metod. Som beskrivs i inledningen regleras de brottsbekämpande myndigheternas tillgång till detta i lagen (2022:482) om elektronisk kommunikation (LEK).[36]

Några av de polisanställda och åklagare som intervjuades har egna erfarenheter av att man inte har haft möjlighet att skicka begäran till operatörer inom det tidsspann som operatörerna enligt LEK ska lagra information. En anledning kan vara att brottet börjar utredas lång tid efter att det har begåtts. En annan anledning till att informationen inte längre finns lagrad hos operatörerna kan vara långa ledtider kopplade till processen kring rättslig hjälp eller till att få biträde från polisens it-forensiker. Vissa av de intervjuade åklagarna och polisanställda menar därför att lagringstiden är för kort.

Ett annat problem som beskrevs under intervjuerna, och som också nämnts i inledningskapitlet, är användningen av NAT-teknik, som möjliggör för flera abonnenter att dela samma IP-adress. Användningen av NAT-teknik innebär att polisen kan få en lista på många användare som delade IP-adress vid den aktuella tidpunkten, vilket utgör en utmaning för att kunna ringa in vilken av användarna som är av intresse för utredningen.

Men det är också vanligt att polisen önskar information från företag som inte har en laglig skyldighet att tillhandahålla denna. Exempelvis menar intervjupersoner att svenska hostingbolag saknar någon skyldighet att lagra

[36] Uppgifter som genereras eller behandlas vid internetåtkomst ska till exempel lagras hos operatören i tio månader, medan lokaliseringsuppgifter (uppgifter om var en mobiltelefon befinner sig när den är påslagen, men inte används) ska sparas i två månader.

och lämna ut data. Polisanställda beskriver en skillnad gentemot vad man är van med i utredningsarbetet med mer traditionell brottslighet:

> En tydlig problematik inom arbetsområdet är att normalt sett är Polismyndigheten van vid att stå och bulta på en dörr och här och nu ska vi in, den och det ska vi ha. Det kan vi oftast inte göra inom det här brottsområdet utan det blir väldigt mycket mössan i handen och kan vi få det här och kan ni hjälpa oss med det här och det innebär ju en problematik helt klart. (Polisanställd vid ett it-brottscentrum)

Vid utredningsarbetet av intrång i social media eller e-tjänster är det vanligt att polisen vill få tillgång till användardata kopplad till konton från företag som erbjuder så kallade OTT-tjänster[37]. Till dessa räknas till exempel Facebook och Instagram. Att till exempel få information om vilken IP-adress som olovligen loggat in på ett konto vid en viss tidpunkt (och därmed begått dataintrånget) är det första steget i att försöka knyta en misstänkt gärningsperson till brottet. När det gäller de här tjänsterna har intervjuade poliser och åklagare en mer positiv erfarenhet, och upplever att det finns väl upparbetade samarbeten och kanaler inom Polismyndigheten och gentemot de stora företagen för att begära ut denna information. Leverantörernas inställning till rättsväsendet får på så sätt betydelse för utredningsarbetet.

Möjligheterna till att vara anonym medför svårigheter att identifiera misstänkta personer

Det finns i dag flera sätt att försöka dölja sin identitet när man är uppkopplad till internet. Många företag erbjuder VPN-tjänster[38], vilket försvårar spårningen av den specifika användaren på internet. Möjligheten att vara anonym är en förutsättning för en fungerande demokrati, men utnyttjas enligt flera av intervjupersonerna av kriminella. En åklagare menar att vissa operatörer till och med aktivt arbetar för att motverka att rättsväsendet ska kunna utreda brott som sker på nätet, till exempel genom att erbjuda krypteringslösningar.

> Men vissa operatörer har varit ganska aktiva och försökt motverka att rättsväsendet ska kunna utreda brott som sker på nätet. Olika operatörer har haft olika inställning till polis och åklagare kan man väl säga […] där känner jag att många teleoperatörer

[37] OTT-tjänster (där OTT står för over-the-top) omfattar operatörsoberoende tjänster där användare kan kommunicera med varandra. På svenska kallas de även ibland nummeroberoende interpersonella kommunikationstjänster.

[38] VPN står för ”virtuellt privat nätverk” och är en tjänst som skyddar användarens internetanslutning och integritet på nätet genom att anonymisera användarens onlinetrafik.

> inte riktigt har det här drivet att hjälpa oss och se till att lagföra brott utan de vill snarare skydda sina kunder och tjäna pengar. (Åklagare)

Det handlar även om att informationen som flödar i nätverken allt mer ofta krypteras, vilket framhålls som problematiskt från flera intervjupersoner.

> […] det förstås är ett problem i Sverige (ur ett utredningsperspektiv) att krypteringen blir bättre och bättre. Privatskyddet ligger alltid steget före lagstiftningen så att säga. […] (Åklagare)

Dataintrångens internationella kopplingar försvårar utredningsarbetet

Såsom framkom i avsnittet ovan finns den information som polisen behöver ofta inte lagrad lokalt på en mobiltelefon, dator eller server utan finns i det så kallade molnet och kan rent fysiskt finnas utanför landets gränser, uppdelad på servrar i olika länder eller så kan det vara omöjligt att veta var den finns lagrad (så kallad loss of location). Den typ av information som polisen kan vara intresserad av i utredningsarbetet vid dataintrångsbrott varierar stort. En åklagare ger några exempel:

> Det kan vara att du gjort intrång nånstans och kommit över uppgifter om bankkonton som du lagrar på en server och säljer vidare för ytterligare brottslighet. Det kan vara ett dokument med det du har stulit nånstans ifrån. Det kan vara en programvara, en command and control-server, de blir ju ett botnet. Man kanske också vill se vilken typ av uppkopplingar som gjorts, så att man kan spåra tillbaka. Det kan alltså både vara kofoten, själva brottsverktyget som ligger där, det kan också vara resultatet av vad brottet gett. Du kanske har dina bitcoin där som du har fått för ransomware. Så det är ju lite olika. (Åklagare)

Vid Brås intervjuer med åklagare framhölls att utredningsarbetet skulle underlättas om det skulle finnas möjlighet att ta del av materialet som finns i molntjänster kopplade till beslagtagna föremål. Sedan intervjuerna genomfördes har lagändringar införts som innebär en möjlighet att säkra tillgång till elektroniska handlingar på externa servrar eller i molntjänster genom den nya lagen om genomsökning på distans. Lagändringarna trädde i kraft den 1 juni 2022. Den nya lagen innebär att när informationen finns lagrad på en server i Sverige kan förundersökningsledaren besluta om att genomföra genomsökning på distans. Även med den nya lagstiftningen menar dock experter i Brås referensgrupp att det fortfarande finns svårigheter med att genomföra genomsökning på distans om informationen finns utanför landets gränser eller om man inte kan säga var den finns lagrad.

Långa ledtider vid rättslig hjälp försvårar utredningsarbetet

Internationell rättslig hjälp i utredningar avser åtgärder som åklagare behöver bistånd med från en annan stat, men vid bevisinhämtning inom EU tillämpas i stället en europeisk utredningsorder (EIO).

Både polis och åklagare lyfter att det ofta tar tid att få hjälp med att genomföra efterfrågade utredningsåtgärder genom rättslig hjälp eller EIO. Det kan ta allt från månader till ibland flera år att få svar från vissa länder. Detta är ett problem då information som finns på nätet snabbt kan flyttas, raderas eller ändras. Detta lyfts speciellt som ett problem vid rättslig hjälp, men vissa beskriver tidsödande processer även vid tillämpningen av EIO inom EU. En polisanställd vid ett av de regionala it-brottscentrum menar att det är särskilt problematiskt om man först får vänta en längre tid, för att sedan få ett svar som inte ger något, eller som innebär att man behöver ställa följdfrågor, eftersom man inte fått ett fullständigt svar. Att man inom ramen för en utredning kan behöva tillämpa en EIO eller begära rättslig hjälp från flera länder försvårar ytterligare.

> Den internationella aspekten har sina utmaningar när man skickar rättslig hjälp. Vi ska veta vilket land är det som vi ska rikta oss mot, och sen ska den skrivas och det tar sin lilla tid kan man säga, sen ska den översättas och skickas via justitiedepartementet och … sen får man hoppas att mottagarlandet har en välfungerande myndighetsstruktur; det ska mottas där och så ska det i sin tur lottas till den åklagaren eller den polisen som utför åtgärderna. Och så ibland riktar vi oss mot flera länder och då krävs det koordinerade tillslag i flera länder, … det är en apparat i sig. Och sen när de då utfört åtgärderna ska de tillbaka hela vägen med översättningar och sånt innan det kommer till oss och då får vi informationen i bästa fall inom ett par veckor, i sämsta fall aldrig, men oftast tar det flera månader. (Åklagare)

Då digital information snabbt kan förflyttas eller raderas är det problematiskt att behöva vänta på att mottagarlandet för en begäran om rättslig hjälp eller en EIO genomför de önskade utredningsåtgärderna. I och med att budapestkonventionen ratificerades 1 maj 2021 infördes dock ett bevarandeföreläggande i svensk lag som innebär att brottsbekämpande myndigheter kan begära att få information fryst så att den inte kan förflyttas eller raderas (prop. 2020/21:72). Ett bevarandeföreläggande behöver inte skickas enligt proceduren för rättslig hjälp till länder utanför det europeiska samarbetet. Inom EU däremot måste en svensk order om att få data fryst gå genom en EIO, vilket är problematiskt då det motverkar syftet som är just att data ska kunna frysas direkt.

Särskilt svårt med bevisning vid organiserad brottslighet

En ytterligare aspekt som lyfts vid Brås intervjuer med polisanställda och åklagare är att det i komplexa dataintrång ofta är organiserade grupperingar som ligger bakom brotten. När det gäller ransomwareattacker uppger polisanställda att man brukar kunna säga vilken grupp som ligger bakom den skadliga koden, vilket dock inte behöver betyda att det är samma grupp som har genomfört attacken.

> När det gäller ransomware brukar man ganska lätt kunna säga vilken grupp som ligger bakom. Alla filer som blir krypterade på en server eller en dator, de får en viss filändelse som är unik för just den här grupperingen. Och då är det olika... Det går i olika vågor med vilka ransomware som är dominerande i samhället […]. Problemet vi hamnar i är att ransomware kanske görs av några men används av en annan grupp. Dom kan hyra den här tjänsten och förfoga över den här tjänsten som de vill. De som gör programmen är inte nödvändigtvis samma som använder programmen. (Polisanställd vid ett it-brottscentrum)

Det som beskrivs i citatet är en tjänst som kallas Ransomware-as-a-Service (RaaS), vilket nämndes i inledningskapitlet. För att utreda dessa komplexa dataintrång menar polisen att man skulle behöva ta sig in i servrar som de kriminella nätverken använder för att avlyssna den nätverkstrafik som går till och från servern. På så sätt kan man spana på den kriminella aktiviteten samt följa trafiken för att hitta gärningspersoner. En åklagare förklarar:

> Om man hade möjlighet till hemlig avlyssning så skulle man kunna lyssna på kommunikationen inom den här gruppen. Man skulle få en ingång i den brottsliga infrastrukturen om man säger så. Där olika personer har olika roller i organisationen. Eller för den delen om det är en person som avlyssnas som kanske har inhämtat information inom nätverket. Det skulle verkligen vara en nyckel att lyssna på den trafiken, även om man inte vet vem som kommunicerar. (Åklagare)

Om vissa kriterier är uppfyllda, såsom att brottet har minst två år i straffskalan samt att man har identifierat en skäligen misstänkt gärningsperson, är det möjligt att använda tekniska metoder som skulle göra detta möjligt att arbeta med på det sätt som beskrivs i citatet ovan genom det relativt nya hemliga tvångsmedlet hemlig dataavläsning (HDA). Problemet är dock att det i princip alltid saknas en skäligen misstänkt i de komplexa dataintrången vilket flera av de intervjuade beskriver som en paradox.[39]

[39] Det finns ett utredningsförslag om att ändra i lagen om hemlig dataavläsning i syfte att kunna använda tvångsmedlet för att utreda vem som kan tänkas misstänkas för ett brott (SOU 2022:19).

> Startpunkten för oss är ett IP-nummer. Det behövs otroligt mycket för att man ska nå fram till en person. Kravet på skäligen misstänkt kommer aldrig kunna tillgodoses utan det är genom infrastrukturen vi kan hitta dem som kopplar upp sig mot de maskinerna som används. (Polisanställd)

Som nämnts i inledningskapitlet finns även möjlighet att beställa överbelastningsattacker. En polisanställd vid ett av polisens it-brottscentrum lyfter att det kan vara svårt att spåra överbelastningsattacker, eftersom målsägaren blir attackerad från infekterade datorer med IP-adresser som leder till många olika länder. Det krävs någon ytterligare bevisning i ärendet för att man ska kunna gå vidare i utredningen.

Andra utmaningar för ett effektivt utredningsarbete

Föregående kapitel redogjorde för de svårigheter rättsväsendets aktörer menar finns när det kommer till att utreda dataintrång. Dessa svårigheter är kopplade till det konkreta arbetet med att utreda dataintrångsärenden. Förutom det framkom i intervjuerna med rättsväsendets aktörer även andra utmaningar, som bland annat är kopplade till polisens organisation och arbetssätt, som påverkar möjligheterna att arbeta med dataintrångsärenden på ett effektivt sätt. Föreliggande kapitel redogör för dessa utmaningar.

Stort mörkertal

Ett återkommande tema i Brås intervjuer är att man påtalar det stora mörkertalet av dataintrång som inte polisanmäls. Exakt hur stort mörkertalet är givetvis svårt att uppskatta. Mörkertalet beror dels på att utsatta inte märker av att de utsatts, dels att utsatta väljer att inte polisanmäla händelsen.

Många dataintrång upptäcks inte

Flera av Brås intervjupersoner menar att många offer troligtvis aldrig upptäcker att de utsatts för dataintrång.

> Det första är ju att man ska märka att man blir anfallen. Och det är inte säkert att man har gjort. […] De allra flesta angrepp märker folk inte före skada sker. Så man märker inte av intrånget, man märker inte av informationsstölden, kopieringen. Man märker när nån krypterar en databank eller nån stänger ner en tjänst. Så jag skulle tro för det första att där att det är nog många som inte vet överhuvudtaget att de har blivit angripna. (It-säkerhetsexpert)

Dataintrång som syftar till att sabotera eller utöva utpressning på offret (till exempel ransomware) kommer med större sannolikhet att upptäckas än dataintrång där syftet är att komma över känslig data. Det framgår också av både Brås genomgång av brottsanmälningarna och av intervjumaterialet att polisen får uppgifter om att företag utsatts för dataintrång som det sedan visat sig att företagen inte kände till när polisen kontaktat dem.

Upptäckta dataintrång polisanmäls inte

En indikation på att anmälningsbenägenheten är låg är att endast 27 procent av de it-incidentrapporter med misstänkta antagonistiska angrepp som inkom till MSB[40] under 2021 har eller planeras att polisanmälas enligt uppgiftslämnarna (MSB 2022). En annan indikation är att det, enligt en intervjuperson från ett privat it-säkerhetsföretag, är få av deras kunder som utsatts för intrång som sedan polisanmäler intrånget. Detta pekar på en stor underrapportering av dataintrång till polisen.

Mörkertalets problem

Mörkertalet vid cyberbrottslighet uppges av Europol (2020) vara en stor utmaning för rättsväsenden i Europa. Flera av Brås intervjupersoner lyfter också mörkertalet som ett stort hinder för att kunna bekämpa dataintrångsbrottsligheten. Inför en av Brås intervjuer med åklagare hade hen kontaktat det nationella nätverket för kontaktåklagare för it-relaterad brottslighet och bett dem ange de största utmaningarna i arbetet mot dataintrångsrelaterad brottslighet. Nätverket ansåg att brott som inte kommer till polisens kännedom var en av de största utmaningarna. Särskilt när det gäller den organiserade cyberbrottsligheten är enskilda brott (exempelvis en ransomwareattack) ofta en del av ett större angrepp, nationellt eller internationellt. Om dessa brott inte kommer till rättsväsendets kännedom försvåras möjligheterna att se mönster och koppla ihop brott som hör ihop samt förutsättningarna för att samarbeta internationellt.

Direktavskrivningar vid polisens kontaktcenter gör att anmälningarna inte kommer fram till utredarna

En stor del av polisanmälningarna om dataintrång inkommer till PKC, som i sin tur fördelar de komplexa dataintrången till KCB-enheterna vid it-brottscenter. Hur PKC hanterar anmälningar om dataintrång är därför av vikt för polisens fortsatta hantering.

Flera av intervjupersonerna inom rättsväsendet uttrycker en frustration över PKC:s hantering av komplexa dataintrång. De handlar främst om att PKC ibland felaktigt direktavskriver ärenden eller inte tar upp anmälningar från anmälare med hänvisning till att dataintrångshändelsen inte skulle vara ett

[40] Alla statliga myndigheter och leverantörer av samhällsviktiga tjänster (så kallade NIS-leverantörer) ska rapportera it-incidenter som deras informationssystem utsätts för eller i tjänster som de tillhandahåller åt en annan organisation.

brott. När detta sker får inte KCB-enheterna in information om de brott som begås. En polisanställd beskriver hur hon under en period gått igenom samtliga anmälningar som inkommit till PKC för att leta efter brottsanmälningar där det rörde sig om ett specifikt it-angrepp som drabbade flera företag och privatpersoner runt om i Sverige under en period. Hen hittade då många ärenden som blivit felrubricerade (i stället för dataintrång var de kodade som bedrägeri eller utpressning), eller som lagts ner innan de nått utredande KCB-enheter.

Intervjuade polisanställda beskriver att man tagit fram metodstöd för PKC samt åkt ut till dem och informerat om brottstypen. Samtidigt finns en förståelse för att PKC tar emot en stor andel av den totala mängden anmälningar som inkommer till polisen. Dataintrång, och särskilt de mer komplexa dataintrången, utgör en antalsmässigt väldigt liten del av dessa. Att ha tillräckligt med kompetens inom alla de typer av brott som polisanmäls för att alltid göra korrekta bedömningar kan tyckas svårhanterligt.

Brister i samordning och informationsdelning mellan it-brottscentren

Förutom att flödet av anmälningar från PKC till utredande enheter behöver ökas, behövs även en samordning av de inkomna ärendena. De komplexa dataintrången, såsom vid ransomwareattacker, kan innebära att många drabbas samtidigt: privatpersoner, företag, organisationer och myndigheter. Genom supply-chain-attacker kan intrång ske på många verksamheter samtidigt, och som uppges av en it-säkerhetsspecialist som Brå intervjuat har dessa ökat dramatiskt på senare tid. Om samma attack sker mot mål i olika regioner, med samma mjukvara eller där de utsatta får samma kontaktuppgifter för att förhandla om lösensumma, menar Brås intervjupersoner att det saknas en adekvat struktur inom polisens utredningsorganisation för att säkra att ärendena samordnas. Utredningarna bedrivs ofta på olika regionala it-brottscentrum, vilket innebär en större risk för att de läggs ned:

> Vi har möten tillsammans, men vi har inte en jättetydlig form för såhär "Okej, nu har jag fått in ett ärende som rör den här ransomware-grupperingen"; då är det jättesvårt för mig att veta om det är en annan region som också har fått in det, på ett annat sätt än att vi säger det på ett möte, om ni fattar vad jag menar. Det skulle finnas andra former för hur man delar den informationen på ett smidigt sätt, för att kunna samarbeta bättre. (Polisanställd vid ett it-brottscentrum)

Enstaka polisanmälningar som inte samordnas medför att utredarna inte får tillgång till all information om brottet. En åklagare berättar:

> Det är många som drabbas såhär, en del har gått till polisen, andra inte. Och det är svårt att se att saker och ting hänger ihop, för det blir så sporadiskt. Jag anmäler det här på en polisstation och sedan har nån annan privatperson anmält nån annanstans. Den här samordningen, att se att nu är det väldigt mycket dataintrång utav den här typen. Det är ju väldigt beroende av dels att polisen kan se i sina system att det här är samma…. Och om man inte ser storskaligheten i det, då tror jag det är svårt att utreda. Det är också just det här att.... den samordningen är jättesvår att hitta. (Åklagare)

Bristande förutsättningar hos KCB-enheterna

Det finns skillnader i hur länge de regionala it-brottscentrum samt det nationella it-brottscentrum har funnits samt hur länge funktionen komplexa cyberbrott (KCB) funnits vid dessa centrum. Det innebär att det är möjligt att intervjupersonernas svar på frågor om resurs och kompetens bland annat präglas av hur länge deras respektive verksamhet har varit igång.

> […] organisationen inom KCB-sidan är inte helt satt ännu så det är mycket som både har utvecklats och som kommer utvecklas, mycket. (Polisanställd)

Brås intervjuer visar att det finns en variation i intervjupersonernas uppfattning om huruvida det finns tillräckligt med resurser och kompetens för att genomföra sitt arbete. Polisanställda från ett relativt nybildat regionalt it-brottcentrum tryckte på det positiva med att ha tillgång till många kompetenser, och såg inga brister i vare sig resurs eller kompetens. Andra polisanställda upplevde däremot både en resurs- och kompetensbrist. Vid vissa it-brottscentrum uppger polisanställda att de är för få utredare som arbetar med komplexa cyberbrott. Ett problem är också att den kompetens kring komplexa cyberbrott som polisens utredare besitter också är attraktiv inom den privata sektorn, där lönerna ofta är mycket högre.

> […] det är alldeles för få som arbetar här. Vi behöver mycket fler personer. Speciellt också fler kunniga personer, men man får låg lön här jämfört med att jobba på företag. Där de kan tjäna hur mycket som helst i månaden. […] så jag tror det finns ett stort problem i att det inte går att locka hit [it-kunnigt] folk. (Polisanställd vid ett it-brottscentrum)

Några av de intervjuade polisanställda lyfter även att det finns en kompetensbrist framför allt när det gäller att analysera skadlig kod.

> Vi har inte så mycket möjligheter till att få hjälp med att analysera skadlig kod. Det är klart det finns ju massa CERT till exempel som är jätteduktiga på den här biten men det är inte deras uppgift. Vi på utredningssidan… Jag tänker i alla fall att jag skulle gärna ha mer möjlighet att få bistånd till analys av skadlig kod. Det är väldigt centralt i tillvägagångssättet. Man kan självklart använda uppgifter från företag också om de har gjort en egen analys, men då kontrollerar ju inte polisen informationen. (Polisanställd vid ett it-brottscentrum)

Därutöver framkommer att vissa ser behov av utbildning för de polisanställda som utreder dataintrång med motiveringen att ”vi har inte tillräckligt mycket folk som kan de tekniska bitarna”. Det ligger i it-brottens karaktär att det hela tiden sker en utveckling av tillvägagångssätt, och polisen behöver kontinuerliga utbildningsinsatser för att följa med i denna utveckling.

Brist på it-forensiker påverkar utredningsarbetet

Vid utredningsarbetet av komplexa dataintrång behövs ofta biträde från it-forensiker för att kunna säkra spår, till exempel för att spegla en server och sedan analysera resultatet. Att de långa ledtiderna hos it-forensiker skapar en flaskhals i utredningsarbetet av it-relaterad brottslighet är väl dokumenterat i tidigare rapporter (Riksrevisionen 2015, Brå 2016a, Polismyndigheten 2020). Det finns inte heller frihetsberövade vid dataintrång, vilket innebär att andra ärenden prioriteras högre av it-forensikern. Behovet av biträde av it-forensiker lyfts även av vissa it-brottscentrum, som framhåller behovet av en snabbare it-forensisk hantering.

> Köerna är hur långa som helst. Det kan liksom vara flera år innan vi får tillbaka resultat av det här. Och om vi då får tillbaka resultatet, då kan det ju bli så att här är en IP-adress, men vi kan inte spåra den, för informationen är inte sparad. Så det finns ingen idé från början att ta in nånting för man vet att det kommer ta så pass lång tid att IP-adresserna inte finns kvar hos operatören innan vi får tillbaka resultatet. Man kan från början se att vissa utredningsåtgärder är helt onödiga och att det inte kommer att gå att lösa ett fall för att ledtiderna hos forensikerna är alldeles för långa. (Polisanställd)

Vidare lyfts även behovet av mer hjälp med analyser av de inhämtade materialen.

> Som it-forensiker för länge sedan, då gjorde it-forensikern allt. Man tog in beslaget, man speglar beslaget, man analyserade beslaget och lämnade en rapport med det som har betydelse för ärendet. Nu gör man det lite lätt för sig och tar in, speglar och skickar ut ett axiom dump, som egentligen är en avbildning, abstraktion av

innehållet så får utredaren själv sitta och klicka runt där. Vilket är ganska olyckligt då det bygger på att utredaren själv har utbildning eller vet vad han håller på med. Man kan hitta, man kan läsa e-post ganska enkelt men man skulle förmodligen missa de lite mer svårfunna spåren. (Polisanställd vid ett it-brottscentrum)

Ärenden utreds inte uttömmande nog

Både polisanställda och åklagare konstaterar att många av de komplexa dataintrången, speciellt ransomware, är mycket svåra att utreda, bland annat på grund av den internationella kopplingen. De intervjuade polisanställda vid it-brottcentrum menar att dessa ärenden inte går att utreda lokalt, och att de läggs ned. Men de poängterar att den information som kommer fram inom ramen för de nedlagda svenska förundersökningarna skickas vidare till Europol och kan bidra till att föra en internationell utredning framåt.

Jag tror inte riktigt att vi ser på de här nedläggningarna som nedläggningar. Utan vi ser det som att vi gör vår del av arbetet men så leder det till nedläggning hos oss men så fort vi har samlat ihop den information vi kan så skickar vi den till Europol för samordning och så väntar vi oss att de fortsätter att arbeta med den på ett eller annat sätt. Medan det svenska ärendet läggs ned i väntan på ytterligare information eller en framtida insats. (Polisanställd vid it-brottscentrum)

Enligt intervjupersoner med inblick i det internationella samarbetet mot komplexa cyberbrott, är det dock vilseledande att tro att information från nedlagda svenska förundersökningar kommer generera utredningsunderlag som kan vara till nytta inom ramen för internationella polisoperationer. I stället är det viktigt att ärenden inte läggs ner för fort, till exempel med hänvisning till att brottet har skett utomlands och att det därför inte går att utreda. Det är när länder arbetar mer uthålligt, med utredningar som de aktivt arbetar med under en längre tid, som man ser resultat av utredningsarbetet.

Lägger vi [polisen] ner ett ärende har vi ofta gjort ett fåtal åtgärder. Sällan har de åtgärderna inkluderat att inhämta information från den kriminella grupperingens infrastruktur. Vi kanske har bitcoinadresser, kanske undersökt målsägandes dator eller har en rapport från ett privat företag. Men det här är ett startskott. Det är en bottenplatta för en ransomwareattack. Sen måste vi gå vidare. Vi måste in i infrastrukturen. Nästa nod måste identifieras medan den fortfarande är aktiv. Den servern ska vi beslagta. (Polisanställd)

För att komma åt dem som begår komplexa dataintrång krävs att man i en högre utsträckning arbetar för att kartlägga ett kriminellt nätverk, snarare än

att endast utreda enskilda brott. Det krävs samordning av brotten inom Sverige och dessutom att man samarbetar med rättsväsenden i andra länder.

Flera samverkande faktorer som försvårar polisens arbete mot dataintrång

Sammanfattningsvis visar Brås intervjuer om de utredningssvårigheter och utmaningar som finns vid polisens arbete mot dataintrång att detta arbete försvåras av flera samverkande faktorer. En del av dessa, till exempel anmälningsbenägenheten och de problem som kopplas till lagstiftningen och operatörer som inte vill samarbeta med brottsbekämpningen, är svåra för polisen att påverka själva.

Samtidigt finns det flera faktorer som skulle kunna påverkas. Även om den låga anmälningsbenägenheten innebär att polisen från början har ett relativt magert underlag att jobba med, är det hos polisen som en del av detta underlag sedan faller bort genom att de brott som faktiskt polisanmäls inte hamnar rätt inom utredningsorganisationen. Anledningen till detta är svårigheter när det gäller att identifiera dataintrång vid anmälnings-upptagningen och se till att de registreras under rätt brottskod och skickas vidare till rätt utredningsenhet.

Därutöver finns en bristande samordning, som innebär att det saknas möjlighet till att uppnå den korsbefruktning som skulle ske om den information som finns i olika ärenden rörande samma kriminella aktör eller brottsupplägg bättre kunde tas tillvara inom ramen för samma utredning. Problemen försvåras ytterligare av att de spår som finns i det material som inkommer till polisen inte kan utnyttjas på ett optimalt sätt på grund av en överbelastad it-forensisk verksamhet som tar så lång tid att nyttan av resultaten för att driva utredningar vidare urholkas. Intervjuerna ger också en bild av att detta leder till att ärenden direktavskrivs eller läggs ner i ett tidigt skede eftersom utredarna inte tror att det är värt att följa de spår som trots allt finns.

Utvecklingsområden

Dataintrång del av ett viktigt men svårhanterligt hot

Dataintrång är en viktig del av den cyberbrottslighet som har ökat i takt med teknikutvecklingen och den tilltagande digitaliseringen av samhället (Centrum för cybersäkerhet 2022, Yar och Steinmetz 2019). Den komplexa dataintrångsbrottsligheten omsätter stora värden, sker i organiserad form och kommer sannolikt att fortsätta att öka. Allteftersom den organiserade cyberbrottsligheten utvecklas menar forskare att den sannolikt i allt högre grad kommer att rikta attacker mot de mest lukrativa målen, såsom företag och stora organisationer, eftersom det är där de största möjligheterna finns för en hög avkastning (Brady och Heinl 2020). Som nämnts i inledningskapitlet finns också ett cyberangreppshot från externa statliga aktörer, som vill bereda sig möjlighet att genom dataintrång störa samhällsviktiga funktioner. Dataintrångsbrottsligheten är därmed ett betydande nuvarande och framtida hot mot såväl svenska företag och medborgare som landets digitala infrastruktur.

Brottsligheten sker både i en digital miljö och över nationella gränser, och som framgår av Brås genomgång av utredningssvårigheterna är brottsligheten förknippad med stora utmaningar när det gäller det svenska rättsväsendets möjligheter att utreda och lagföra brotten. Historiskt sett har de flesta brottstyper kunnat utredas inom Sveriges gränser, och framför allt på lokalnivå. Vidare har de flesta traditionella brottstyper kunnat utredas med fokus på den enskilda polisanmälan eller ärendet. Detta är inte möjligt med i synnerhet de komplexa dataintrångsbrotten, dels för att de enskilda brotten oftast bara utgör en liten pusselbit, som endast ger en mycket begränsad inblick i den mer omfattande brottsligheten som ligger bakom, dels för att den information som behövs för att utreda brotten ofta finns utomlands. Jämfört med den traditionella brottsligheten kräver således komplexa cyberbrott, däribland dataintrångsbrotten, ett annat tillvägagångssätt och ett annat sätt att organisera brottsbekämpningsarbetet.

Viktigt med ett fokus på det internationella polisiära samarbetet

En slutsats utifrån den befintliga kunskapen på området och Brås genomgång av de anmälda brotten, som också lyfts av flera intervjupersoner, är att ett

framgångsrikt brottsbekämpningsarbete mot den organiserade dataintrångsbrottsligheten kräver ett aktivt polisiärt samarbete på internationell nivå. På grund av den organiserade cyberbrottslighetens strukturer och tillvägagångssätt är den här typen av samarbete en förutsättning för att kunna åstadkomma effektiva brottsbekämpningsåtgärder. Dels handlar det om att driva uthålliga brottsutredningar mot kriminella grupperingar. Enligt intervjupersoner kan det krävas flera år av spaningsarbete mot en viss kriminell gruppering för att kartlägga den. Dels kan det handla om att slå mot den kriminella infrastrukturen som möjliggör för komplexa cyberbrott, till exempel genom att ta ner forum som används av kriminella och marknadsplatser på darkweb där kriminella köper och säljer tjänster och stulen information (se t.ex. Europol 2021). Enligt Brås intervjupersoner utgör detta arbete en viktig brottsförebyggande åtgärd.

Brås intervjuer visar att den svenska polisen i dag i mångt och mycket fortfarande arbetar på ett relativt traditionellt sätt vid de nya regionala it-brottscentrumen, där de enskilda ärendena framför allt utreds i respektive region för sig. Den svenska polisens bidrag till det internationella samarbetet har enligt intervjupersoner framför allt handlat om att utreda dessa enskilda ärenden så långt det går, och sedan, efter nedläggning, skicka den insamlade informationen till Europol. Som också nämnts menar dock intervjupersoner med inblick i det internationella samarbetet mot komplexa cyberbrott, att det är vilseledande att tro att detta arbetssätt kommer generera underlag som kan vara till nytta inom ramen för internationella polisoperationer.

Utifrån Brås kartläggning framstår det som att det som i stället behövs är ett mer uthålligt arbete, där enskilda ärenden inte läggs ner för snabbt, och där man får bättre möjligheter att identifiera och samordna ärenden som härrör från samma kriminella aktör, både regionalt och nationellt, och att därmed kunna utreda brotten utifrån ett mer omfattande underlag, till exempel i team där det ingår representanter från såväl regionerna som det nationella it-brottscentrumet.

I förlängningen skulle detta skapa mer gedigna utredningar, som enligt intervjupersoner är en förutsättning för svensk polis att delta aktivt i internationella polisiära operationer mot den organiserade cyberbrottsligheten. Den här typen av delaktighet skulle i sin tur ha en kompetenshöjande effekt för både de enskilda polisteam som deltar i de internationella samarbetena och för deras kollegor på regionerna och det nationella it-brottscentrumet. Att kunna vara med i dessa internationella sammanhang

förutsätter dock en utrednings- och underrättelseorganisation inom polisen som möjliggör för svensk polis att arbeta fram de nödvändiga utredningsunderlagen, samt även att det finns en tydlig målbild om att nå dit, och en långsiktig strategi för att åstadkomma detta inom polisorganisationen.

En viktig del i detta arbete är också att identifiera prestationsmått för cyberbrottsbekämpningen inom polisorganisationen som tar sikte på de steg som behöver uppfyllas för att uppnå målbilden. Ett fokus på person-uppklaring på ärendenivå kommer vara problematiskt i detta sammanhang, eftersom även ett mycket framgångsrikt arbete med fokus på internationella samarbeten sannolikt inte kommer att leda till ett större antal lagföringar för dessa brott just i Sverige. Detta är också en viktig faktor för polisen att ta hänsyn till i sitt kommunikationsarbete med målgrupper som företag och andra organisationer.

Som nämnts i rapporten är den låga anmälningsbenägenheten för komplexa cyberbrott ett problem för polisens möjligheter att identifiera och samordna brott som begås av samma grupper av kriminella aktörer. Det kan finnas flera olika anledningar bakom den låga anmälningsbenägenheten, exempelvis skamkänslor eller en rädsla bland företag inför att offentliggöra att man blivit utsatt för dataintrång, då detta skulle kunna skada förtroende för företaget. Men i den mån den låga anmälningsbenägenheten också beror på en förtroendebrist kopplat till en låg personuppklaring på ärendenivån, är det viktigt för polisen att kunna kommunicera att de har ett arbetssätt som siktar mot att ha effekt på den organiserade cyberbrottsligheten. Det är också viktigt att klargöra att även om arbetets resultat inte i första hand kommer bli synligt i den svenska uppklaringsstatistiken, blir effekten av ett mer utvecklat internationellt samarbete ett förbättrat skydd för svenska företag, myndigheter, organisationer och privatpersoner. Vidare är det viktigt för polisen att kommunicera framgångar i det internationella arbetet mot cyberbrottsligheten på ett effektivt sätt.

En mer utvecklad och ändamålsenlig, och mindre sårbar, polisiär organisation

Brås intervjuer med personer i olika positioner inom polisorganisationen ger en samlad bild av en polisiär infrastruktur för utredning av komplexa cyberbrott som fortfarande är under uppbyggnad, och som också är sårbar. Organisationen med de regionala it-brottscentrumen är relativt ny, och som

framgick i förra kapitlet saknas det en tydlig samordningsfunktion på nationell nivå.

Det framgår också av Brås intervjuer med polisanställda att det finns skillnader mellan regionerna i hur långt man har kommit i uppbyggnadsarbetet och också i hur man har strukturerat arbetet mot komplexa cyberbrott på den regionala nivån. Enligt intervjupersoner finns exempelvis en dedikerad it-forensisk resurs kopplad till komplexa cyberbrott i vissa regioner men inte i andra. I de fall där det saknas en dedikerad it-forensisk resurs måste cyberbrottsutredningar konkurrera med andra typer av brottsutredningar, bland annat sådana där en person har häktats. Vikten av att snabbt kunna inhämta och analysera it-forensiskt material innebär att avsaknaden av en dedikerad resurs fungerar som en stoppkloss i utredningsarbetet som riskerar hela utredningen. En dedikerad it-forensisk resurs som jobbar nära utredningarna är också en förutsättning för att utveckla och upprätthålla de specifika typerna av it-forensisk kompetens som behövs till utredningar om komplexa cyberbrott, och som skulle ge förutsättningar för att bidra till dessa utredningar på ett optimalt sätt.

Att de regionala centrens arbete fortfarande är under uppbyggnad innebär att det också är sårbart. Flera intervjupersoner pratade till exempel om sårbarheter kopplade till personberoenden, till exempel om någon skulle byta jobb eller få i uppgift att biträda i andra utredningar som givits högre prioritet. En förutsättning för att kunna arbeta uthålligt och ändamålsenligt är att arbetet dimensioneras på ett sätt som minimerar eller eliminerar dessa sårbarheter.

Förbättrat stöd till polisens kontaktcenter (PKC)

Som nämnts i förra kapitlet är en annan viktig förutsättning för att förbättra utredningsmöjligheterna att polisens cyberbrottscenter får in mer information om de komplexa cyberbrott som sker i samhället. Detta är delvis ett problem som är kopplat till den låga anmälningsbenägenheten för komplexa cyberbrott, som nämnts i avsnittet ovan. Men den låga anmälnings-benägenheten gör det ännu viktigare att den information som faktiskt kommer in till polisen hamnar rätt inom polisorganisationen. En slutsats av Brås studie är att en del av den information som kommer in till polisen i form av anmälningar via PKC inte hamnar på rätt bord. Ett problem här är att det inte finns någon möjlighet för de anställda som arbetar vid dessa kontaktcenter att bli experter på alla de olika typer av brott som anmäls till

polisen. Ett viktigt utvecklingsområde för polisens arbete mot cyberbrottsligheten är därmed att utveckla det stöd som finns för PKC-anställda, till exempel genom att utveckla ett digitalt stöd vid anmälningsupptagning, så att de anställda får bättre möjlighet att identifiera anmälningar som rör komplexa cyberbrott och att se till att de hamnar rätt inom polisorganisationen samt att de inte direktavskrivs redan vid anmälningstillfället.

Ett utvecklat samarbete med privata aktörer

Ett ytterligare utvecklingsområde avser möjligheterna till samverkan mellan polisen och privata aktörer inom it-säkerhetsområdet. Både poliser och it-säkerhetsspecialister som intervjuats i studien menar att denna samverkan kan vara en viktig framgångsfaktor i arbetet med att bekämpa cyberbrottsligheten. Europol har löst samarbetsproblematiken genom att upprätta icke juridiska bindande kontrakt, så kallade Memoranda of Understanding, där det tydligt framgår vad Europol förväntar sig av de privata aktörerna och vice versa. De privata aktörerna sitter med vid ett *Advisory Board* vid *European cybercrime center* (EC3). En liknande funktion vid polisens nationella it-brottscentrum skulle kunna stödja centret i dess arbete och främja möjligheten att dela och ta del av information om bland annat cyberbrottslighetens utveckling, aktiva kriminella grupperingar, skadlig infrastruktur och nya brottsupplägg. Dessa samarbeten kan också ge polisen viktiga inblickar i attacker mot exempelvis företag som väljer att inte polisanmäla, men som ändå vänder sig till privata säkerhetsaktörer för hjälp. Samtidigt finns det enligt polisanställda svårigheter med att formalisera den här typen av samarbete, bland annat på grund av sekretessfrågor.

En fortsatt modernisering av relevant lagstiftning

Även med utvecklingsarbete av den typ som beskrivits ovan är polisens möjligheter att utreda komplexa dataintrång och delta i internationella sammanhang beroende av en ändamålsenlig lagstiftning. En utmaning som lyfts både i tidigare Bråapporter (t.ex. Brå 2015, Brå 2016a) och i intervjuer med polis och åklagare i den här studien är att lagstiftningen inte har hängt med i den digitala brottsutvecklingen.

Under de senaste åren har regeringen tillsatt ett flertal utredningar med syftet att se över olika delar av lagstiftningen kopplat till rättsväsendets möjligheter att bereda sig tillgång till elektroniska uppgifter i utredningsarbetet i syfte att

anpassa lagen efter dagens digitala verklighet.[41] En del förändringar har skett under de senaste åren, såsom lagarna om de nya tvångsmedlen hemlig dataavläsning (HDA) och genomsökning på distans, som ger möjlighet för polisen att bereda sig tillgång till information som finns lagrad i molnet.

Ett fortsatt arbete med att modernisera lagstiftningen och anpassa den efter den föränderliga digitala verkligheten är också en förutsättning för de brottsbekämpande myndigheterna att kunna arbeta effektivt mot dataintrång och andra typer av cyberbrott.

De ”icke-komplexa” dataintrången

Huvudfokus för Brås analys av utvecklingsområden för det brottsbekämpande arbetet har haft fokus på de komplexa dataintrångsbrotten, framför allt på grund av att dessa utgör det största hotet mot svenska företag och myndigheter, och i förlängningen mot samtliga svenska medborgare. Samtidigt visar Brås genomgång av de polisanmälda brotten att det också sker ett stort antal dataintrångsbrott, bland annat i form av olovliga registerslagningar och genom intrång i sociala medie- och andra e-tjänstkonton, som inte utreds inom polisens organisation för komplexa cyberbrott.

När det gäller rättsväsendets arbete med att utreda och lagföra brotten sticker de olovliga registerslagningarna ut i den mening att de oftare leder till uppklaring i de fall där anmälningarna inte läggs ner med hänvisning till att den anmälda händelsen inte utgjorde ett brott. Som nämnts tidigare beror detta bland annat på att dessa utredningar inte står inför samma utredningssvårigheter som andra typer av dataintrång när det gäller förutsättningarna för att identifiera en misstänkt person och samla in bevisning som kan koppla den misstänkte till brottshändelsen.

En del av de brott som sker via intrång i sociala medie- och andra e-tjänstkonton är också kopplade till den organiserade cyberbrottsligheten i och med att intrången används som ett led i exempelvis nätfiske- eller bedrägeriupplägg. Brås senaste fördjupningsstudie om bedrägeribrottsligheten (Brå 2016b) visade att dessa brott sällan ledde till personuppklaring, främst på grund av samma typer av utredningssvårigheter som lyfts av intervjupersonerna i denna rapport. Detsamma gäller de typer av

[41] Se till exempel SOU 2017:89, SOU 2017:100, Dir 2021:58.

dataintrång som används av privatpersoner som ett sätt att kränka eller begå brott som hot, ofredande eller ärekränkningsbrott, som Brå tidigare beskrivit i en rapport om hot och kränkningar via internet (Brå 2015).

I båda dessa rapporter drogs slutsatsen att omfattningen av dessa brottstyper, och de svårigheter som är kopplade till utredningsarbetet, innebär att det är orealistiskt att förvänta sig att de brottsbekämpande myndigheterna kommer kunna åstadkomma någon dramatisk ökning av personuppklaringsnivåerna för dessa brottstyper. Samtidigt lyftes en del utvecklingsområden som skulle ge bättre förutsättningar för utredningsarbetet, bland annat förbättrade möjligheter att snabbt inhämta och analysera digital information i utredningssyfte. Ett centralt återkommande tema i både dessa tidigare Bråapporter och den här rapporten är att tillgång till it-forensisk kapacitet och kompetens är en förutsättning för att driva framgångsrika brottsutredningar, vilket även gäller de flesta andra brottstyperna, då en mycket stor andel av samtliga brottsutredningar i dag måste kunna hantera och analysera digital bevisning (Brå 2016a).

Viktigt med uppmaningar och stöd för att skydda sig mot dataintrång

Mot bakgrund av de hot och skador som kopplas till dataintrångs-brottsligheten samt de svårigheter som kännetecknar utrednings- och lagföringsarbetet är det viktigt med uppmaningar och stöd till företag, organisationer och privatpersoner för att skydda sig mot dataintrång.

Även om dataintrångsbrottsligheten är varierad och komplex är en gemensam nämnare att gärningspersonerna utnyttjar sårbarheter i det digitala ekosystemet för att olovligen skaffa sig tillgång till olika digitala miljöer. En utmaning för det förebyggande arbetet är att det finns en stor variation även i dessa sårbarheter. Det kan handla om allt från säkerhetsluckor i datorsystem eller programvara till den mänskliga faktorn, till exempel att anställda missbrukar sina behörigheter, eller att personer använder osäkra lösenord eller luras till att lämna ifrån sig information som sedan kan användas för att få tillgång till en digital miljö, exempelvis ett företags datorsystem eller ett användarkonto på en mejl- eller sociala medietjänst. En annan viktig utmaning är också att föränderligheten i den digitala miljön och i gärningspersoners tillvägagångssätt innebär att det kontinuerligt uppstår både nya sårbarheter och nya sätt att utnyttja dem.

Olika aktörsgrupper har olika roller i det förebyggande arbetet

På samma sätt som vid brott mer generellt krävs en delaktighet från flera olika aktörsgrupper i det förebyggande arbetet mot dataintrång. För att jämföra med en mer traditionell motsvarighet till dataintrång drivs det förebyggande arbetet mot fysiska inbrott fram av bland annat privata aktörer som utvecklar och tillverkar mer inbrottssäkra fönster, dörrar och larmsystem, parallellt med att myndigheter och andra aktörer sprider rekommendationer om hur man skyddar sig mot inbrott, till exempel att man inte ska sprida information om när man kommer vara bortrest på sociala medier. Men för att dessa förbättringar ska få effekt på brottsligheten krävs också en delaktighet och engagemang från bostadsinnehavare och andra fastighetsägare. Dessa måste ta tillvara de skyddsmöjligheter och rekommendationer som utvecklas och finns tillgängliga – till exempel genom att installera mer inbrottssäkra dörrar och fönster, och att faktiskt låsa dem.

Som nämndes i inledningskapitlet finns det ett flertal offentliga aktörer som arbetar förebyggande mot cyberbrottslighet och andra former av cyberangrepp såväl på europeisk nivå (t.ex. Europeiska unionens cybersäkerhetsbyrå och Europol) som i Sverige (t.ex. FRA, Säpo och MSB), och det finns också ett stort antal privata aktörer som arbetar för att erbjuda ständigt uppdaterade digitala säkerhetslösningar för såväl privatpersoner som myndigheter och företag. Eftersom dataintrång spelar en central roll i förhållande till cyberangrepp har dessa aktörers arbete ett viktigt fokus på att försvåra och förebygga dataintrång, bland annat genom att bevaka utvecklingen samt identifiera och täppa till upptäckta säkerhetsluckor och därmed minska sårbarheter.

Brås kartläggning har inte haft fokus på att undersöka dessa offentliga och privata aktörers säkerhetsarbete eller vilka utvecklingsmöjligheter som finns i detta arbete. Däremot har en referensgrupp med representanter från både offentliga och privata datasäkerhetsaktörer knutits till arbetet i syfte att bland annat diskutera åtgärder för att förebygga dataintrång.

Samtliga internetanvändare har en nyckelroll

En viktig slutsats från Brås diskussioner med dessa experter, som också får stöd i forskningen (se t.ex. Graham och Triplett 2016, Back och LaPrade 2019), är att en central målsättning för det förebyggande arbetet bör vara att få flera internetanvändare att ta till sig de möjligheter som faktiskt finns för att skydda sig mot dataintrång. För att återgå till jämförelsen med fysiska

inbrott menar de säkerhetsexperter som Brå haft kontakt med att det redan i dag finns välutvecklade säkerhetslösningar och rekommendationer för att skydda sig mot digitala inbrott, men att många fortfarande inte ”låser dörren” eller lämnar sina digitala fönster öppna. De säkerhetslösningar och rekommendationer som löpande utvecklas och sprids av både privata och offentliga aktörer kan bara få effekt i den mån de faktiskt tillämpas av digitala användare.

För privatpersoner handlar det främst om att ha ett antivirusprogram på alla digitala enheter (som datorn, mobilen och surfplattan) för att skydda sig mot skadlig programkod. Det är även viktigt att kontinuerligt installera säkerhetsuppdateringar till operativsystem och andra programvaror när de görs tillgängliga, eftersom dessa uppdateringar tas fram just i syfte att täppa till tidigare okända sårbarheter i hård- och mjukvara som har upptäckts och som åtgärdas med hjälp av uppdateringarna. Ett ytterligare enkelt sätt att skydda sig är att ha långa och säkra lösenord till olika digitala tjänster och konton (till exempel i form av en mening som också innehåller en siffra och ett fråge- eller utropstecken), och att inte dela med sig av sina lösenord eller spara dem på ett sätt som möjliggör för andra att komma åt dem.

Det grundläggande skyddet mot dataintrång skulle stärkas ytterligare om fler följde befintliga rekommendationer för att minska risken för att oavsiktligt ladda ner skadlig kod eller lämna ifrån sig information som kan användas i brottsligt syfte. Här handlar det till exempel om att inte lämna ifrån sig personliga ekonomiska uppgifter, som kort- eller kontonummer, att inte klicka på misstänkta eller okända länkar och bifogade dokument i mejl samt att bara e-handla från betrodda företag.[42]

För myndigheter, företag och andra organisationer finns en lista på MSB:s webbplats med säkerhetsrekommendationer för att skydda sig mot cyberangrepp. Utöver att kontinuerligt installera säkerhetsuppdateringar rekommenderas bland annat att se till att behörigheter förvaltas på ett säkert sätt, att man tillämpar starka autentiseringsfunktioner, att man segmenterar nätverk och upprättar filtreringsfunktioner mellan olika nätverksdelar och att man ser till att obehörig och otillåten mjukvara inte används inom organisationens informationssystem. [43] Utöver de mer grundläggande

[42] För mer detaljer kring dessa och ytterligare rekommendationer se https://internetstiftelsen.se/tanksakert/

[43] Hela listan finns på: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/cyberhot/rekommenderade-sakerhetsatgarder/

tekniska skydden är det också viktigt att företagen utarbetar kontinuitetsplaner för hur verksamheten ska upprätthållas vid incidenter (som exempelvis driftstopp) samt cybersäkerhetsstrategier som en del av företagens cybersäkerhetsarbete (Franke 2020).

De befintliga åtgärderna och rekommendationerna kommer inte innebära ett komplett skydd mot dataintrång, men enligt både experter i Brås referensgrupp och forskning (se t.ex. Waldrop 2016, Maimon och Louderback 2019) skulle en betydande del av de dataintrång som sker i dag kunna förebyggas om fler tog till sig och följde dessa rekommendationer. Bland privatanvändare skulle det dessutom inte bara innebära ett ökat skydd för den enskilda användaren, utan även för användarens mejlkontakter och kontakter på sociala medier, då både denna rapport och tidigare Bråapporter (t.ex. Brå 2016b) visar att kapade mejl- och sociala mediekonton bland annat används i syfte att begå bedrägerier mot, och att lura till sig personlig information från, kontoinnehavarnas kontakter.

Information bör spridas på olika nivåer och anpassas till olika grupper

Informations- och utbildningsinsatser är en viktig åtgärd för att öka medvetenheten om hur man kan skydda sig mot dataintrång. En förutsättning för sådana insatser är att centrala aktörer i samhället prioriterar att denna information samlas och kontinuerligt uppdateras. Ett exempel på den här typen av arbete är ”Tänk säkert” som drivs i ett samarbete mellan MSB och Polisen. Bland annat sker en informationskampanj under oktober månad varje år, som är EU:s informationssäkerhetsmånad. Utöver MSB och Polisen deltar ett flertal samarbetspartner från privat, offentlig och ideell sektor i att sprida kampanjens budskap, till exempel Internetstiftelsen, Stöldskyddsföreningen, Sveriges kommuner och regioner och en del storföretag.[44] Informationen sprids bland annat på TV, i sociala medier och via olika webbplatser.[45]

Ett problem med generella informationskampanjer är att information i sig inte behöver innebära ett mer aktivt säkerhetstänk eller en förändring i beteende. Enligt forskning ökar dock sannolikheten att åstadkomma beteendeförändringar om informationsinsatser riktas på ett mer direkt och

[44] Under 2022 har MSB också haft ett särskilt regeringsuppdrag att genomföra en informationskampanj till företag och allmänheten om informations- och cybersäkerhet (Ju2022/01292).

[45] Se t.ex. https://tanksakert.sakerhetskollen.se/, https://internetstiftelsen.se/tanksakert/,

anpassat sätt till olika målgrupper (Brady och Heinl 2020). Av denna anledning är det viktigt att även andra aktörer tar den information som finns samlad och anpassar och sprider den till sina egna målgrupper, till exempel inom skolan och högskolesektorn, bransch- och intresseorganisationer samt enskilda företag och myndigheter. I och med att Brås granskning av de polisanmälda dataintrången också visar att intrång i bland annat sociala mediekonton används för att utöva kontrollerande beteenden samt begå brott som hot, ofredande och ärekränkningsbrott, i synnerhet bland kvinnor och unga, är det också viktigt att grupper som kommer i kontakt med brottsoffer, till exempel kvinno- och ungdomsjourer, också har förmågan att informera om hur man kan skydda sig mot dataintrång. Brås granskning visar också vikten av att förebyggande åtgärder mot bland annat mobbning, hot och ofredande tar hänsyn till att dessa handlingar ofta sker i en digital miljö samt att dataintrång används som ett verktyg i dessa sammanhang.

Referenser

Al-Musib, N.S., Al-Serhani, F.M., Humayun, M. och Jhanjhi, N.Z. (2021). Business email compromise (BEC) attacks. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.03.647

Back, S. och LaPrade, J. (2019). The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. *International Journal of Cybersecurity Intelligence & Cybercrime* 2(2), s. 1–4. https://www.doi.org/10.52306/02020119KDHZ8339

Brady, S. och Heinl, C. (2020). *Cybercrime: Current Threats and Responses. A review of the research literature*. Department of Justice and Equality; Dublin. Hämtad 2020-10-22 från: http://www.justice.ie/en/JELR/Pages/PR20000232.

Brottsförebyggande rådet, Brå (2013). *Bestämmelsen om kontakt med barn i sexuellt syfte*. Rapport 2013:14. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2015). *Polisanmälda hot och kränkningar mot enskilda personer via internet*. Rapport 2015:6. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2016a). *It-inslag i brottsligheten och rättsväsendets förmåga att hantera dem*. Rapport 2016:17. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2016b). *Bedrägeribrottsligheten i Sverige. Kartläggning och åtgärdsförslag*. Rapport 2016:9. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2018). *Personuppklaring i relation till förändrad brottsstruktur*. Kortanalys 1/2018. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2022). *Klassificering av brott. Anvisningar och regler*. Version 10.2, juli 2022. Stockholm: Brottsförebyggande rådet.

Centrum för cybersäkerhet, RISE (2022). Cyberhot mot Sverige. En sammanfattning för ledare och beslutsfattare. Hämtad 2022-09-01 från:

https://www.ri.se/sites/default/files/2022-09/Rapport%20Cybers%C3%A4kerhet.pdf

Den militära underrättelse- och säkerhetstjänsten, MUST (2022). *Årsöversikt 2021*. Hämtad 2022-07-01 från: https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/rapporter/musts-arsoversikt-2021-.pdf

Dir. 2021:58 *Datalagring vid brottsbekämpning – ytterligare åtgärder för en modern och ändamålsenlig reglering*. Stockholm: Justitiedepartementet.

Domenie, M.M.L., Leukfeldt, E.R., van Wilsem. J.A., Jansen, J. och Stol. W.Ph. (2013). *Victimisation in a Digitised Society: A Survey Among Members of the Public Concerning E-fraud, Hacking and Other High Volume Crimes*. Eleven international publishing.

Ds 2019:8 *Värnkraft – Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025*. Europarådets konvention om it-relaterad brottslighet (ETS 185).

ENISA (2021). *ENISA Threat Landscape 2021. April 2020 to mid-July 2021*. Hämtad 2022-09-28 från: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Europaparlamentets och rådets direktiv 2013/40/EU från den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF.

Europol (2018). *The Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: European cybercrime centre, Europol. Hämtad 2022-07-01 från: https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

Europol (2020). *The Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: European cybercrime centre, Europol. Hämtad 2022-07-01 från: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

Europol (2021). *The Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: European cybercrime centre, Europol. Hämtad 2022-07-01 från: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

Europol och Eurojust (2019). *Common challenges in combating cybercrime. Joint report, Europol och Eurojust Public Information*. Hämtad 2020-09-01 från: https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf

Federal Bureau of Investigation, FBI (2017). *Booter and Stresser Services Increase the Scale and Frequency of Distributed Denial of Service Attacks*. Publicerad: 17-10-2017. Hämtad 2019-07-09 från: https://www.ic3.gov/media/2017/171017-2.aspx

Franke, U. (2020). Cybersäkerhet för en uppkopplad ekonomi. *Entreprenörskapsforum*. Tryck: Örebro universitet.

Försvarets radioanstalt, FRA., m.fl. (2020). *Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden*. Hämtad 2022-06-16 från: https://www.msb.se/siteassets/dokument/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nationellt-center-for-cybersakerhet/rapport-cybersakerhet-i-sverige-2020--hot-metoder-brister-och-beroenden.pdf

Graham, R. och Triplett, R. (2016). Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization. *Deviant Behavior* 38, s. 1371–1382.

Hoque, N., Bhattacharyya, D.K. och Kalita, J.K. (2015). Botnet in DDoS attacks: trends and challenges. *IEEE Communications Surveys & Tutorials*. 17(4), s. 2242–2270. Doi:10.1109/COMST.2015.2457491.

Integritetskyddsmyndigheten, IMY (2021*). Integritetsskyddsrapport 2020 – redovisning av utvecklingen på it-området när det gäller integritet och ny teknik*. IMY rapport 2021:1. Hämtad från 2022-07-01 från: https://www.imy.se/globalassets/dokument/rapporter/integritetsskyddsrapport2020.pdf

Maimon, D. och Louderback, E.R. (2019). Cyber-Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology*. 2, s.191-216.

Myndigheten för samhällsskydd och beredskap, MSB (2022). *En inblick i Sveriges cybersäkerhet. Årsrapport it-incidentrapportering 2021*. MSB1913.

Hämtad 2022-09-29 från: https://www.msb.se/sv/publikationer/en-inblick-i-sveriges-cybersakerhet--arsrapport-it-incidentrapportering-2021/

Myndigheten för samhällsskydd och beredskap, MSB och CERT-SE (2019-11-20). *Ny våg av angrepp mot e-postkonton i Office 365 och Exchange.* Hämtad 2022-09-28 från: https://www.cert.se/2019/11/ny-vag-av-angrepp-mot-e-postkonton-i-office-365-och-exchange

Ojha, G. och Tak, G.K. (2012). A novel approach against e-mail attacks derived from user-awareness based techniques. *International journal of information technology convergence and services*, *2*(4). Hämtad 2022-07-01 från: https://arxiv.org/pdf/1209.2557.pdf

Paquet-Clouston, M., Haslhofer, B. and Benoit, D. (2019). Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity*. *5*(1). https://doi.org/10.1093/cybsec/tyz003

Polismyndigheten (2020). *Granskning av den it-forensiska verksamheten.* (Diarienummer: A482.094/2019).

Polismyndigheten, m.fl. (2019). *Myndighetsgemensam lägesbild om organiserad brottslighet*. Stockholm: Polismyndigheten. (Dnr: A457.772/2019). Hämtad 2022-07-01 från: https://polisen.se/siteassets/dokument/organiserad_brottslighet/myndighetsgemensam-lagesbild-om-organiserad-brottslighet-2019.pdf/download

Prop. 2006/07:66. *Angrepp mot informationssystem*. Stockholm: Justitiedepartementet.

Prop. 2013/14:92. *Skärpt straff för dataintrång*. Stockholm: Justitiedepartementet.

Prop. 2020/21:72. *Sveriges tillträde till Europarådets konvention om it-relaterad brottslighet*. Stockholm: Justitiedepartementet.

PTSFS 2019:2. *Post- och telestyrelsens föreskrifter om vilka andra uppgifter som ska lagras för att identifiera abonnent och registrerad användare vid användning av NAT-teknik*. Stockholm: Post- och telestyrelsen. Hämtad 2022-07-01 från: https://www.pts.se/globalassets/startpage/dokument/legala-dokument/foreskrifter/internet/ptsfs-2019_2_slutlig191212.pdf

Regeringsbeslut Fö2019/01330. *Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter*. Hämtad 2022-06-01 från: https://www.regeringen.se/4af5d9/globalassets/regeringen/dokument/forsvarsdepartementet/regeringsbeslut/uppdrag-om-fordjupad-samverkan-inom-cybersakerhetsomradet-genom-ett-nationellt-cybersakerhetscenter.pdf

Regeringsbeslut Ju2022/01292. *Uppdrag till Myndigheten för samhällsskydd och beredskap att genomföra en informationskampanj till allmänhet och företag om informations- och cybersäkerhet*. Hämtad 2022-05-30 från: https://www.regeringen.se/496aca/contentassets/cdfef170ee634fb6965c67e919a216a6/uppdrag-till-myndigheten-for-samhallsskydd-och-beredskap-att-genomfora-en-informationskampanj-till-allmanhet-och-foretag-om-informations--och-cybersakerhet.pdf

Riksrevisionen (2015). *It-relaterad brottslighet – polis och åklagare kan bli effektivare*. RiR 2015:21. Stockholm: Riksrevisionen.

Salahdine, F. och Kaabouch, N. (2019) Social engineering attacks: A survey. *Future Internet* 11(4), s. 89.

SOU 1992:110. *Information och den nya informationsteknologin – straff- och processrättsliga frågor m.m.* Betänkande av Utredningen om datastraffrätt.

SOU 2013:39. *Europarådets konvention om it-relaterad brottslighet*. Betänkande av Utredningen om it-brottskonventionen. Stockholm: Fritzes.

SOU 2017:89. *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet*. Stockholm: Fritzes.

SOU 2017:100. *Beslag och husrannsakan – ett regelverk för dagens behov. Betänkande av Beslagsutredningen*. Stockholm: Fritzes.

SOU 2022:19. *Utökade möjligheter att använda hemliga tvångsmedel. Delbetänkande av Utredningen om utökade möjligheter att använda hemliga tvångsmedel*. Stockholm: Fritzes.

Svenskt näringsliv (2021). *Företagen och it-säkerheten – hotbilder, motåtgärder och behov*. Publicerad 31 mars 2021. Hämtad 2022-07-01 från: https://www.svensktnaringsliv.se/bilder_och_dokument/rapporter/645tao_foretagen-och-it-sakerheten-hotbilder-motatgarder-och-behovpdf_1168795.html/F%25C3%2596RETAGEN+OCH+IT-

S%25C3%2584KERHETEN+%25E2%2580%2593+hotbilder%252C+mot%25C3%25A5tg%25C3%25A4rder+och+behov.pdf

Teknikföretagen (2019). *Cyberhoten. Så ser hotbilden och attackerna ut mot svenska teknikföretag*. Hämtad 2022-07-01 från: https://www.teknikforetagen.se/globalassets/rapporter/digitalisering/cyberhoten---sa-ser-hotbilden-och-attackerna-ut-mot-svenska-teknikforetag.pdf

van de Weijer, S.G.A., Leukfeldt, R. och Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*. 16(4), s. 486–508. https://doi.org/10.1177/1477370818773610

Waldrop, M.M. (2016). How to hack the hackers: the human side of cybercrime. *Nature* 533, s. 164–167.

Yar, M. och Steinmetz, K. (2019). *Cybercrime and Society*. London: Sage.

Bilageförteckning

Bilaga 1 Redovisning av resultat från granskningen av ärenden

Tabell 1. Fördelningen av antalet målsägare i ärendena, uppdelat på brottskod.

	Överbelastnings-attacker		**Skadlig kod**		**Sociala medier**		**Olovlig registerslagning**		**Övrigt**	
	Antal	Andel	Antal	Andel	Antal	Andel	Antal	Andel	Antal	Andel
En	26	96 %	154	99 %	116	97 %	60	61 %	116	97 %
Flera	1	4 %	1	1 %	4	3 %	18	18 %	2	2 %
Framgår ej							21	21 %	2	2 %
Totalt	*27*	*100 %*	*155*	*100 %*	*120*	*100 %*	*99*	*100 %*	*120*	*100 %*

Tabell 2. Fördelningen av juridisk person och privatperson i ärendena, uppdelat på brottskod.

	Överbelastnings-attacker		**Skadlig kod**		**Sociala medier**		**Olovlig registerslagning**		**Övrigt**	
	Antal	Andel	Antal	Andel	Antal	Andel	Antal	Andel	Antal	Andel
Juridisk person	15	56 %	114	74 %	2	2 %	12	12 %	25	21 %
Privatperson	11	41 %	41	27 %	118	98 %	68	69 %	94	78 %
Både och	1	4 %					1	1 %		
Framgår ej							18	18 %	1	1 %
Totalt	*27*	*100 %*	*155*	*100 %*	*120*	*100 %*	*99*	*100 %*	*120*	*100 %*

Tabell 3. Fördelningen av målsägares kön i ärendena, uppdelat på brottskod.

	Överbelastnings-attacker		**Skadlig kod**		**Sociala medier**		**Olovlig registerslagning**		**Övrigt**	
	Antal	Andel	Antal	Andel	Antal	Andel	Antal	Andel	Antal	Andel
Kvinna	4	15 %	14	9 %	74	62 %	26	26 %	53	44 %
Man	8	30 %	27	17 %	40	33 %	27	27 %	41	34 %
Både och					4	3 %	11	11 %		
Ej aktuellt/ Framgår ej	15	56 %	114	74 %	2	2 %	35	35 %	26	22 %
Totalt	*27*	*100 %*	*155*	*100 %*	*120*	*100 %*	*99*	*100 %*	*120*	*100 %*

Tabell 4. Fördelningen av minderåriga i ärendena, uppdelat på brottskod.

	Överbelastnings-attacker		**Skadlig kod**		**Sociala medier**		**Olovlig registerslagning**		**Övrigt**	
	Antal	Andel	Antal	Andel	Antal	Andel	Antal	Andel	Antal	Andel
Minderårig	1	4 %	3	2 %	16	13 %	7	7 %	3	3 %
Ej minderårig/ Framgår ej/ Ej aktuellt	26	96 %	152	98 %	104	87 %	92	93 %	117	98 %
Totalt	*27*	*100 %*	*155*	*100 %*	*120*	*100 %*	*99*	*100 %*	*120*	*100 %*

Samhällets digitalisering innebär stora möjligheter, men skapar också sårbarheter som kan utnyttjas av kriminella aktörer. En central brottstyp i detta sammanhang är dataintrång, som kan handla om allt från att kapa någons sociala mediakonto till att olagligen få tillgång till myndigheters eller företags datorsystem i syfte att exempelvis stjäla kundinformation eller kryptera information i utpressningssyfte.

Med utgångspunkt i intervjuer och polisanmälningar beskriver denna rapport dels de typer av dataintrång som anmäls till polisen, dels de problem och utmaningar som rättsväsendets aktörer möter i sitt arbete med att utreda och lagföra brotten.

Rapporten vänder sig i första hand till polis och åklagare men även till forskare och övriga intresserade inom rättsväsendet.

brå

Brottsförebyggande rådet/National Council for Crime Prevention

Box 1386/Tegnérgatan 23, SE-111 93 STOCKHOLM
Tel +46 (0) 8 527 58 400, info@bra.se, www.bra.se

urn:nbn:se:bra-1074