Bedrageri mot næringslivet

NTAES – Nasjonalt tverretatlig analyse- og etterretningssenter – 2019

Utgitt: Februar 2019
Utgitt av: Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES)
Kontakt: post@ntaes.no
Postadresse: c/o ØKOKRIM, Postboks 2096 Vika, NO-0125 Oslo
Besøksadresse: C. J. Hambros plass 2, 0164 Oslo

Illustrasjoner / Grafisk design: ØKOKRIM

1 SAMMENDRAG

Bedragerianmeldelser har økt

Antall bedragerianmeldelser har økt med 36 prosent i Norge de ti siste årene. I samme periode har antall anmeldte lovbrudd gått ned 20 prosent. I 2018 ble det anmeldt 22 525 bedragerier. I omtrent 10 prosent av disse anmeldelsene er et privat foretak registrert som den fornærmede.

Høye mørketall, lav anmeldelsestilbøyelighet

Det er trolig svært høye mørketall knyttet til økonomisk- og digital kriminalitet rettet mot næringslivet. Lav oppklaringsprosent ved bedragerier, opplevelsen av at det er ressurskrevende å anmelde samt manglende mulighet til å få tilbake det økonomiske tapet, medfører at mange ikke anmelder. Frykt for tap av omdømme dersom bedrageriet gjøres kjent, bidrar ytterligere til lav anmeldelsestilbøyelighet.

Kortbedrageri og investeringsbedrageri medfører størst potensielt tap

Basert på tilgjengelige tall, og målt på *estimert angrepssum* for 2018, utpeker kortbedrageri hvor kortet ikke er tilstede og investeringsbedrageri seg som bedrageriformene med størst potensielt tap. Dernest kommer fakturabedrageri og direktørsvindel.

Små og mellomstore foretak er særlig utsatt

Forsøk på bedrageri og digitale angrep rammer alle typer virksomheter. Hvorvidt forsøket lykkes, beror på foretakets håndteringsevne. Store selskap har ressurser og kapasitet til å prioritere sikkerhetsarbeidet. Dette bidrar til at bedrageriforsøk og dataangrep avverges. Små og mellomstore foretak mangler ofte kunnskap og kapasitet til å sikre seg mot kriminalitet. Samtidig blir trusselaktører som foretakene står overfor stadig mer profesjonelle og målrettede.

Kriminelle manipulerer ansatte for å skaffe seg tilgang til foretakets systemer, verdier eller informasjon

Det er estimert at 90 prosent av all hacking som lykkes globalt stammer fra e-poster med formål om å manipulere mottakeren til å utføre en handling, såkalt phishing. Dette foregår ofte ved at en ansatt åpner vedlegg i e-post som er infisert med skadevare, eller følger en lenke til en kompromittert nettside. Slikt datainnbrudd kan gi tilgang til

systemer, informasjon og verdier som senere utnyttes i forbindelse med sosial manipulasjon, til å gjennomføre databedrageri eller drive utpressing overfor foretaket.

Næringslivet utsatt for både massebedrageri og målrettede angrep

Phishing-kampanjer og fakturabedrageri med utsendelse av et stort antall likelydende fakturaer er eksempler på massebedragerier. De aller fleste bedrageriformer rettet mot næringslivet er imidlertid mer tilpasset et bestemt mål. Direktørsvindel, kapret faktura og nettbankbedrageri er eksempler på modus som krever særlig tilpasning.

Kriminelle kartlegger foretaket digitalt

Målrettede angrep fordrer i mange tilfeller at gjerningspersonene gjør seg kjent med foretaket før bedrageriet utføres. Digital kartlegging av foretaket gjøres for eksempel ved besøk på foretakets nettside, kartlegging av ansatte på sosiale medier, eller ved installasjon av skadevare i foretakets e-post-system. Sistnevnte muliggjør overvåking og/eller videresending av e-post til gjerningspersonen.

Kriminelle aktører – både enkeltpersoner og organiserte kriminelle

Den typiske bedrageren av næringslivet er en mann på 36 år, uten arbeid og uten ledende rolle i næringslivet. Avhengig av modus er aktørene dels norske statsborgere, dels utenlandske. Sistnevnte er ofte del av en organisert kriminell gruppering, og er i liten grad representert i det norske straffesaksregisteret i forbindelse med bedrageri.

Digital utvikling stiller større krav til datasikkerhet

Høye forventninger til brukervennlige og raske løsninger gjør at foretak ofte må avveie brukervennlighet mot kontrollmekanismer. Vektes brukervennlighet for høyt i forhold til sikkerhet øker sårbarheten for bedrageri og dataangrep. Samtidig øker forekomsten av digital kriminalitet hvilket medfører økt krav til datasikkerhet hos foretak i norsk næringsliv, både av tekniske sikkerhetsløsninger og interne rutiner. Mange foretak er ikke rustet for å imøtegå den digitale kriminaliteten.

Saker sees i varierende grad i sammenheng av politiet

Politiet ser i begrenset grad et anmeldt bedrageri i sammenheng med bedragerianmeldelser i andre politidistrikt. Konsekvensen kan bli at sakens fulle bredde ikke belyses. Å se sakene i sammenheng, både for å avdekke og for å forebygge, er en forutsetning for å bekjempe systematiske bedragerier.

Hverken politi eller næringsliv har fullstendig oversikt over omfang og modus

Det finnes ingen nasjonal oversikt over antall utførte bedrageri i Norge, eller hvilke modus som til en hver tid er mest fremtredende. Kunnskapen er fragmentert. Politi og næringslivsaktører er gjensidig avhengig av hverandres informasjon for å bekjempe bedrageri mot næringslivet. Det er behov for samlet kunnskap for å forebygge, se saker i sammenheng og prioritere egnede saker.

Forebygging – andre land har flere verktøy enn Norge

Som en erkjennelse av at det strafferettslige sporet ikke er tilstrekkelig for å bekjempe bedragerier, har myndighetene både i Sverige og Storbritannia styrket forebyggende innsats og initiert utstrakt samarbeid mellom politi og næringsliv.

1 Sammendrag 3

Innledning 6

2 Metode og data 7
2.1 Datagrunnlag 7
2.2 Kvalitativ metode 8

3 Bedrageri i lovens forstand 9

4 Omfang og utvikling 10
4.1 Den registrerte kriminaliteten 10
4.2 Mørketall 15
4.3 Transaksjoner i banksystemet som kan knyttes til bedrageri 16

5 Sosial manipulasjon 20

6 Databedrageri og forholdet til datakriminalitet 25

7 Modus 28
7.1 Direktørsvindel 28
7.2 Nettbankbedrageri 30
7.3 Fakturabedrageri 32
7.4 Kreditt- og lånebedrageri 37
7.5 Kortbedrageri 39
7.6 Investeringsbedragerier 41
7.7 Telekommunikasjonsbedrageri – manipulering av anropstrafikk 43
7.8 Manipulering av strømmetjenester 45

8 Digitale angrep – ikke alt er bedrageri 47
8.1 Utpressing etter datainnbrudd 47
8.2 Datatrafikk som verktøy 48

9 Kjennetegn ved gjerningspersoner 49
9.1 En typisk bedrager 49
9.2 Løs tilknytning til arbeidslivet 50
9.3 Ledende roller 53

10 Kjennetegn ved fornærmede 55

11 Næringslivets rolle 56

12 Politiets straffesaksbehandling av bedrageri 58

INNLEDNING

Nasjonalt tverretatlig analyse- og etterretningssenter ble i mars 2018 gitt i oppdrag av Det sentrale samarbeidsforum å kartlegge bedrageri mot næringslivet i Norge. Bakgrunnen for oppdraget var den omfattende økningen av anmeldte bedragerier i både Sverige og Danmark. Som en konsekvens av økningen ble det gjennomført offentlige utredninger om bedragerier i Sverige. Utredningene ble iverksatt for å øke kunnskapen i politi og næringsliv og for å iverksette tiltak. En lignende kartlegging er ikke foretatt i Norge.

Formålet med rapporten er å beskrive registrert omfang og utvikling av bedragerier mot næringslivet. Den beskriver gjerningspersoner og fornærmede, ulike modus, næringslivets rolle og politiets håndtering.

2 METODE OG DATA

For at et bedrageri skal bli registrert er det en forutsetning at bedrageriet er oppdaget og forstått som en straffbar handling. Videre må forholdet være anmeldt til politiet. Et ukjent antall bedragerier blir aldri anmeldt. Anmeldelser gir dermed ikke et helhetlig bilde av det totale antallet bedragerier som utføres i Norge.

Kvalitative og kvantitative metoder er benyttet ved utarbeidelse av rapporten. Med «næringsliv» forstås foretak i privat sektor som produserer varer og tjenester med formål om å skape profitt. Analysen er primært utført med tanke på bedrageri mot foretak som er registrert i Norge, og som har virksomhet i Norge.

2.1 DATAGRUNNLAG

Både i analysen av omfang og utvikling, og analysen av kjennetegn ved gjerningspersoner og fornærmede, er anmeldelser av bedrageri lagt til grunn. Det er imidlertid noen forskjeller i hvilke koder fra politiets straffesaksregister (PAL Strasak) som legges til grunn for bedrageri i de to analysene.

Analysene tar på ulike måter også i bruk koder fra straffelovens kapittel om *Vern av informasjon og informasjonsutveksling*, som inneholder straffebestemmelser for ulike typer datakriminalitet. Dette gjelder datainnbrudd og identitetstyveri, som ofte er å finne i bedragerisammenheng. Undersøkelser av straffesaker som er registrert på straffesakskoder i nevnte kapittel viser at bedragerisaker i noen tilfeller blir registreres der.

2.1.1 Omfang og utvikling

I kapittelet *Omfang og utvikling* er antall bedragerianmeldelser hentet fra Statistisk sentralbyrå (SSB) for bedragerikoder frem til og med 2017. Anmeldelsestall for 2018 er basert på JUS065 i Pal Strasak.

Det er benyttet eget uttrekk i undersøkelse av underliggende fornærmedeforhold i anmeldelsene. Antall anmeldelser oppgitt kan derfor avvike noe fra egne uttrekk.

Ved undersøkelse av fornærmedeforhold i anmeldelsene er det sortert ut antall fornærmede per fødselsnummer og per organisasjonsnummer. Det innebærer at saker hvor det ikke er registrert en fornærmet part faller utenfor analysen. Fornærmedes organisasjonsnummer er sammenstilt mot Enhetsregisteret for å undersøke hvorvidt de er registrert som offentlig eller privat foretak.

2.1.2 Kjennetegnsanalysen

I kapitlene *Kjennetegn ved gjerningspersoner* og *Kjennetegn ved fornærmede* er statistikkgruppene for bedragerier, og koder underlagt straffelovens kapittel *Vern av informasjon og informasjonsutveksling* slått sammen i analysen.[1] Dette innebærer en viss risiko for at utvalget inneholder enkelte saker som ikke inneholder bedragerielementer. Ved å ekskludere disse sakene vil imidlertid en vekslende andel av bedragerisaker bli

1 Statistikkgruppene 2602, 2603, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2666, 2667, 2670, 2671, 0351, 0352, 0353, 0354, 0355, 0356, 0357, 0358, 0362, 0398. Vi gjør robusthetsanalyser hvor noen av disse statistikkgruppene er ekskluderte, for å undersøke om avgrensningen påvirker konklusjonene.

holdt utenfor.[2] Statistikkgruppene for bedragerier utgjør 86 prosent av det endelige utvalget.

Analysen av kjennetegn ved gjerningspersoner er basert på registerdata på person og foretaksnivå fra politiet koplet sammen med opplysninger fra Enhetsregisteret, Folkeregisteret og Arbeidstaker- og arbeidsgiverregisteret. Utvalget av gjerningspersoner består av mistenkte, siktede og domfelte i bedragerisaker og utvalgte strasak-koder underlagt kapittel om Vern av informasjon og informasjonsutveksling. Utvalget er begrenset til saker hvor gjerningsperson er kjent. Videre er det et kriterium at fornærmet i saken er registrert med et organisasjonsnummer. Det skilles ikke her på private og offentlige foretak. Med «næringsliv» menes her både foretak i privat og offentlig sektor.

En annen begrensning er at politiet ikke registrerer D-numre på samme måte som fødselsnumre i politiets saksbehandlingssystem.[3] Dette skaper skjevheter, og medfører at gjerningspersoner som oppholder seg midlertidig i landet ikke inngår i analysen.

Analysen av kjennetegn ved fornærmede er basert på registerdata fra politiet, koplet sammen med data fra Enhetsregisteret.

2.2 KVALITATIV METODE

Den kvalitative delen beskriver systematiske bedragerier som begås mot næringslivet.

Med systematiske bedragerier menes bedragerier som begås av en aktør eller et nettverk gjentatte ganger mot flere mål, og med lik fremgangsmåte eller modus.[4] Systematiske bedragerier består altså av flere separate bedragerier. Først når likhetstrekk mellom bedragerier oppdages, avdekkes det om de er systematisk utført.

Med fokus på systematiske bedragerier utelukkes bedragerier begått av personer ved enkelttilfeller i den kvalitative analysen. Dette kan for eksempel være personer som unnlater å betale for en drosjetur eller hotellovernatting, eller forsikringsbedrageri. Sistnevnte tilfeller inngår i den *kvantitative* analysen.

Det er foretatt seks intervjuer og enkelte mer uformelle samtaler med fagpersoner i politi, næringslivsorganisasjoner og bank. Flere av intervjuobjektene har etterforsket bedragerisaker, innehar stillinger hvor de på andre måter avdekker bedrageri eller representerer medlemmer som er utsatt for bedrageri.

Straffesakskoder sier ikke nødvendigvis så mye om fremgangsmåter ved bedragerier. Dommer og enkelte straffesaker som omhandler bedrageri mot næringslivet er gjennomgått for å gi en mer utfyllende beskrivelse av fremgangsmåter.

---

2 Den vekslende tilbøyeligheten til å registrere bedragerier mot næringslivet som henholdsvis bedragerier og datakriminalitet skaper skjevheter som vil kunne gi utslag på resultatet av analysen.

3 D-nummer er et midlertidig identitetsnummer som kan tildeles utenlandske personer som i utgangspunktet skal oppholde seg i Norge mindre enn seks måneder.

4 Begrepet massebedrageri er vurdert til ikke å være dekkende nok da modus som bærer preg av en mer individuell tilpasset målutvelgelse (som eksempelvis direktørsvindler) faller utenfor.

3 BEDRAGERI I LOVENS FORSTAND

Bedrageri straffes etter straffeloven[5] (strl.) § 371, med strafferamme på inntil to år. Et bedrageri innebærer at noen, med *forsett om vinning* for seg eller andre, *forleder* noen til å *gjøre noe*, eller *unnlate å gjøre noe* som medfører et *tap* for vedkommende eller andre. Forledelsen følger av at lovbryter *fremkaller*, *styrker* eller *utnytter* en villfarelse.

Bedrageribestemmelsen skiller på *bedrageri* og *databedrageri. Bedrageri*, jf. strl. § 371(a), begås i en sosial situasjon. Handlingen begås overfor en person som forledes fordi lovbryteren gir uriktige opplysninger, eller unnlater å gi eller korrigere opplysninger som vedkommende vet er motiverende for den annen part.[6] Ved *databedrageri* foretar lovbryteren en handling *overfor et datasystem*, jf. § strl. 371(b).

For at bedrageriet skal være fullbyrdet må handlingen volde «tap eller fare for tap for noen». Tapet må være av økonomisk art. Det vil si at «den aktuelle gjenstanden» må ha en viss omsetnings- eller bruksverdi.

Grovt bedrageri straffes etter strl. § 372 og har en strafferamme på fengsel inntil seks år. Ved avgjørelse av om bedrageriet er grovt skal det særlig legges vekt på om

a) det har hatt til følge en betydelig økonomisk skade[7],
b) det er voldt velferdstap eller fare for liv eller helse,
c) det er begått ved flere anledninger eller over lengre tid,
d) det er begått av flere i fellesskap eller har et systematisk eller organisert preg,
e) lovbryteren har foregitt eller misbrukt stilling, verv eller oppdrag,
f) det har ført eller utarbeidet uriktige regnskaper eller uriktig regnskapsdokumentasjon, eller
g) lovbryteren har forledet allmennheten eller en større krets av personer

Mindre bedrageri straffes med bot etter strl. § 373.[8]

Bedrageribestemmelsen § 371

Med bot eller fengsel inntil 2 år straffes den som med forsett om å skaffe seg eller andre en uberettiget vinning

a. fremkaller, styrker eller utnytter en villfarelse og derved rettsstridig forleder noen til å gjøre eller unnlate noe som volder tap eller fare for tap for noen, eller
b. bruker uriktig eller ufullstendig opplysning, endrer data eller datasystem, disponerer over et kredittkort eller debetkort som tilhører en annen, eller på annen måte uberettiget påvirker resultatet av en automatisert databehandling, og derved volder tap eller fare for tap for noen.

5 Lov av 20. mai 2005 nr. 28 om straff (straffeloven).

6 Sunde, Inger Marie (2016) *Datakriminalitet* kapittel 7.1 s. 118.

7 Det følger av Norsk Lovkommentar (sist hovedrevidert 1.7.2018) at det ikke er mulig å angi nøyaktig hvor stort beløpet må være for å regnes som «betydelig», men at det må antas at grensen i dag må trekkes ved ca. kr. 100 000.

8 Veiledende verdigrense for «ubetydelig verdi» er ca. kr. 2 000, ref. HR-2018-1160-A

4 OMFANG OG UTVIKLING

4.1 DEN REGISTRERTE KRIMINALITETEN

Det anmeldes generelt færre straffbare forhold nå enn tidligere. Dette gjelder derimot ikke bedrageri – som øker. Hvilke former for bedragerier blir hyppigst anmeldt – og hvem er de fornærmede? I rapporten er omfanget av bedragerianmeldelser og fornærmede undersøkt. I tillegg er enkelte kriminalitetstyper knyttet til straffelovens kapittel Vern av informasjon og informasjonsutveksling inkludert – da dette er kriminalitet som ofte gjennomføres i sammenheng med bedragerier begått i det digitale rom.

4.1.1 Antall anmeldte bedragerier øker

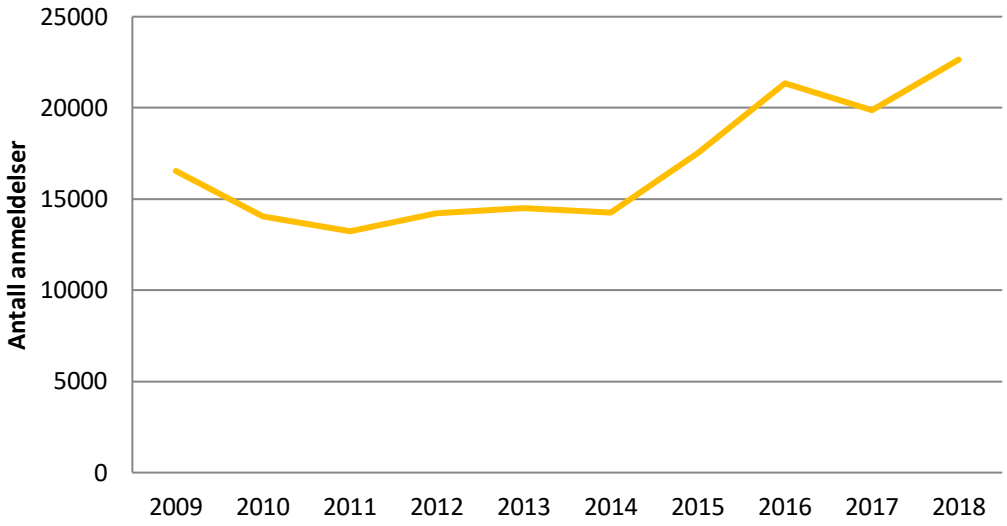
Som vist i figur 1 ble det anmeldt 22 525 bedragerier i Norge i 2018.[9] Det tilsvarer en økning på 36 prosent de ti siste årene. I samme periode var det nedgang på 20 prosent i antall anmeldte lovbrudd totalt. Innføringen av ny straffelov av 2005 vanskeliggjør sammenligning av antall anmeldelser før og etter ikrafttredelsen 1. oktober 2015. Den markante økningen fra 2014 til 2016 skyldes med all sannsynlighet endringer i registreringskoder som følge av den nye straffeloven. Mindre bedrageri, samt forsøk på bedrageri og forsøk på grovt bedrageri, ble lagt til som egne lovbestemmelser, mens andre ble opphevet.[10]

Politireformen med virkning fra 1. januar 2016 kan ha medført restanser i registreringen av anmeldelser og kan være en medvirkende årsak til nedgangen i antall anmeldelser registrert mellom 2016 og 2017. Utviklingen i antall bedragerianmeldelser synes å være stabil fra 2016–2018.

---

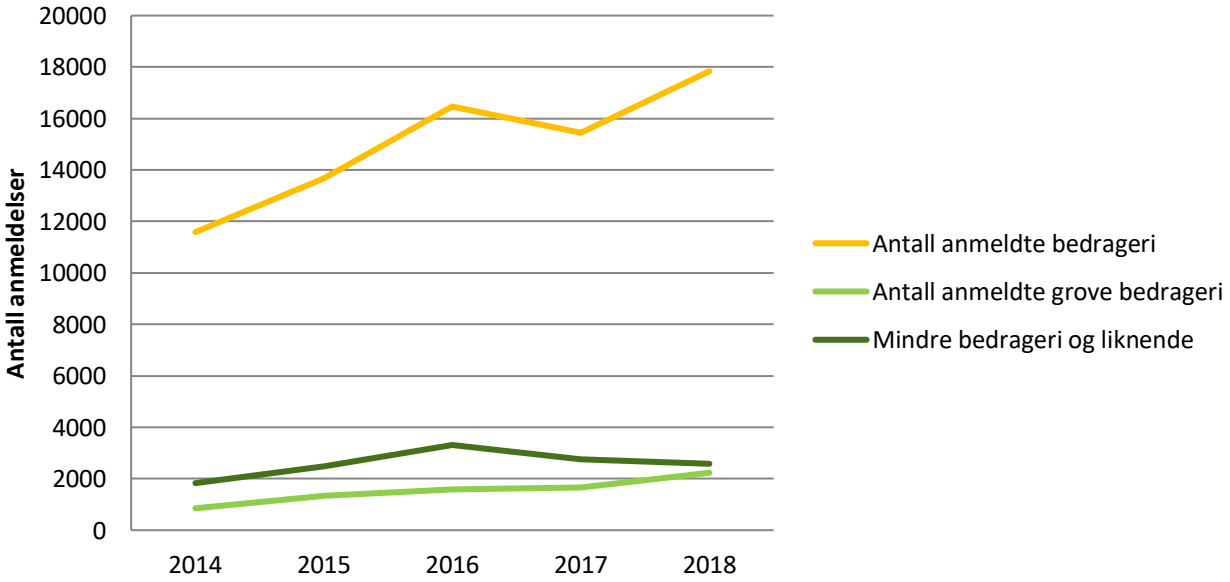
9 Kilde for datagrunnlaget 2009-2017: SSB Tabell 08484. *Antall anmeldte lovbrudd. Absolutte tall*. Datagrunnlag for 2018: JUS 065 på koder: 4301, 4302, 4303, 2601, 2602, 2603, 2607, 2608, 2609, 2610, 2611, 2612, 2615, 2616, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2699. Kodene er tilsvarende de SSB bruker.

10 Politidirektoratet: *Strasakrapporten. Anmeldt kriminalitet og politiets straffesaksbehandling. Første og andre tertial 2018,* s. 32



Figur 1: Antall anmeldte bedragerier 2009-2018

Figur 2[11] viser antall anmeldte bedrageri, fordelt på kategoriene mindre bedrageri og lignende, bedrageri og grovt bedrageri i perioden 2014-2018. Anmeldelser av grovt bedrageri øker mest i undersøkelsesperioden fra 850 anmeldelser i 2014 til 2 219 i 2018. Dette tilsvarer en økning på hele 161 prosent. Det er likevel anmeldelser av alminnelig bedrageri som øker mest i antall, fra 11 585 i 2014 til 17 740 anmeldelser i 2018. Dette tilsvarer en økning på 53 prosent.



Figur 2: Antall anmeldte bedragerityper 2014-2018

11 Kilde for datagrunnlaget 2014-2017: SSB Tabell 08484. Antall anmeldte lovbrudd. Absolutte tall. Datagrunnlag for 2018: JUS 065

4.1.2 Fornærmede i bedragerisaker

Kun én av ti fornærmede i bedragerisaker i årene 2015 til 2018 er private foretak. I 2018 utgjorde dette 2 460 private foretak av totalt 21 915 fornærmede. Andelen fornærmede private foretak gikk ned to og et halvt prosentpoeng fra 2016 til 2018. Forholdet mellom antall fornærmede personer, offentlige- og private foretak synes å være stabil i perioden. Det er vanskelig å si om fordelingen gjenspeiler virkeligheten. En mulig feilkilde kan være at anmeldelser feilaktig registreres med navn og fødselsnummer til personen som representerer foretaket når anmeldelse inngis på vegne foretaket. Flere foretak er ikke registrert med organisasjonsnummer da dette ikke er påkrevd i saksbehandlingssystemet til politiet.[12,13,14]

4.1.3 Andelen av private foretak øker med alvorlighetsgrad og ved bedrageriforsøk

I figur 3[15] fremgår det at andel private foretak er høyere ved *forsøk* på bedrageri enn ved gjennomført bedrageri, og at andelen private foretak øker med alvorlighetsgraden av bedrageriet.

Hele 60 prosent av de fornærmede ved forsøk på grovt bedrageri er private foretak. Til sammenligning utgjør private foretak 37 prosent av de fornærmede ved anmeldte grove bedragerier. Den samme tendensen er tydelig ved alminnelige bedragerier. Private foretak utgjør 28 prosent av de fornærmede ved bedrageriforsøk, mens ved fullendte bedragerier er andelen gått ned til 7 prosent. Kun fire prosent av fornærmede ved mindre bedrageri er private foretak.

Det ble anmeldt kun 147 forsøk på grovt bedrageri i 2018 og derfor vil små endringer i sammensetningen av private foretak og andre grupper fornærmede kunne medføre store prosentvise endringer.

En mulig forklaring til at tilbøyeligheten til å anmelde forsøk er høyere blant private foretak, er at foretaket, ved å anmelde, viser at de har avdekket bedrageriet *før* det medførte tap. Motsatt kan lavere tilbøyelighet til å anmelde fullendte bedrageri forklares med at foretak ikke vil synliggjøre at foretaket har blitt lurt fordi det kan eksponere manglende sikkerhetsrutiner og svekke foretakets omdømme.

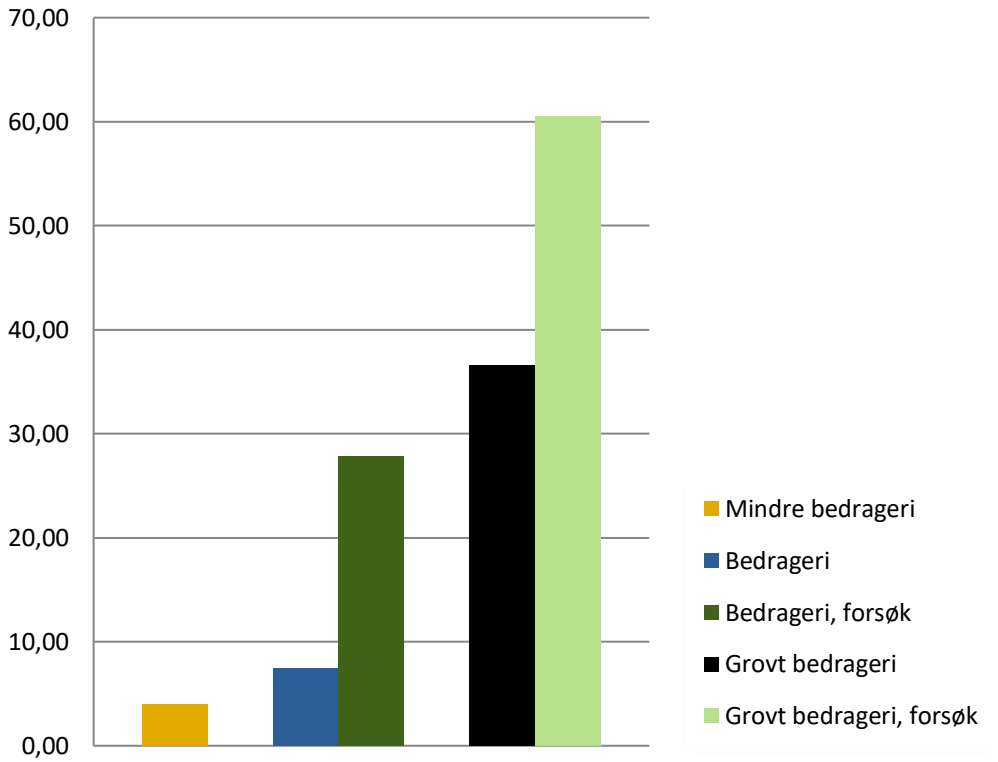
---

12 Datagrunnlaget er basert på uttrekk fra Pal Strasak i januar 2019

13 Foretak registrert med organisasjonsnummer er koblet til Enhetsregisteret for å undersøke hvilken enhetstypegruppe de kategoriserer under. Offentlig forvaltning (OFORV) og offentlig virksomhet (OVIRK) er lagt til grunn for offentlige foretak. I den grad offentlige foretak er registrert med en annen enhetstype er dette ikke fanget opp. De resterende kategoriene defineres som private foretak. En liten andel av de fornærmede er hverken registrert med fødselsnummer eller organisasjonsnummer og er derfor ikke inkludert i tabellen nedenfor.

14 Kilde: Uttrekk i Pal Strasak på forhold i utvalgte bedragerisaker januar 2017. Strasak-koder: 2601, 2602, 2603, 2608,2612,2615,2616, 2651, 2652, 2653, 2654, 2655, 2656 og 2661.

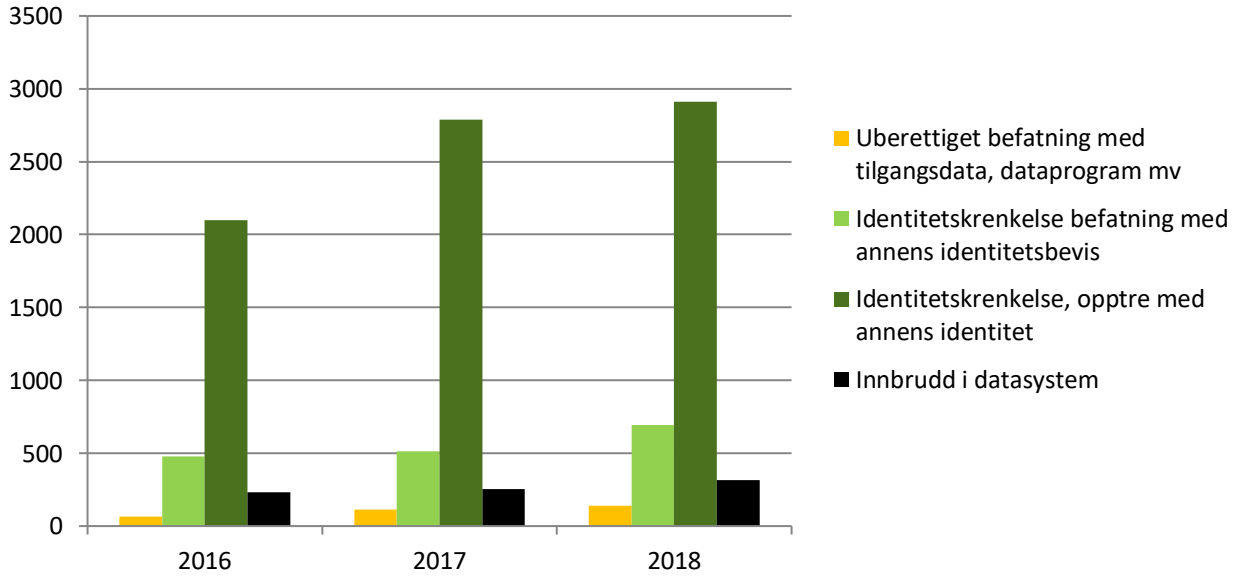
15 Kilde: Uttrekk i Pal Strasak på forhold i utvalgte bedragerisaker januar 2017. Strasak-koder: 2601,2602, 2603, 2608, 2612, 2651,2652, 2653, 2654, 2655.



Figur 3: Prosentandel av private foretak som fornærmet i 2018.

4.1.4 Vern av informasjon og informasjonsutveksling

Antall anmeldelser for et utvalg av lovbruddstyper underlagt straffelovens kapittel 21, Vern av informasjon og informasjonsutveksling, fremgår av figur 4. Kapittelet inneholder blant annet straffebestemmelser knyttet til ulike former for datakriminalitet. Noen av disse er straffbare handlinger som ofte utføres i forbindelse med bedrageri.



Figur 4: Antall anmeldelser 2016–2018 for utvalgte koder.

Stikkprøver på straffesaker som er registrert på lovbruddstyper i kapittel 21, viser at særlig følgende typer lovbrudd opptrer i forbindelse med-, eller forveksles med bedrageri;

- Uberettiget befatning med tilgangsdata, dataprogram mv,
- Identitetskrenkelse ved *befatning* med annens identitetsbevis
- Identitetskrenkelse ved *bruk* av annens identitetsbevis
- Innbrudd i datasystem

Eksempler på lovbrudd registrert under disse straffebestemmelsene er business email compromise, hacking med tap av informasjon, innlogging med annen persons brukeridentitet for så å endre informasjon i datasystem, og kortbedrageri ved såkalt *card not present*. Datainnbrudd med hensikt å stjele eller kopiere informasjon er en velkjent inngang for senere bedragerier eller sosial manipulasjon. Tilsvarende er endring av informasjon i datasystem potensielt nært forbundet med et databedrageri. Omfang og utvikling for ovennevnte straffebestemmelser er derfor inntatt i rapporten.

Figur 4 viser at samtlige av utvalgte lovbruddstyper har økt i løpet av treårsperioden. Det er relativt få anmeldelser i datagrunnlaget. Unntaket er *identitetskrenkelse ved å opptre med en annens identitet* som i 2018 utgjorde 2 910 anmeldelser, og som har økt med 39 prosent fra 2016 til 2018. Det å opptre med en annens identitet er et sentralt element ved kredittbedragerier som utføres i andres navn.

Antall anmeldelser i de andre bestemmelsene er få og selv små endringer kan gi store prosentvise utslag. Uberettiget befatning med tilgangsdata eller dataprogram har økt mest med hele 120 prosent på tre år, fra 64 saker i 2016 til 141 saker i 2018. *Tilgangsdata* er data som kan fungere som sikkerhet for konfidensialitet og som mekanisme for autentisering, eksempelvis brukernavn og passord til en PC, kodenøkler til krypterte filer, tilgangsdata for innlogging til nettbankkonto eller PIN-kode til vern av mobiltelefon eller nettbrett.[16]

Befatning med annens identitetsbevis har økt med 46 prosent i perioden, fra 476 saker i 2016 til 694 saker i 2018. Innbrudd i datasystem har økt med 35 prosent, fra 234 saker i 2016 til 316 saker i 2018.[17]

4.1.5 Trolig høye mørketall knyttet til datainnbrudd

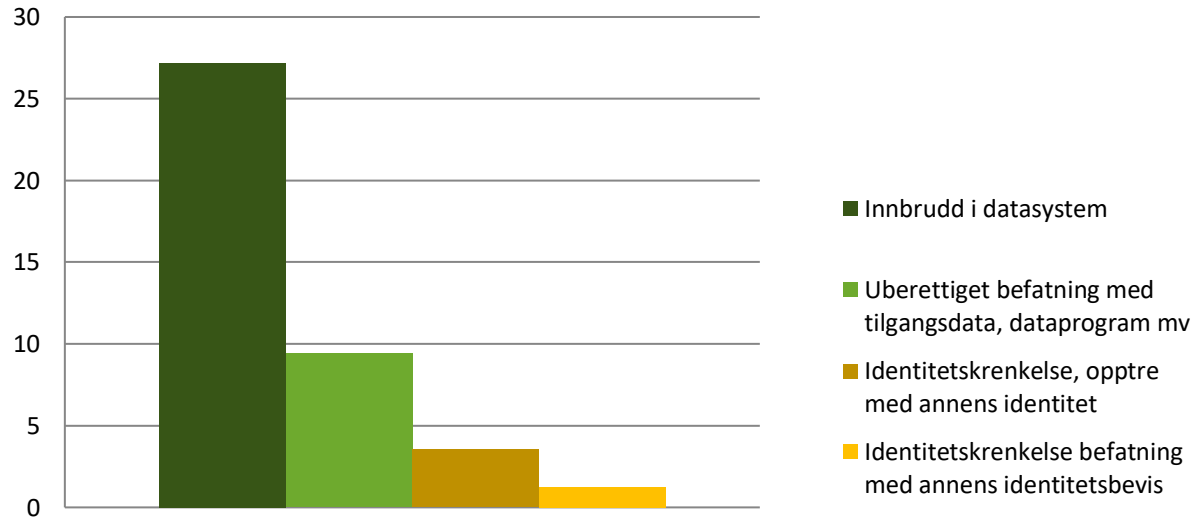
Private foretak utgjør 27 prosent av de fornærmede ved anmeldte innbrudd i datasystem i 2018 (figur 5).[18] 86 av totalt 316 fornærmede er private foretak. Videre utgjør private foretak 9 prosent av de fornærmede ved uberettiget befatning med tilgangsdata eller dataprogram.

Datainnbrudd, og uvedkommendes befatning med foretakets lagrede tilgangsdata eller dataprogram, kan være vanskelig for foretaket å avdekke. Datainnbrudd oppdages i mange tilfeller lang tid etter at innbruddet har funnet sted, hvis det i det hele tatt avdekkes. Det er derfor potensielt høye mørketall knyttet til disse straffebestemmelsene, utover det som kan tilskrives generell lav anmeldelsestilbøyelighet. At kun 86 private foretak har anmeldt datainnbrudd i 2018 er svært få. 13 prosent av foretakene som

16 Sunde, Inger Marie (2016), *Datakriminalitet,* s. 156
17 Uttrekk fra Pal Strasak 23. januar 2019 på kodene 351, 352, 353 og 355.
18 Uttrekk fra Pal Strasak 23. januar 2019 på kodene 351, 352, 353 og 355.

deltok i mørketallsundersøkelsen 2018 svarte at de har vært utsatt for forsøk-, og 5 prosent svarte at de har vært utsatt for datainnbrudd/hacking i 2017.[19] Det er ingenting som tilsier at antall datainnbrudd skulle være kraftig redusert fra 2017 til 2018. Det følger imidlertid også av mørketallsundersøkelsen at bare 9 prosent av de som opplever sikkerhetsbrudd anmelder forholdet til politiet.

Private foretak utgjør mindre enn 4 prosent av de fornærmede ved identitetskrenkelser. Dette er naturlig da identitetstyveri hovedsakelig rammer privatpersoner. Det er imidlertid eksempler på at kriminelle urettmessig utgir seg for å representere et foretak, ofte med hensikt å oppnå kreditt overfor en forhandler eller kredittinstitusjon.



Figur 5: Prosentandel hvor private foretak er fornærmet i utvalgte kriminalitetstyper i 2018

4.2 MØRKETALL

Mange bedragerier blir ikke rapportert til politiet. Det er derfor vanskelig å anslå det faktiske omfanget av bedrageri mot næringslivet. Én av ti virksomheter forespurt i Kriminalitets- og sikkerhets-undersøkelsen i Norge 2017 anmeldte ikke lovbrudd de var utsatt for siste år.[20] Andelen har holdt seg stabil over flere år. Ved å se på hvilke typer kriminalitet virksomheter ikke anmelder utgjør økonomisk kriminalitet 16 prosent og kriminalitet i det digitale rom 10 prosent. Til sammenligning utgjør vinningskriminalitet 63 prosent av kriminaliteten som ikke anmeldes.

Registrering av lovbrudd i straffesaksregisteret avhenger av flere faktorer. For det første må det oppdages. Bedrageri handler om å forlede eller manipulere, og enkelte bedragerier oppdages aldri. Virksomheter uten styringssystem og sikkerhetsrutiner oppdager gjerne sikkerhetsbrudd ved en tilfeldighet.[21]

---

19 Næringslivets Sikkerhetsråd, Mørketallsundersøkelsen 2018, s. 20

20 Næringslivets sikkerhetsråd, *Kriminalitets- og sikkerhetsundersøkelsen i Norge 2017*, s. 34. Undersøkelsen kartlegger kriminalitet og sikkerhetsutfordringer i offentlig og privat sektor og bygger på svar fra et utvalg ledere og sikkerhetsansvarlige i 2000 private og 500 offentlige virksomheter. Se også Næringslivets sikkerhetsråd, *Mørketallsundersøkelsen 2018* s. 28.

21 Næringslivets sikkerhetsråd, *Mørketallsundersøkelsen 2018*. s. 21.

For det andre må bedrageriet *forstås* som noe kriminelt. Tolkningen av handlingen avgjør om bedrageriet er straffbart eller ikke. Selv om bedrageriforsøk er straffbart, oppleves det ikke alltid som noe kriminelt fordi fornærmede ikke har blitt frarøvet noe. Andre ganger kan ledelsen i et foretak tro at de står ovenfor et underslag fra en ansatt når det egentlig er en ansatt som er blitt lurt i en direktørsvindel. Dersom bedrageriet både er oppdaget og forstått som noe kriminelt gjenstår selve avveiningen av om forholdet skal rapporteres til politiet.

Oppfatningen i næringslivet er at politiet i stor grad henlegger saker, og at kriminelle som begår økonomisk kriminalitet ikke blir tatt.[22] Det er også en utbredt oppfatning i politi og næringsliv at det er for tungvint å anmelde kriminalitet til politiet. Tidligere var det nødvendig med påtalefullmakt for å anmelde et straffbart forhold på vegne av en virksomhet. Dette opphørte imidlertid ved ikrafttredelsen av ny straffelov av 2005. Flere av intervjuobjektene mener at anmeldelsestilbøyeligheten øker dersom virksomheter i stedet kan anmelde bedrageri og datakriminalitet til politiet på internett.

En annen årsak til at bedrageri og datakriminalitet ikke anmeldes av næringslivet er det dårlige omdømmet det kan påføre virksomheten. Å bli bedratt er en erkjennelse av å ha blitt lurt eller at sikkerhetsrutiner eller datasikkerhet er for dårlig.

Beløp som tapes kan også medvirke i avveiningen om bedrageriet skal anmeldes. Jo lavere beløp desto mindre sannsynlig er det at virksomheten anmelder forholdet.

4.2.1 Holdning til digital kriminalitet

Det viktigste for foretak som blir bedratt er å få pengene tilbake og hindre at de blir utsatt for lignende kriminalitet igjen. I dag stanses mange transaksjoner av norske bankers deteksjonssystemer. E-poster med skadevare filtreres ut og forsøk på datainnbrudd avdekkes og stanses før de fullføres. Alle disse sikkerhetsmekanismene er det næringslivet selv som opererer. Dette kan være en årsak til at digitale lovbrudd anses som et sikkerhetsbrudd som best løses innad i næringsliv, finans og cybersikkerhetsmiljøene. Anmeldelse av det straffbare forholdet til politiet oppleves overflødig når kriminaliteten håndteres operasjonelt av næringslivet selv.[23]

4.3 TRANSAKSJONER I BANKSYSTEMET SOM KAN KNYTTES TIL BEDRAGERI

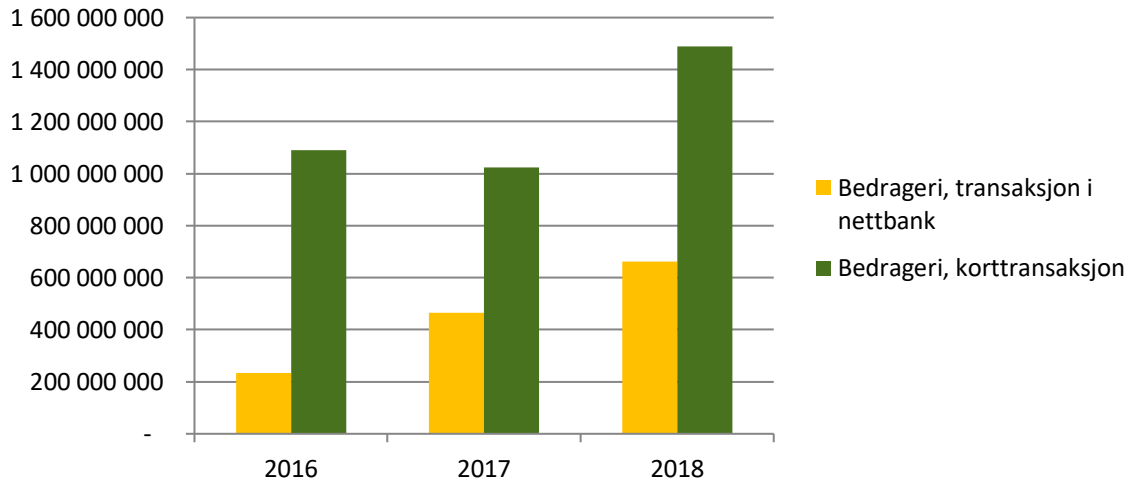
De aller fleste transaksjoner relatert til bedrageri passerer gjennom banksystemer, enten i nettbank eller ved bruk av betalingskort. Bankene kan monitorere og stanse transaksjonene. Gjennom overvåkning og analyse av transaksjoner og kundedialog kan bankene skaffe en unik innsikt i hvilke former for bedrageri som forekommer til enhver tid. På samme måte får bankene også kunnskap om hvilke beløp som kan knyttes til de ulike bedrageriformene. Innsikten i dette varierer imidlertid mellom bankene.

Figur 6 viser fordelingen mellom transaksjoner knyttet til bedrageri som er gjennomført eller forsøkt gjennomført gjennom henholdsvis nettbankløsninger og kortbetalinger i Norge i treårsperioden 2016–2018. Tallstørrelsene er estimater for Norge basert på rapporterte angrepssummer fra DNB. Tallene inkluderer både privat- og bedriftskunder og differensierer ikke mellom dem.

---

22 Næringslivets sikkerhetsråd, *Kriminalitets- og sikkerhetsundersøkelsen i Norge 2017*, s. 35, samt intervjuobjekter.

23 Oslo politidistrikt, *Trender i kriminalitet 2018-2021* s. 18



Figur 6: Estimert angrepssum bedrageri, fordelt på transaksjoner gjennomført eller forsøkt gjennomført gjennom hhv. nettbankløsninger og kortbetalinger i Norge i 2016–2018.

Angrepssum innebærer summen av *gjennomførte*- og *forsøk* på transaksjoner, registrert av finansinstitusjonen. Eventuelle mørketall kommer i tillegg. Figur 6 viser at det er høye beløp knyttet til forsøk på bedrageri ved korttransaksjoner.[24] For 2017 utgjorde estimert angrepssum 1 milliard kroner. Dette er primært kortbedrageri hvor kortet ikke er til stede (*Card Not Present).* Tall fra Finanstilsynet viser at faktiske tap knyttet til kortbedragerier utgjorde 145 millioner kroner i 2017.[25] Dette viser at svært mange forsøk på bedrageri med betaling via kort avverges. Dette kan trolig tilskrives at selskaper driver kontinuerlig overvåkning av korttransaksjoner på vegne av norske banker. For 2018 utgjorde estimert angrepssum på kortbedragerier 1,4 mrd. NOK. Fem prosent av angrepssummen var korttransaksjoner knyttet til investeringsbedrageri. Resterende beløp var hovedsakelig kortbedragerier hvor kortet ikke var til stede.

Figur 7 viser estimert angrepssum for transaksjoner foretatt gjennom nettbank i 2018, fordelt på ulike bedrageriformer[26]. Fakturabedrageri, direktørsvindel og investeringsbedragerier utgjorde de klart største gruppene, sammen med kjærlighetssvindel og svindel gjennom sosiale medier.

Både privatpersoner og foretak utsettes for fakturabedrageri. Estimert angrepssum knyttet til fakturabedrageri med betaling gjennom nettbank utgjorde 147 millioner kroner i 2018 (person og foretak). Ifølge Kriminalitets- og sikkerhetsundersøkelsen (KRISINO) 2017 har 66 prosent av private virksomheter opplevd å få tilsendt faktura for varer eller tjenester som ikke er bestilt.[27]

Direktørsvindel er en bedrageriform som kun gjennomføres overfor foretak. Estimert angrepssum knyttet til direktørsvindel med betaling gjennom nettbank utgjorde 134 millioner kroner i 2018. Til sammenligning utgjorde faktisk tap som følge av direktørs-

24 Kortbedragerіers mål er som regel privatkunders betalingskort. Banker må som regel dekke slike tap, ergo er kortbedragerier behandlet i rapporten.

25 Finanstilsynet, *Risiko- og sårbarhetsanalyse 2017* s. 19

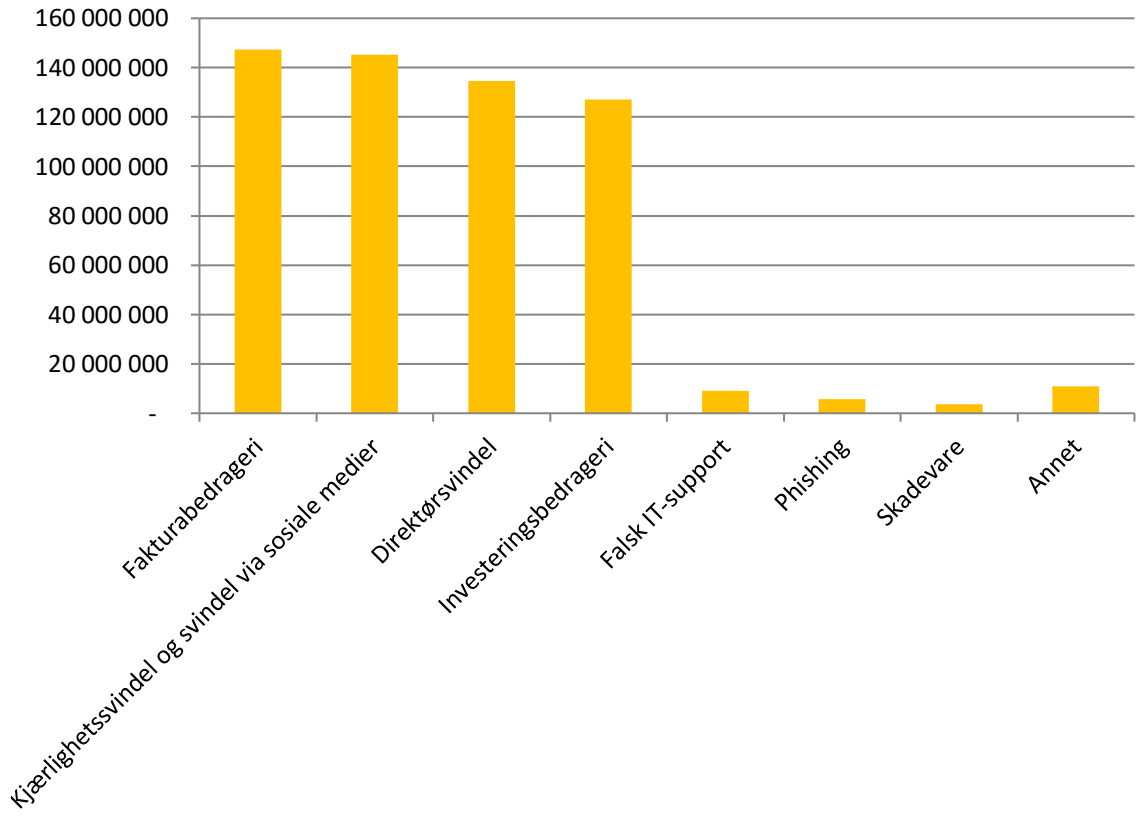
26 DNB

27 Næringslivets Sikkerhetsråd, *Kriminalitets- og sikkerhetsundersøkelsen 2017*, s. 26

vindel 294 millioner kroner i 2016.[28] I følge Finanstilsynet registrerte bankene en økning i både reelle- og avvergede tap som følge av direktørsvindel i 2017. Tilsvarende vurderinger for 2018 er ikke tilgjengelig. Ifølge kilder i politiet er beløpene i de enkelte angrepene lavere i 2018 enn tidligere år, men antall angrep er høyere. Hvorvidt tap som følge av direktørsvindel har gått ned i 2018 kan imidlertid ikke konkluderes ut fra dette.

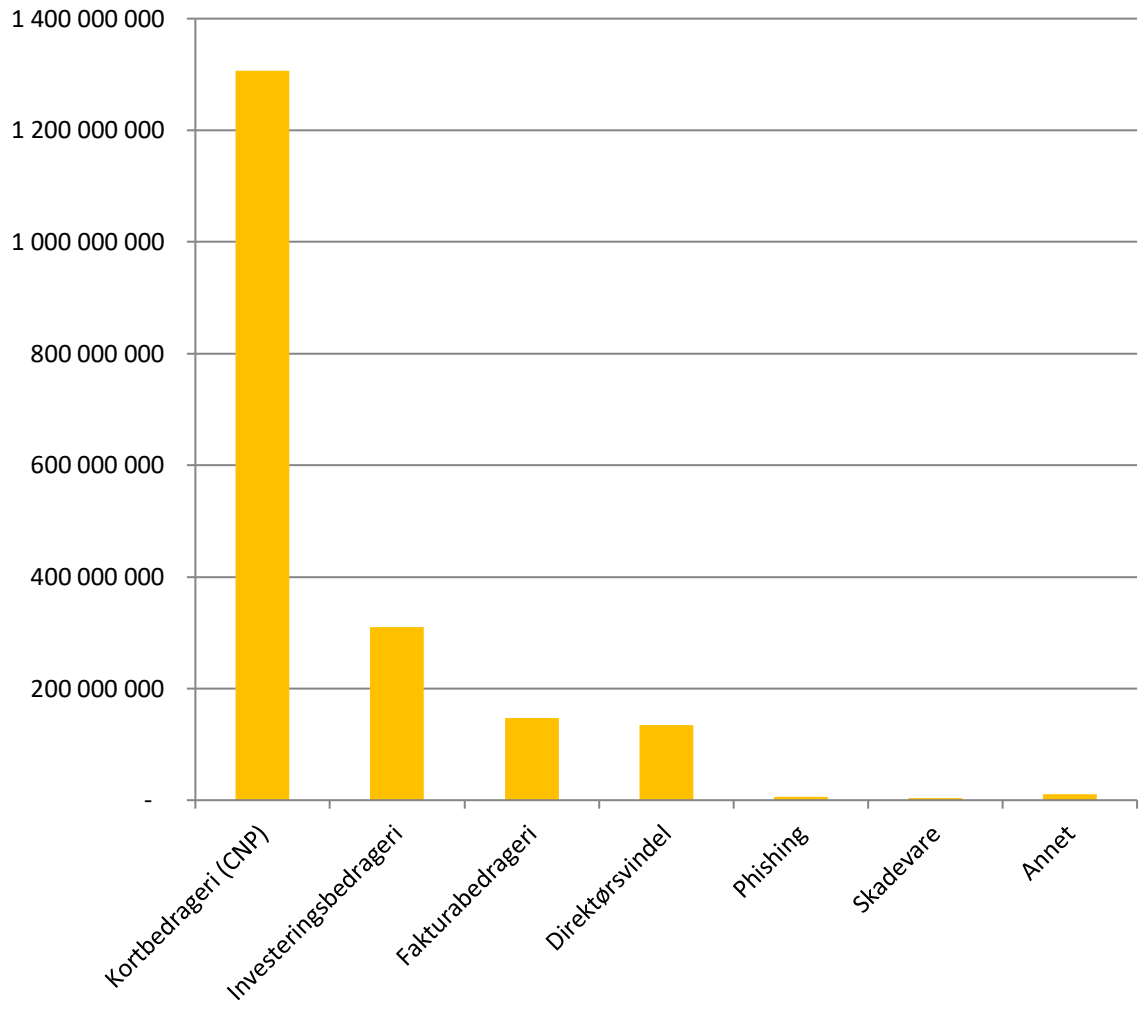
Investeringsbedrageri er en bedrageriform både privatpersoner og foretak utsettes for. Estimert angrepssum knyttet til investeringsbedrageri med betaling gjennom nettbank utgjorde 127 millioner kroner i 2018 (person og foretak). I tillegg kommer anslagsvis 182 millioner kroner i korttransaksjoner som kan knyttes til forsøk på- eller gjennomførte investeringsbedragerier. Dette gjør investeringsbedrageri til en av de største gruppene vurdert ut fra angrepssum. Ifølge Nordea var også investeringssvindel den bedrageriformen deres kunder var hyppigst utsatt for i 2018.[29]

Med søkelys på angrepssummer for det enkelte modus uavhengig av betalingstype, er tradisjonelle kortbedragerier svært fremtredende, se figur 8. Denne kategorien inneholder primært kortbedrageri hvor kortet ikke er til stede.



Figur 7: Estimert angrepssum for transaksjoner foretatt gjennom nettbank i 2018, fordelt på modus.

28 Finanstilsynet (2016), *Risiko og sårbarhetsanalyse*, s. 17
29 Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018,* s. 51



Figur 8: Estimert angrepssum for transaksjoner foretatt gjennom nettbank og med kort i 2018, fordelt på modus.

5 SOSIAL MANIPULASJON

Å manipulere er å påvirke en person på en fordekt måte med det mål om at den skal handle i en bestemt retning.[30] Teknikker som spiller på motpartens følelser som tillit, frykt og fristelse benyttes, og det foregår ansikt til ansikt, ved bruk av e-post, telefonoppringning eller på SMS.[31] Sosial manipulasjon kan brukes til å begå bedrageri, men kan også være en innledning til annen kriminalitet.

Bedrageri ved hjelp av sosial manipulasjon vil bestå i å forlede en person til å gi fra seg sensitiv informasjon eller foreta handling personen normalt ikke ville ha gjort. Sensitiv informasjon i denne sammenhengen er eksempelvis passord, brukeridentitet og bankopplysninger. Dette benyttes til å overta kontoer, misbruke identitet eller initiere betalinger, men kan også være en vare som kan videreselges til andre kriminelle.

Sosial manipulering kan også benyttes til å installere skadevare i datamaskiner gjennom e-post med vedlegg som fremstår uskyldig, eller at en link til en infisert internettside er inkludert.[32]

Metoden er ideell fordi mennesker er subjektive i sin vurdering av informasjon, og derfor et svakere ledd enn et godt sikret datasystem.[33] Styrket datasikkerhet gjør det vanskeligere å gjennomføre datainnbrudd for å stjele informasjon, penger eller gjøre skade. Ved sosial manipulering utnyttes en uskyldig person som døråpner for den kriminelle.

5.1.1 Phishing

Ved phishing benyttes e-post for å «fiske» etter informasjon. E-posten ser ut til å komme fra en velrennomert virksomhet, merkevare eller person, i den hensikt å få mottaker til levere fra seg sensitiv informasjon og/eller utfører en handling som ellers ikke ville blitt gjennomført. I en slik e-post er e-postadressen byttet ut med en annen

30 www.naob.no/ordbok/manipulere (Lesedato: 8.1.2019)
31 Brottsförebyggande rådet, *Bedrägeribrottsligheten i Sverige*, s. 104
32 Europol, *Internet organised crime threat assessment 2018*, s. 55
33 Europol, *Internet organised crime threat assessment 2017*, s. 56–58

adresse enn den reelle ved for eksempel å endre én bokstav. Logo, layout og e-postsignaturer kan være tilsynelatende lik den angitte avsenders. Mottaker oppfordres gjerne til å klikke på en lenke som leder til en falsk internettside der manglende betalingsinformasjon skal legges inn.

En slik e-post kan forlede mottakeren til å tro at vedkommende har vunnet i et lotteri, men at ekstra informasjon må oppgis for at gevinsten kan utbetales.
I tilfeller hvor den falske e-posten tilsynelatende sendes fra en kjent virksomhet er næringslivet skadelidende ved at omdømmet både misbrukes og svekkes.

Næringslivet rammes direkte når ansatte i foretak utsettes for manipulasjon og forledes til å foreta seg handlinger som utsetter bedriftshemmeligheter eller bedriftens kapital for fare. E-post er spesielt utsatt. Ved overtakelse av e-post til ansatte blir det mulig å overvåke e-postkommunikasjon og stjele informasjon. Dette kan også foranledige annen utnyttelse som for eksempel direktørsvindel. En forholdsvis enkel måte å beskytte seg mot sosial manipulasjon på er å benytte to-faktor-autentisering.[34]

5.1.2 Vishing og smishing

Såkalt vishing (voice-phishing) foregår ved telefonsamtale i stedet for e-post. Metoden er ellers som phishing. IP-telefon benyttes ofte for å manipulere trafikkdata og logginformasjon slik at mottagerens telefon opplyser at samtalen kommer fra en tilsynelatende sikker kilde eller en velrennomert virksomhet. Eksempler på vishing er telefonsamtaler hvor oppringer utgir seg å ringe fra Microsoft og tilbyr IT-support. Smishing (sms-phishing) følger samme fremgangsmåte, men her kommuniseres det med tekstmeldinger. I 2017 ble det rapportert om syv tilfeller av smishing hvor merkenavnet til dagligvarekjeden Coop ble benyttet. I 2018 fikk Coop 2 500 henvendelser på svindelforsøk, der flesteparten var sosial manipulering ved bruk av sms.[35]

5.1.3 Pharming

Såkalt pharming skjer når bedragerne installerer skadelig programvare på en pc eller server. Programvaren videresender alle klikk brukeren utfører til en tilknyttet webside. Slik skaffer bedragerne tilgang på finansiell informasjon.

5.1.4 Spearfishing

Spearfishing blir brukt når kriminelle utpeker et spesifikt mål for fiskingen. Angrepet kan være svært effektivt fordi den kriminelle aktøren skreddersyr språk og kontekst for hvert angrepsmål.[36] Når angrepet begås spesielt mot foretak med mye ressurser kalles det whaling.

5.1.5 Omfang og utvikling – mange angrep, få sikre tall

Det er ingen offisiell oversikt over antall phishingangrep i Norge. Tallfesting av denne svindelmetoden er krevende fordi den rommer flere forholdsvis ulike handlinger. Mye tyder på at store virksomheter selv fører oversikt over angrep som begås, men at de færreste angrep anmeldes til politiet.[37,38]

---

34 Næringslivets sikkerhetsråd, *Mørketallsundersøkelsen 2018*, s. 43
35 http://www.norsis.no/coop-advarer-mot-smishing. (Lesedato: 8.1.2019)
36 http://www.blog.dashlane.com/phishing-statistics. (Lesedato 8.1.2019)
37 Næringslivets sikkerhetsråd: *Mørketallsundersøkelsen 2018*, s. 52

I Mørketallsundersøkelsen 2018 svarte 18 prosent av virksomhetene at de hadde vært utsatt for phishing eller andre elektroniske angrep med forsøk på sosial manipulasjon i 2017. I 2015 var tallet 8 prosent, og var da den kriminalitetstypen som økte mest mellom undersøkelsene.

IT-sikkerhetsnettstedet Cybersecurity Ventures mener at 90 prosent av hackingen som lykkes stammer fra e-poster med formål om å forlede mottakeren til å utføre en handling, altså phishing.[39]

Internasjonalt har nettfiske økt. The Anti-Phishing Working Group (APWG) rapporterer antall varsler som mottas om unike phishingforsøk (som for eksempel e-postkampanjer) og unike falske websider øker. Figur 9[40] viser at antall unike phishingforsøk øker med 264 prosent i løpet av en seksårsperiode. Antall avdekkede unike phishing-websider har i likhet med phishing-e-post økt i løpet av samme periode, men er i tredje kvartal 2018 på samme nivå som i 2012.

Videre har APWG registrert en nedgang i antall merkevarer som er kapret i forbindelse med phishingkampanjer i samme periode som over.[41]

Sakseksempel fra Norge

Butikkjeden Kiwi utsettes jevnlig for svindelforsøk. Privatpersoner mottar e-post eller SMS som ser ut til å være fra Kiwi og som kan inneholde informasjon om at vedkommende er valgt ut til å delta i en undersøkelse, og at alle deltakere mottar gevinst. Det eneste mottaker må gjøre er å fylle ut kontaktinformasjon eller betalingsinformasjon.

Angrepene viser at både privatpersoner og selskaper blir skadelidende av samme bedrageriforsøk. Privatpersonene som gir fra seg sensitiv informasjon og kanskje lider økonomisk tap, og selskapet ved at merkevaren utnyttes til gjennomføring av dette.

42,43

38 Se http://www.nrk.no/norge/kripos-advarer_-_-stor-okning-i-datakriminalitet-1.13436174. (Lesedato: 9.1.2019)

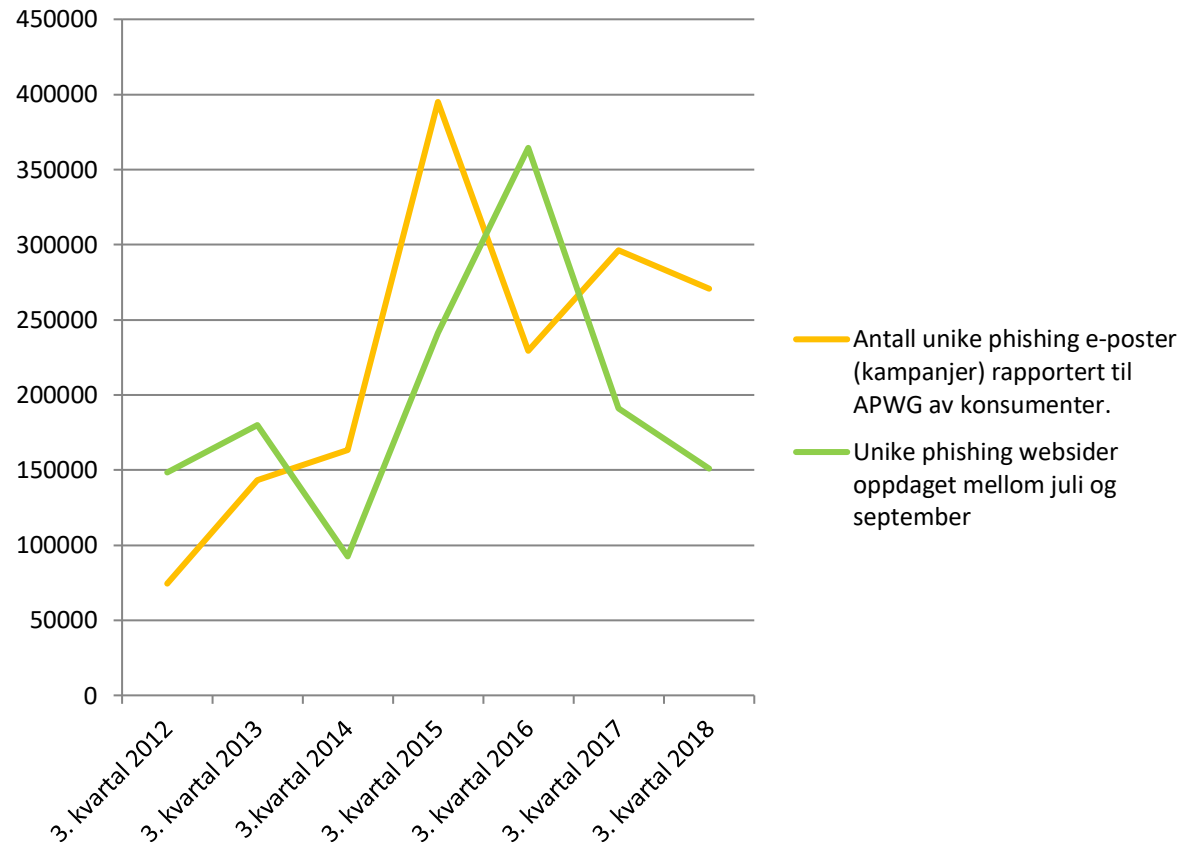
39 Cybersecurity Ventures: *2019 Official Annual Cybercrime report*. Sponset av Herjavec group

40 http://www.antiphishing.org/resources/apwg-reports. *Phishing activity Trends Report 3rd quarter* for årene 2012-2018. (Lesedato: 7.1.2019)

41 http://www.antiphishing.org/resources/apwg-reports. *Phishing activity Trends Report 3rd quarter* for årene 2012-2018. (Lesedato: 7.1.2019).

42 http://www.kiwi.no/informasjon/Denne-mailen-er-ikke-fra-KIWI. (Lesedato: 8.1.2019)

43 Næringslivets sikkerhetsråd: *Mørketallsundersøkelsen 2018*, s. 52



Figur 9: Antall rapporterte phishing-e-poster og phishing-websider 2012–2018.

5.1.6 Trender – angrepene blir mer målrettet

Tidligere ble phishing i stor grad utført ved masseutsendelse av uoppfordrede e-poster eller spam. Dette er fremdeles en vanlig form for phishing, men ikke den mest utbredte. Phishing inntar nye former når det kommer til leveranse og distribusjon, målutvelgelse og formålet med handlingen.

Et økende fenomen er at sosial manipulering benyttes til å infisere mobiler eller datamaskiner ved at mottaker åpner et vedlegg i e-posten eller en linker. Dette inkluderer også spearfishing e-poster. Det utføres også digital kartlegging for å lokalisere og identifisere personer med tilgang til store virksomheters bankkonto eller sensitive data.

I og med at informasjon er blitt en høyomsettelig vare forekommer det også at foretak utsettes for overvåking etter et phishingangrep. Et såkalt root kit følger som vedlegg til e-post til en utvalgt ansatt i en virksomhet, og installeres ved åpning av vedlegget. Installasjonen gir den kriminelle tilgang til å fjernstyre administratortilganger og videre gis det tilgang til sensitiv data eller mulighet til å overvåke datamaskinen over tid før det planlagte angrepet utføres. Det er også registrert økt bruk av phishing-websider

som har HTTPS og SSL sertifikat, noe som gir en falsk opplevelse av trygghet for brukerne.[44]

5.1.7 Gjerningspersoner – organiserte kriminelle står ofte bak

Organiserte kriminelle grupperinger står bak de mer avanserte phishingangrepene.[45] Betalingstransaksjonene som følger av nettfiske overføres til utlandet. IP-adresser som spores i forbindelse med disse angrepene fører også til utlandet. Språket i slike e-poster bærer preg av å være oversatt til norsk ved hjelp av elektronisk oversettingsverktøy. Ved målrettet phishing mot konkrete personer eller virksomheter er angriperne teknisk kompetente nok til å trenge gjennom sikkerhetssystemer både i maskin- og programvaren.[46] Transaksjonene utføres gjerne av andre personer enn de som utfører selve manipuleringen og innehar den tekniske kompetansen.

Sosial manipulasjon som metode medfører også at kriminelle uten spesielt høy teknisk kompetanse, eller som ikke ønsker å kjøpe denne type kompetanse, er i stand til å utføre bedrageri. Dette gjelder nettfiske som ved masseutsendelse av e-poster, telefonoppringninger eller tekstmeldinger.

5.1.8 Fornærmede

Mennesker forledes ved sosial manipulering. Virksomhetens akilleshæl er derfor de ansatte. På grunn av kjeden av teknologiavhengigheter og tingenes internett er skadepotensialet stort dersom kriminelle får tilgang til et foretaks data og datasystem. Gode sikkerhetsrutiner gjennom opplæring av ansatte i sikkerhetskultur og en viss grad av datakompetanse er en forutsetning for forebygging. Virksomheter som har to-trinnsverifisering på e-post og ved transaksjoner er i større grad beskyttet mot sosial manipulering.

Sosial manipulering rammer ikke nødvendigvis bare ansatte i virksomheten, men også virksomhetens kunder. Stjålne opplysninger om foretakets kunder kan brukes til å kapre kontoer eller stjele identiteter og videre utføre kreditt- og lånebedrageri. Virksomheter med en kjent merkevare er også spesielt utsatt for omdømmetap ved phishingkampanjer.

44 http://www.antiphishing.org/apwg-news-center/newfaceofphishing. (Lesedato: 7.1.2019)

45 http://www.nrk.no/norge/kripos-advarer_-_-stor-okning-i-datakriminalitet-1.13436174. (Lesedato: 9.1.2019)

46 www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime/social-engineering

6 DATABEDRAGERI OG FORHOLDET TIL DATAKRIMINALTET

I mai 2018 ble strømmetjenesten Tidal anmeldt av fire norske musikkorganisasjoner for å ha manipulert antall avspillinger av enkelte sanger. Anmeldelsene kom i kjølevannet av Dagens Næringslivs dokumentar «Strømmekuppet»[47] hvor det ble hevdet at minst 320 millioner falske avspillinger av Beyoncé og Kanye West skal ha blitt lagt til Tidals lyttertall. Som et resultat, og på bekostning av andre artister, skal de to artistene og deres plateselskaper ha fått for høye utbetalinger.[48] En slik form for manipulasjon av data kan anses som *databedrageri.*

Databedrageribestemmelsen, strl. § 371 b)
«Med bot eller fengsel inntil 2 år straffes den som med forsett om å skaffe seg eller andre en uberettiget vinning, (...), bruker uriktig eller ufullstendig opplysning, endrer data eller datasystem, disponerer over et kredittkort eller debetkort som tilhører en annen, eller på annen måte uberettiget påvirker resultatet av en automatisert databehandling, og derved volder tap eller fare for tap for noen.»

Databedrageri er bedrageri begått med bruk av datateknologi, ved en «uberettiget påvirkning av resultatet av en automatisert databehandling».[49] Et annet eksempel på databedrageri, er inngivelse av uriktige opplysninger i elektroniske meldekort til NAV. Opplysninger fra elektroniske meldekort behandles automatisk, og handlingen er derfor å anse som et databedrageri. Dersom uriktige opplysninger gis til en saksbehandler, er det å anse som alminnelig bedrageri. Databedrageri skiller seg fra vanlig bedrageri først og fremst ved at det ikke er en person som direkte forledes, og ved at det er uvesentlig

47 www.dn.no/staticprojects/special/2018/05/09/0600/dokumentar/strommekuppet/ (Lesedato: 28.1.2019)
48 http://www.dn.no/musikk/okokrim-bekrefter-etterforsker-databedrageri-i-tidal/2-1-515215 (Lesedato: 28.1.2019)
49 Sunde, Inger Marie (2016) *Datakriminalitet, kapittel 7.3,* s. 122

for straffansvaret hvem tapet eller faren for tap rammer.[50] Databedrageri straffes etter strl. § 371 (b).

Nettbankbedrageri ved bruk av trojaner og SWIFT-bedrageri[51] er andre eksempler på databedrageri, der gjerningspersonen endrer data eller datasystem og slik påvirker resultatet av en automatisert databehandling. Enkelte former for kortbedrageri anses også som databedrageri.[52]

Kripos vurderer *IKT-kriminalitet* å omfatte kriminalitet rettet mot datasystemer, og bruk av IKT som sentralt verktøy i utøvelsen av kriminalitet.[53] I dagligtale legges denne definisjonen til grunn for begrepet «datakriminalitet» i politiet. Begrepsbruken legges også til grunn her.

Datakriminalitet og databedrageri er altså ikke sammenfallende begreper. Modus som nettbankbedrageri ved bruk av trojaner og SWIFT-bedragerier vil likevel falle inn under begge kategorier. I de fleste tilfeller er imidlertid datakriminaliteten et ledd i en kjede av handlinger som til sammen utgjør et bedrageri. Ofte er det snakk om innledende handlinger som muliggjør bedrageriet.

6.1.1 Datainnbrudd som inngang til bedrageri eller utpressing

Et eksempel på en innledende handling som muliggjør bedrageri er datainnbrudd. Datainnbrudd kan gjennomføres ved å utnytte tekniske svakheter i datasystemet, eller ved å forlede en ansatt i foretaket til å installere skadevare.[54] Svært ofte skjer dette ved at en ansatt åpner vedlegg i e-post som er infisert med skadevare, eller følger en lenke til en kompromittert nettside. Flere norske virksomheter utsettes daglig for tusenvis av slike fiendtlige e-poster.[55]

Datainnbrudd kan ha til formål å stjele eller kopiere informasjon som senere utnyttes i forbindelse med sosial manipulasjon, eller til å gjennomføre databedrageri (eksempelvis kortbedrageri). Den stjålne informasjonen kan også brukes til å drive utpressing overfor foretaket. Det er potensielt større risiko for slike informasjonstyverier fra foretak etter innføring av personvernforordningen (GDPR). Etter GDPR kan foretaket få bot for å ha blitt frastjålet sensitiv informasjon, og vil derfor ha større insentiv til å betale løsepenger.

6.1.2 Digital utvikling stiller større krav til datasikkerhet

Den teknologiske utviklingen bidrar til at kriminalitet i økende grad utføres digitalt. Dette stiller økte krav til datasikkerheten hos foretakene i norsk næringsliv, både teknisk og med hensyn til interne sikkerhetsrutiner. I Mørketallsundersøkelsen oppgir 67 pro-

---

50 Ot.prp. nr. 22 (2008-2009), kapittel 11.2.1 s. 325

51 Ved SWIFT-bedrageri infiltrerer svindlere systemet som overfører penger mellom finansinstitusjoner i ulike land (SWIFT står for Society for Worldwide Interbank Financial Telecommunication). Det har vært flere tilfeller av slik svindel i utlandet, der store beløp har gått tapt. Det har ikke enda vært gjennomført SWIFT-bedrageri i Norge.

52 Kortmisbruk kan etter omstendighetene være straffbart som alminnelig bedrageri, databedrageri eller tyveri. Blant annet er det av betydning hva kortet brukes til. Se Sunde, Inger Marie (2016) *Datakriminalitet* kapittel 7.4.2 s. 125.

53 Kripos, *Trusler og utfordringer innen IKT-kriminalitet (2017),* s. 4

54 Med skadevare menes i denne sammenheng ondsinnet programvare som typisk stjeler brukerdata, for eksempel kredittkortnummer, innloggingsinformasjon og personlig informasjon fra infiserte datamaskiner, se Kripos, *Trusler og utfordringer innen IKT-kriminalitet (2017),* s. 9

55 Kripos, *Trusler og utfordringer innen IKT-kriminalitet (2017),* s. 9

sent av respondentene at sikkerhetsbrudd som deres virksomhet har vært utsatt for, blant annet skyldtes tilfeldigheter eller uflaks.[56] Mange svarte også at hendelsen skyldtes menneskelig feil (55 prosent), mangel på sikkerhetsbevissthet hos de ansatte (39 prosent), eller at eksisterende prosesser ikke ble fulgt (28 prosent).

I en undersøkelse som Norsk senter for informasjonssikring (NorSIS) har utført, oppgir 48 prosent av respondentene at de ikke har fått opplæring i datasikkerhet på arbeidsplassen.[57] I en annen undersøkelse svarer 71 prosent at de ikke har fått opplæring i informasjonssikkerhet i løpet av de to siste årene.[58]

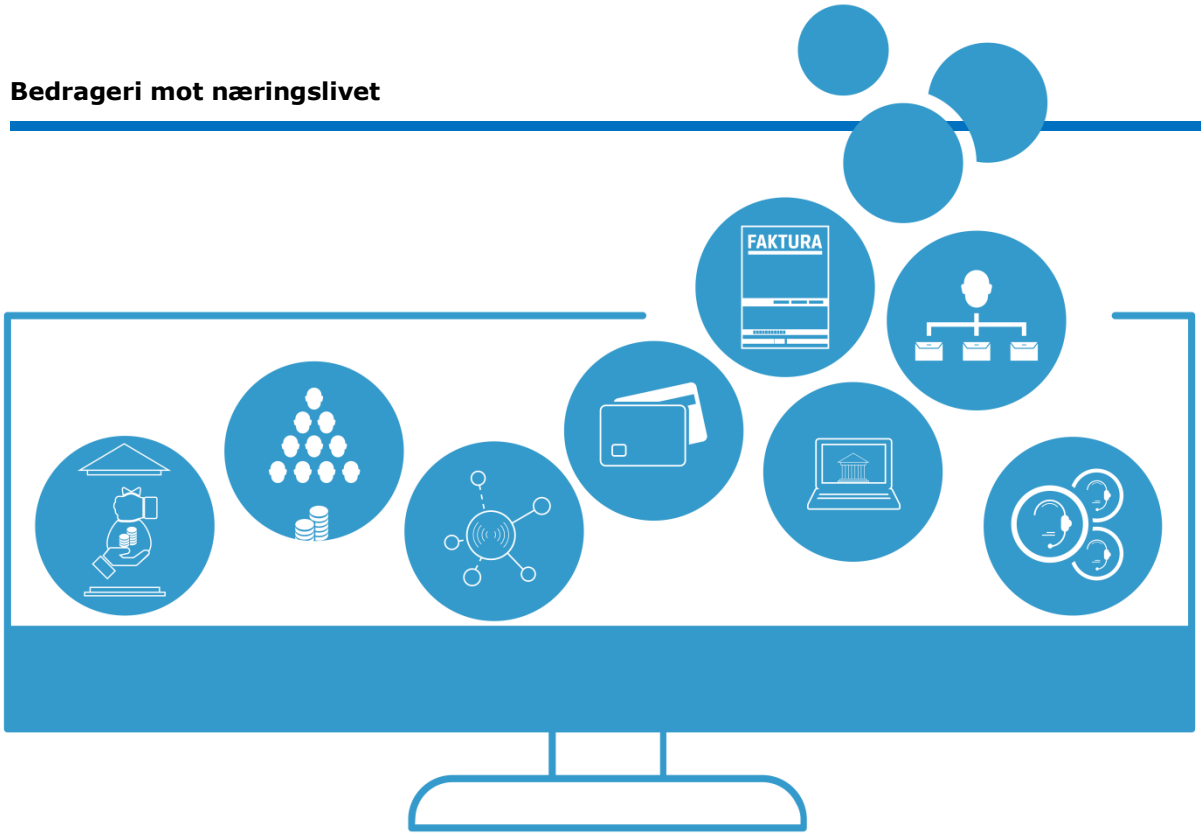
6.1.3 Hvorvidt forsøk lykkes avhenger av foretakets håndteringsevne

Forsøk på bedrageri og digitale angrep rammer alle typer virksomheter. Hvorvidt forsøk på bedrageri og digitale angrep lykkes, beror på foretakets håndteringsevne. Ifølge NorSIS blir trusselaktører som møter små og mellomstore virksomheter stadig mer profesjonelle og målrettede.[59] Store selskap har ofte ressurser og kapasitet til å prioritere sikkerhetsarbeidet. Dette bidrar til at bedrageriforsøk og dataangrep avverges. De små og mellomstore virksomhetene mangler ofte kunnskap og kapasitet til å sikre seg mot kriminalitet. Sikkerhetsarbeidet blir unntaksvis prioritert og baseres ofte på enkelte medarbeideres kompetanse. Dette gjør små og mellomstore virksomheter særlig utsatt.

6.1.4 Banknæringen frykter at PSD2 vil gjøre bankene mer sårbare for bedragerier

Banknæringen frykter at innføringen av PSD2 (Payment Service Directive 2) vil gjøre bransjen mer utsatt for bedrageriforsøk gjennom en tredjepart. PSD2 åpner det norske betalingsformidlingsmarkedet opp for aktører (kalt «betalingsfullmektiger») som kan initiere betaling fra konto i banken, på vegne av kunden. Dette fordrer at bankene åpner sine programmeringsgrensesnitt (API'er) overfor betalingsfullmektigene.[60] Åpne programmeringsgrensesnitt gjør det mulig for tredjeparter å koble seg opp mot bankens systemer, men gjør samtidig banken sårbar for manglende datasikkerhet hos tredjeparten. Bankene er bekymret for at de nye, mindre, FinTech-selskapene ikke skal ta sikkerhet tilstrekkelig på alvor, slik at nødvendige sikkerhetsmekanismer blir nedprioritert til fordel for brukervennlighet. Dersom kundens betalingsfullmektig blir utsatt for datainnbrudd, kan dette medføre at banken mottar falske initieringer, eller mottar initieringer fra aktører som utgir seg for å være den betalingsfullmektige.[61]

56 Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*, s. 20
57 http://www.norsis.no/en-av-to-uten-opplaering-i-datasikkerhet-pa-jobb/ (Lesedato:28.1.2019)
58 Norsk senter for informasjonssikring (NorSIS), *Nordmenn og digital sikkerhetskultur 2018*, s. 38
59 Norsk senter for informasjonssikring (NorSIS), *Nordmenn og digital sikkerhetskultur 2018,* s. 9
60 API står for *Application Programming Interface*
61 Europol, *Internet Organised Crime Threat Assessment 2018*, s. 45



7 MODUS

7.1 DIREKTØRSVINDEL

Direktørsvindel (også omtalt som CEO-svindel) foregår ved at ansatte i selskap blir kontaktet, enten via e-post eller telefon, av personer som utgir seg for å være direktør i selskapet, og som anmoder om at en eller flere transaksjoner foretas til konto i utlandet.

Moduset fordrer at gjerningsperson på forhånd har gjort seg kjent med navn og roller for nøkkelpersoner i virksomheten, og kartlagt hvem som foretar utenlandsbetalinger. Det er ofte økonomiansvarlig eller regnskapsfører med ansvar for utenlandstransaksjoner som kontaktes. Gjerningspersonen manipulerer vedkommende enten til å foreta overførselen, eller til å gi gjerningspersonen tilgang til den ansattes e-post konto.

Slik urettmessig tilgang til den ansattes e-postkonto kalles *business email compromise*. Gjerningspersonen skaffer seg tilgang ved å hacke seg inn i systemet, eller ved å manipulere den ansatte til enten å laste ned skadevare, eller oppgi påloggingsdetaljer. Bruk av forfalsket avsenderadresse i e-post, såkalt «*spoofing*», er en annen form for business email compromise.

Tilgang til e-postkontoen gir gjerningspersonen mulighet til å utgi seg for å være vedkommende – for å få andre til å utføre- eller endre en transaksjon til gjerningspersonens fordel.

Business email compromise kan også utføres med hensikt om å avlytte den ansattes e-postkommunikasjon. Avlytting skjer ved at gjerningspersonen bruker skadevare til å sette inn en videresendingsregel i den ansattes e-postkonto, slik at kopi av alle e-poster videresendes til e-postadresse som gjerningspersonen benytter. Slik avlytting kan foregå over lang tid uten at virksomheten er klar over det. Avlyttingen kan være kilde til verdifull informasjon, for eksempel ved senere forsøk på direktørsvindel.

Direktørsvindel ved sosial manipulasjon

Økonomiansvarlig i en norsk avdeling av et utenlandsk selskap ble i januar 2016 kontaktet av en person som utga seg for å være direktør i selskapet. Han ba vedkommende bistå i et planlagt oppkjøp. Gjerningspersonen sa at dette var børssensitiv informasjon, og at økonomiansvarlig ikke måtte snakke med noen om det. Gjennom flere samtaler ble den økonomiansvarlige manipulert til å overføre nesten 66 millioner dollar, over 500 millioner kroner. Svindelen ble oppdaget ved en tilfeldighet under et møte med ledergruppen i virksomheten. De la merke til at økonomiansvarlig til stadighet ble oppringt, og spurte hva som foregikk. Økonomiansvarlig fortalte om oppkjøpet. Lederen avkreftet dette og slo alarm.

Pengene var overført til to bankkonti i hhv. Hong Kong og Kina. Selskapet kontaktet bankene som pengene ble overført til, og klarte å fryse deler av beløpene. Mange millioner var imidlertid allerede videresendt til andre konti. Ifølge en kunngjøring selskapet senere ga om bedrageriet, kom svindlerne unna med 13 millioner dollar.

62

7.1.1 Utvikling/fornærmede – målene og beløpene blir mindre

Direktørsvindel har vært et kjent fenomen i Norge siden slutten av 2015. Tidligere var det store internasjonale selskap med regelmessige utenlands-transaksjoner som ble rammet. Da var det forholdsvis få angrep, men med store beløp. I 2016 rapporterte bankene, på vegne av kundene, et tap relatert til direktørbedrageri på nesten 300 millioner, fordelt på 214 saker.[63] Finanstilsynet har ikke innhentet tilsvarende tall for 2017, men opplyser at bankene har registrert en økning både i reelle tap og potensielle tap som følge av direktørsvindel.[64]

I Kriminalitets- og sikkerhetsundersøkelsen (KRISINO) 2017 svarte 14 prosent av private virksomheter at de hadde opplevd direktørsvindel.[65] 9 prosent av disse opplevde at svindelen medførte økonomisk tap. Undersøkelsen viste også at selskaper med aktiviteter internasjonalt var mer utsatt for direktørsvindel – 23 prosent av dem som hadde aktiviteter i utlandet hadde opplevd direktørsvindel.

I 2018 har det vært en dreining mot mindre virksomheter, hvor det er lettere å skaffe seg oversikt over de ansatte og deres roller og hvor sikkerhetsrutiner antas lettere å omgå. Tendensen er at direktørsvindel rettes mot mykere mål, som festivaler, foreninger og museer, fordi store selskaper er mer oppmerksomme på modus, og har bedret sikkerhetsrutinene. Beløpene i de enkelte angrepene er lavere, men antall angrep er høyere. For 2018 var estimert potensielt tap som følge av direktørsvindel 134 millioner kroner på landsbasis.[66]

---

62 www.vg.no/nyheter/innenriks/i/Aa93z/historien-om-operasjon-jackpot-politi-spilte-direktoer-og-rundlurte-svindlere (Lesedato: 14.12.2018)

63 Finanstilsynet, *Risiko og sårbarhetsanalyse (ROS) 2016*, s. 17

64 Finanstilsynet, *Risiko og sårbarhetsanalyse (ROS) 2017*, s. 19

65 Næringslivets sikkerhetsråd, *Kriminalitets- og sikkerhetsundersøkelsen i Norge 2017*, s. 26

66 Beløpet er et estimat basert på rapportert angrepssum fra DNB i 2018. *Angrepssum* innebærer at dette er summen av forsøk og gjennomførte direktørsvindler som er registrert i 2018. Ev. mørketall kommer i tillegg.

7.1.2 Gjerningspersoner

Bedrageriene utføres av organiserte kriminelle grupperinger i utlandet. I flere av sakene som er belyst i norske medier er det grupperinger i Israel som står bak. I november 2016 førte en razzia i Israel til at tolv personer ble pågrepet for å ha vært involvert i slik svindel mot utenlandske selskaper, inkludert norske.[67] Utenom Israel kjenner man til flere grupperinger i Vest-Afrika som bedriver slik svindel.

7.2 NETTBANKBEDRAGERI

Ved nettbankbedrageri angripes bankens infrastruktur via kundenes nettbank. Moduset innebærer at en nettbank-kunde får sin datamaskin infisert med en trojaner (skjult dataprogram) som lar gjerningspersonen utnytte kundens nettbankforbindelse. Infiseringen foregår ved at kunden besøker en kompromittert nettside som initierer nedlasting av trojaneren, eller ved at kunden mottar skadevaren i e-post. Skadevaren henter kundens påloggingsdetaljer, og kunden får presentert falske bilder i nettbanken som forleder vedkommende til å legge inn engangskode på nytt. Dette gir gjerningspersonen anledning til å gjennomføre transaksjoner uten kundens kunnskap. I etterkant av bedrageriet blir kunden presentert for falske bilder i nettbanken hvor saldo ikke er påvirket av de urettmessige transaksjonene.

Nettbankbedrageri mot norske banker

Våren 2011 var en rekke norske banker utsatt for et planlagt og delvis gjennomført nettbankbedrageri. En estisk statsborger bosatt i Norge opprettet konto med nettbankløsning i bankene, for så å overlate kodebrikke og påloggingsdetaljer til personer i Estland. Dermed kunne disse utvikle angrepskoder tilpasset den enkelte bank. Gjerningspersonene lyktes å gjennomføre transaksjoner i én av bankene, etter å ha skaffet seg tilgang til kontoen til 25 av bankens nettbankkunder. Esteren ble dømt for datainnbrudd og medvirkning til grovt databedrageri.

68

7.2.1 Utvikling

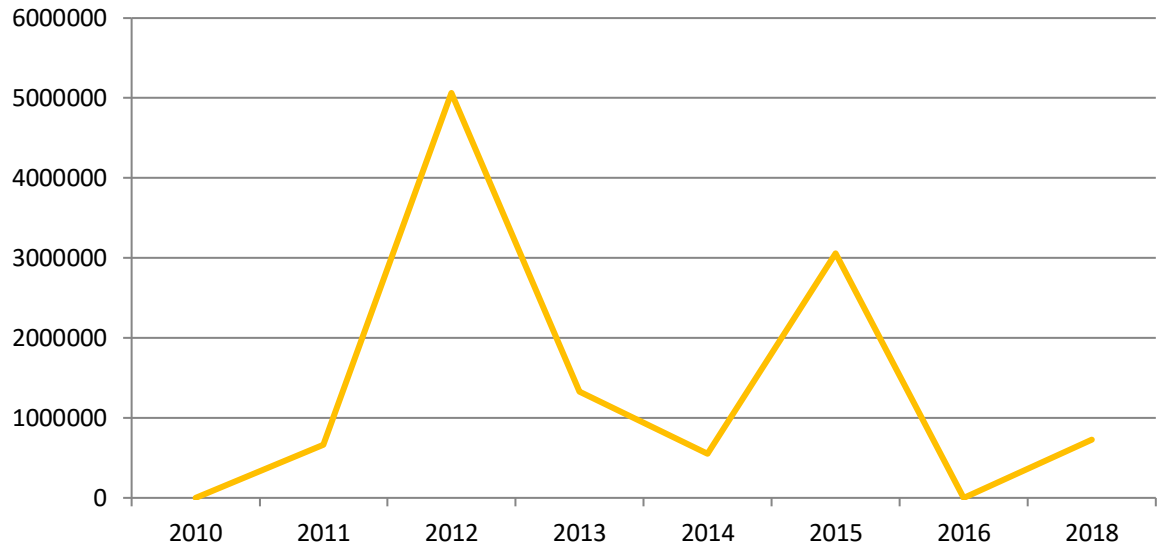
I 2010 og 2011 registrerte bankene økt aktivitet fra trojanere mot nettbanker i Norge, men tap i forbindelse med slike angrep forble små.[69] I 2012 opplevde imidlertid norske banker, i likhet med andre europeiske land, en betydelig økning i antall angrep, hvorpå tapstallene steg. Bankenes rapporter til Finanstilsynet viste at de *potensielle* tapene var vesentlig høyere enn de faktiske.[70]

I etterfølgende år gikk tapene som følge av nettbankbedragerier ned. Nedgangen kunne til dels tilskrives iverksatte tiltak fra bankenes side, og dels færre angrep.[71] I 2015 kom

67 http://www.vg.no/nyheter/innenriks/i/Aa93z/historien-om-operasjon-jackpot-politi-spilte-direktoer-og-rundlurte-svindlere (Lesedato: 14.12.2018)
68 HR-2012-02397-A
69 Finanstilsynet, *Risiko- og sårbarhetsanalyse (ROS) 2011*, s. 24
70 Finanstilsynet, *Risiko- og sårbarhetsanalyse (ROS) 2012*, s. 22
71 Finanstilsynet, *Risiko- og sårbarhetsanalyse (ROS) 2013*, s. 53

imidlertid en ny topp, som følge av trojaneren Dyre. Dyre herjet i mange europeiske land, inntil bakmennene bak trojaneren ble arrestert i Moskva i november 2015.[72]

Antall vellykkede nettbankbedragerier har deretter gått ned, blant annet som følge av bankenes økte deteksjonsmuligheter. Årlige tap knyttet til nettbankbedragerier ved bruk av skadevare er dermed kraftig redusert, se figur 10.[73]



Figur 10: Tap som følge av angrep mot nettbank ved bruk av ondartet programkode (trojaner) på kundens PC eller sikkerhetsmekanisme.

Angrep mot bankenes nettbankstruktur har likevel ikke opphørt. Det har vært flere eksempler på at aktører har utviklet og testet angrepskode mot norske bankers nettbankstruktur. Testingen har i disse tilfellene blitt fanget opp av banken før det har vært gjort forsøk på å gjennomføre transaksjoner.[74]

7.2.2 Gjerningspersoner – organiserte kriminelle med klar arbeidsdeling

Til tross for at angrepskoder omsettes på nett, innebærer nettbankbedragerier en omfattende prosess som krever planlegging og organisering over tid. Bedrageriet krever at ulike roller bekles. Det er nødvendig å rekruttere pengemuldyr, innehavere av testkonti og uttaksledd. Dessuten må angrepskoden tilpasses før den brukes.

Organiserte kriminelle aktører står bak tilpasning av angrepskoden og selve angrepet. Flere av de domfelte for nettbankbedragerier i Norge er østeuropeiske statsborgere som har oppholdt seg i Norge og medvirket til utvikling og testing av angrepskode.[75]

---

72 Finanstilsynet, *Risiko- og sårbarhetsanalyse (ROS) 2015*, s. 35

73 Finanstilsynet, *Risiko- og sårbarhetsanalyse (ROS) 2017* tabell 3 s. 19, *Risiko- og sårbarhetsanalyse (ROS) 2011*, tabell 2 s. 22.

74 TOSLO-2014-50167, TSTRO-2015-163354

75 HR-2012-02397-A, TOSLO-2014-50167, TSTRO-2015-163354

Nettbankbedragerier ledsages ofte av annen kriminalitet. Dette kan være dokumentfalsk i forbindelse med opprettelse av testkonto, hvitvasking av utbyttet, og andre former for bedragerier for å finansiere nettbankbedrageriet.[76]

Angrep ved bruk av nettbanktrojanere går i bølger, og flytter seg mellom land.[77] Norske banker har delvis vært skånet for koder som er utviklet for angrep mot europeiske banker på grunn av særegne bokstaver i alfabetet og annen måte å skrive beløp på. Toppen i angrep 2013, og vedvarende utvikling og testing av angrepskoder tilpasset norske banker, tilsier imidlertid at risiko for nettbankbedragerier i Norge fortsatt er til stede.

7.3 FAKTURABEDRAGERI

Ved fakturabedrageri forledes mottakeren av en faktura til å betale for en vare eller tjeneste som ikke er bestilt. Alternativt forledes mottakeren til å betale en kapret faktura eller en faktura som gjelder et annet beløp, eller med andre vilkår enn det som er avtalt.

Fakturabedrageri gjennomføres på mange ulike måter. Ved masseutsendelser eller ved kontakt i forkant, ved bruk av datatekniske innganger eller ved utnyttelse av såkalt factoringordning.[78] Kategoriseringen er ikke gjensidig utelukkende. En fremgangsmåte kan ha elementer fra flere kategorier.

Eksempel på tilbudsfaktura

Flere virksomheter i Norge har mottatt faktura fra European Finance hvor det kreves betaling for Førstehjelpspakker XL som ikke er bestilt. Logoen på fakturaen er et hvitt kors på grønn bakgrunn og er lik Røde Kors sin logo som har et hvitt kors på rød bakgrunn. Fakturaen er påført mottakervirksomhetens navn og adresse samt navnet på daglig leder/styreleder i virksomheten som referanse. Det er med andre ord innhentet informasjon om de mottakende foretakene. Det kreves betalt for NOK 19.875 for 5 førstehjelpspakker som skal betales til konto i utlandet, uten MVA.

7.3.1 Uten kontakt på forhånd/masseutsendelser

Ved masseutsendelser av fakturaer er det som regel ingen kontakt på forhånd. Ingenting er bestilt. De kriminelle håper at noen virksomheter betaler uten å oppdage at de ikke har en avtale med fakturautsteder. Enkelte av fakturaene er utelukkende kun et tilbud og ikke betaling for noe som er bestilt. Utformingen av fakturaen er likevel slik at dette kan være vanskelig å forstå.

76 TKOEI-2017-101657
77 Finanstilsynet, *Risiko- og sårbarhetsanalyse 2014*, s. 19
78 Brottsförebyggande rådet (2016), *Bedrägeribrottsligheten i Sverige*, s. 68-70

Anmeldelse levert til politiet i 2017. Fornærmedes beskrivelse av gjerningen:

«XXX har mottatt falske fakturaer, og har betalt totalt 6,5 mill til kontonummer i xxx Bank tilhørende xxx. Faktura ble mottatt på mail fra det som tilsynelatende så ut som riktig avsender. Det var en troverdig kopi av faktura fra gjeldende leverandør, hvor annet kontonr var lagt inn. Antakelig har mail vært hacket, slik at de kjente våre rutiner. Faktura ble mottatt til vanlig tid.»

Etter etterforskning avdekkes det at gjerningspersonen har spoofet e-posten til foretakets leverandør ved å utelate en bokstav i e-postadressen. Fakturaen ser også legitim ut, men kontonummeret er ikke riktig. Ved senere korrespondanse med banken spoofes også e-postadressen til fornærmede foretak. De forsøker å stanse transaksjonene ved å sende e-post til banken. Tolv minutter etter at e-posten er sendt til banken mottar banken en ny e-post, tilsynelatende også den fra fornærmede, med beskjed om å se bort fra forrige e-post. Dette tyder på at e-postkontoen til foretaket er hacket og overvåket. (Sak 14311293. Anonymisert av NTAES og brukt med tillatelse fra politidistriktet som mottok anmeldelsen.)

7.3.2 Kapret faktura – kjent leverandør, falsk regning

En kapret faktura fremstår som om den er utstedt av en for mottaker kjent leverandør. Fakturaen er påført leverandørens navn, logo og kontaktinformasjon. Alternativt er fakturaen kapret ved at kontonummer på en korrekt faktura endres slik at pengene overføres bedrageren i stedet for opprinnelig utsteder. Bedrageriet utføres ved at et foretak får informasjon om at en leverandør har endret kontonummer, eller det inngår i det som kalles Business Email Compromise (BEC).

Ved sistnevnte fremgangsmåte bruker kriminelle sosial manipulasjon for å stjele brukernavn og passord slik at de kan hacke epostkonti tilhørende et foretak. Tilgangen benyttes til å overvåke e-postkorrespondanse i påvente av at en faktura mottas for betaling. Fakturaen redigeres ved å endre kontonummeret slik at transaksjonen betales til bedrageren. E-postinnstillingene er endret slik at den originale e-posten med faktura markeres som lest og flyttes til en annen mappe. På denne måten oppdages det ikke at den originale e-posten er ankommet.

7.3.3 Etter kontakt – feil mengde, produkt uten verdi, nye vilkår

Fakturabedrageri begås også etter at det har vært kontakt, eller det påstås at det har vært kontakt mellom selger og kjøper. I følge avsender har kontakten resultert i en avtale dem i mellom.[79]

7.3.3.1 Katalogoppføring

En kjent fremgangsmåte ved fakturabedrageri etter kontakt i Norge er salg av katalogoppføring. Virksomheter kontaktes av en telefonselger som tilbyr abonnement, eller videreføring av en katalogoppføring på internett. Formålet er angivelig å gjøre foretak søkbar og synlig på internett. Under samtalen sender oppringer en e-post som mottaker bes godkjenne ved å trykke på en knapp i e-posten. Dette ønskes utført i løpet av samtalen. Tjenesten betales gjennom faktura. Det viser seg deretter at katalogoppføringen er uten reell verdi, enten fordi internettsiden ikke eksisterer, eller fordi den ikke er pro-

79 Brottsförebyggande rådet (2016), *Bedrägeribrottsligheten i Sverige*, s.71

filert på internett i nevneverdig grad. Katalogoppføring rammer i særlig grad nyetablerte foretak, små og mellomstore foretak, eller foretak med manuelt arbeid.

I flere av nettverkene som står bak svindelfakturering for katalogoppføring i Norge, benyttes enkeltpersonforetak (ENK) og aksjeselskap i utøvelsen av bedrageriet. Det opprettes såkalte callsenter hvor det ansettes telefonselgere. Ved bruk av ENK betales det ikke arbeidsgiveravgift og etter hvert som omdømmet til foretaket svekkes slås aksjeselskapet konkurs, eller enkeltpersonforetaket avvikles for så å lage et nytt selskap eller ENK med nytt navn.

Katalogsvindel uten kontakt og med oppkrevd merverdiavgift

I november 2018 ble to menn dømt av Follo tingrett til fengsel i to år og fire måneder for katalogsvindel. De domfelte opprettet en internettside med opplysninger om norske foretak. Opplysningene var hentet fra Brønnøysundregisteret. 93.000 virksomheter ble tilsendt faktura med beløp på mellom 4.990 eller 5.990 kroner inkludert merverdiavgift for annonsering på internettsiden, uten at de hadde noen kunnskap om nettsiden på forhånd. De domfelte gjorde minimalt for å gjøre nettsiden søkbar. Totalt mottok bedragerne over fire millioner kroner, med tillegg av oppkrevd merverdiavgift på cirka en million kroner. Dommen er anket og således ikke rettskraftig. (Saksnummer: 18-063499MED-FOLL)

7.3.4 Domeneadresser og falske produkter

En annen variant er å forledes til å kjøpe domeneadresser som ligner virksomhetens domene til en høy pris, gjerne ti ganger så høy som reell verdi. Telefonselgeren påstår at noen andre er interessert i det aktuelle domenet og at det vil lønne seg å kjøpe det. Det er ofte et hasteelement involvert og svar bes avgitt raskt.

Andre eksempler er nettsteder som selger kopivarer eller falske produkter, eller salg av rekvisita over telefon der en mottar varer i en helt annen størrelsesorden enn avtalt, med dertil høye fakturakrav.

7.3.5 Factoringsvindel – både kunde og mellommann lures

Factoring er en finansieringsform der et foretak får kreditt med sikkerhet i egne fakturaer. Foretaket overlater fakturaer til factoringselskap som betaler inntil 85 prosent av fakturaen omgående. Factoringselskapet videreformidler fakturaene til de respektive mottakerne og krever betaling og står for eventuelle purringer. Når fakturaene er betalt betales det resterende beløpet til foretaket.

Faktura kan være betalingskrav for en vare eller tjeneste som enten ikke finnes, eller er av en annen verdi enn avtalt. På denne måten blir factoringselskapet innkrever av penger fra virksomheter som er utsatt for fakturabedrageri, samtidig som de selv er bedratt fordi de har gitt kreditt basert på verdiløse fakturaer.[80]

80 Brottsförebyggande rådet (2016:10), *Kriminell infiltration av företag,* s. 69 samt Statens offentliga utredningar (2015:77), *Fakturabädragerier*

7.3.6 Innledende handlinger

I forbindelse med et bedrageri kan den innledende handlingen gi et forvarsel om hva som er i ferd med å gjennomføres. Med kunnskap om inngangene som benyttes kan foretak avdekke bedrageriforsøk før handlingen volder tap.

Endringer i leverandørens navn, adresse eller kontonummer kan være en inngang til kapring av fakturaer. Det samme gjelder spoofede e-poster, ved at den tilsynelatende legitime e-postadressen eksempelvis mangler en bokstav. I forbindelse med bedragerier med katalogoppføring henter gjerningspersonene informasjon om foretak fra Brønnøysundregisteret. Særlig nyetablerte foretak og enkeltmannsforetak er utsatt siden Brønnøysundregisteret kunngjør nyregistrerte foretak.[81] De fornærmede forledes gjerne over telefon ved at innringer presenterer seg med et firmanavn som er påfallende likt en kjent merkevare eller nummeropplysning, noe som inngir tillit. Hastelementet er også ofte tilstede her.

7.3.7 Målutvelgelse – tilpasser ofre

Fakturabedrageri er ofte systematisk utført ved at en person eller et nettverk benytter samme fremgangsmåte mot flere mål over tid. Fakturabeløpene ved masseutsendelser og faktura etter kontakt er som regel på mellom 3000–20 000 kroner. Selv om få velger å betale, blir gevinsten stor, ofte på flere millioner kroner for bedragerne.

Noen av straffesakseksemplene viser at enkelte fakturabedragere hensyntar foretakets størrelse før valg av beløp som skal faktureres. Desto større foretak, jo høyere beløp. Ved kaprede fakturaer kan de kriminelle i større grad velge å redigere fakturaer med høye beløp, eller endre beløpssummen.

Enkelte foretak betaler fakturaen vel vitende om at dette er bedrageri. Årsaken kan være frykt for at foretaket skal få betalingsanmerkninger eller inkassovarsel og at dette kan medføre større vansker med å få kreditt og lån i banker. Andre anser beløpet så lavt at det ikke er verdt bryderiet med å få betalingsanmerkninger eller purring per telefon.

Ferier er høysesong for bedragerier. De kriminelle spekulerer ofte i at det er færre fast ansatte på jobb og kontrollen er lavere enn vanlig.[82]

7.3.8 Omfang og utvikling – en langvarig landeplage

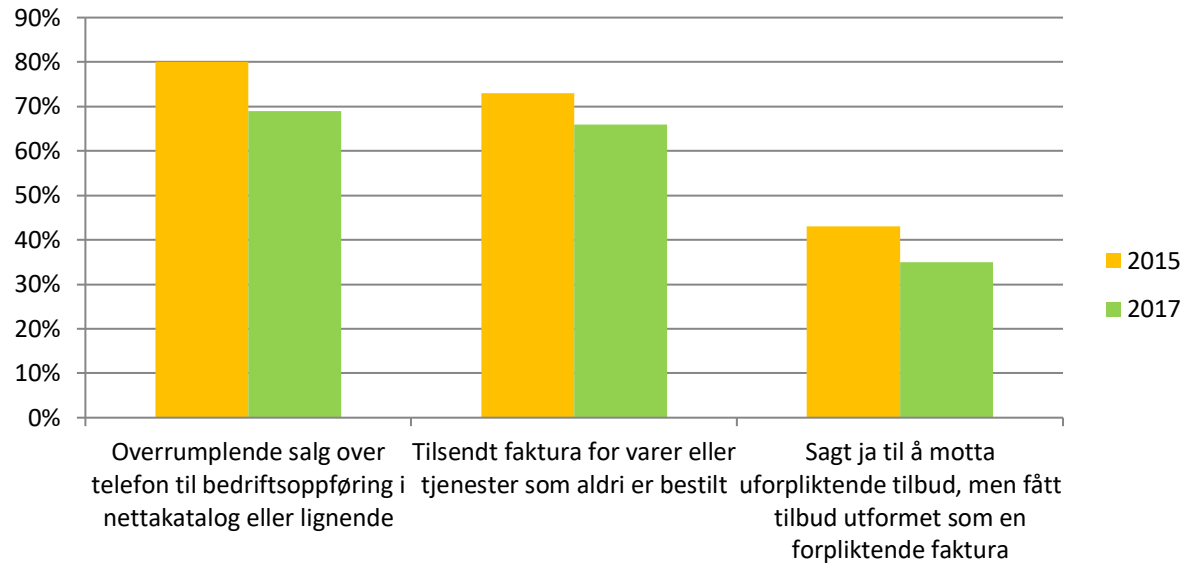
Fakturabedrageri er trolig den bedrageriformen som har rammet næringslivet i Norge oftest. Medieoppslag og avgjørelser i rettsapparatet viser at denne bedragerimetoden har vært fremtredende over flere tiår. Som figur 11[83] viser svarte sju av ti ledere i private virksomheter i 2017 at de har blitt utsatt for overrumplende salg over telefon til bedriftsoppføring i nettkatalog eller lignende.

---

81 Dette har bedret seg etter at Brønnøysundregisteret sluttet å legge ut informasjon om nyregistreringer på nett før firmaet selv har fått beskjed (tidligere ble det sendt pr post). De kriminelle utnyttet et tidsvindu før virksomheten var klar over offentliggjøringen.

82 ØKOKRIM 28.06.18 – *Ikke la deg lure i sommer, (okokrim.no)*

83 Næringslivets sikkerhetsråd, *Kriminalitetsundersøkelsen 2015*, s.18 og *2017* s.26



Figur 11: Andel private virksomheter som er blitt svindlet eller forsøkt svindlet ved fakturabedrageri.

Tidligere ble fakturabedrageri begått ved utsendelse av fakturabrev, nå sendes de i stor grad som vedlegg i e-post. Det gjør det langt enklere å sende ut store mengder fakturaer. Bedrageriene er mer omfattende i antall, men det er likevel få som betaler. Bankenes kontrollvirksomhet er blitt bedre og flere fakturabedrageriforsøk avdekkes før transaksjonen fullføres. Konti som brukes i bedrageriøyemed kan sperres og innbetalte beløp kan gjøres utilgjengelig for bedragerne. DNB estimerer at angrepssummen for fakturabedrageri i Norge i 2018 er på cirka 147 millioner norske kroner.[84]

I Sverige er anmeldte bedrageri med bruk av «bluffaktura» gått ned 34 prosent fra 2016 til 2017.[85] Det antas at forekomsten av tradisjonelle fakturabedragerier er redusert til fordel for fakturabedrageri begått som databedrageri eller ved hjelp av internett. Disse modusene registreres som forskjellige typer bedragerier i svensk kriminalstatikk. En annen forklaring kan være at foretakene i mindre grad anmelder fakturabedragerier enn før.

7.3.9 Hvem er gjerningspersonene?

Fakturabedrageri med salg av katalogoppføring er godt dokumentert i flere etterforskninger og dommer i Norge. Gjerningspersonene bak denne fremgangsmåten er i hovedsak etnisk norske. De er veltalende og opererer i gråsonen mellom det lovlige og ulovlige. Ofte er de et nettverk av personer med definerte roller med ledere og selgere.

Aktører i Norge, Sverige, Estland og Bulgaria står bak flere av masseutsendelsene av tilbudsfakturaer. Aktørene forsvinner ved vedvarende negativ publisitet, men dukker gjerne opp under nye navn etter en viss tid.

---

84 Med angrepssum menes alle forsøk, uavhengig av resultat. Det vil si total sum av stansede og vellykkede angrep.

85 En bluffaktura kan være masseutsendelser av tilbudsfaktura, faktura fra ukjent leverandør eller kapret faktura. Brottsförebyggande rådet (2016), *Bedrägeribrottsligheten i Sverige*

7.3.10 Hvem er de fornærmede?

«Alle typer bedrifter opplever forsøk, forskjellen ligger i hvordan de er i stand til å håndtere det.»[86]

Fakturabedrageri rammer både små og store foretak, men det medfører ikke økonomisk tap for alle. Under 20 prosent av foretakene som var utsatt for fakturabedrageri opplevde økonomisk tap.[87] Med andre ord er *forsøkene* på fakturabedrageri mange, men de fleste oppdages før det gjennomføres en betaling.

Når det gjelder fullbyrdede fakturabedragerier tilsier informasjon fra næringslivet at bransjer med manuelt arbeid, foretak hvor arbeidere har utenlandsk opphav, små- og mellomstore foretak og enkeltpersonforetak er særskilt utsatt. Små foretak og enkeltpersonforetak har ikke kunnskap, kontroll eller kapasitet til å sikre seg mot kriminalitet i like stor grad som de større. Foretak i etableringsfasen er også spesielt utsatt. Det er flere som velger å betale fakturaen når det ligger en «avtale» til grunn, altså når det har vært en kontakt på forhånd.[88]

7.4 KREDITT- OG LÅNEBEDRAGERI

Kreditt- og lånebedragerier er en av finansnæringens største finansielle risikoer. Bedrageriformen innebærer kjøp av varer og tjenester på kreditt, eller opptak av lån- eller inngåelse av avtale om kreditt hos bank eller finansieringsselskap, uten å ha til hensikt å betale kravet når det forfaller. Bedrageriet begås i eget eller andres navn, eller ved bruk av et selskap.

Kreditt- og lånebedragerier som begås i andres navn er ofte innledet av et identitetstyveri. Stjålne identiteter benyttes som regel til kredittbedrageri overfor et stort antall forhandlere og finansinstitusjoner.[89] Foruten bruk av stjålne identiteter ses det også bruk av helt falske og/eller manipulerte identitetsdokumenter i forbindelse med denne kriminaliteten.[90]

7.4.1 Kredittbedrageri ved bruk av selskap

Kreditt- og lånebedragerier hvor avtale om kreditt er inngått av selskap innebærer gjerne bruk av manipulert dokumentasjon på selskapets kredittverdighet. Kreditter som gis til selskaper basert på uriktig regnskapsmateriale, gir økt risiko for tap for finansinstitusjoner fordi selskapene vil få videre kredittrammer enn personkunder.[91] Det kan være selskapets rettmessige eier eller leder som står bak bedrageriet, men det kan også være personer som urettmessig har tatt kontroll over selskapet- eller som utgir seg for å være eier eller leder. I Sverige finnes det eksempler på at virksomheter har blitt overtatt eller «kapret» for å utnytte selskapets kredittverdighet til å begå kredittbedrageri.[92]

---

86 Intervjuobjekt
87 Næringslivets Sikkerhetsråd, *Kriminalitets- og sikkerhetsundersøkelsen i Norge 2017*, s. 27
88 Statens offentliga utredningar (2015:77), *Fakturabädragerier* s. 17 og 18
89 TOSLO-2016-20077, LA-2016-96929, LB-2015-56957
90 Brottsförebyggande rådet (2016), *Bedrägeribrottsligheten i Sverige*, s. 91
91 Justis- og beredskapsdepartementet (2018), *Nasjonal risikovurdering*, s. 20
92 Brottsförebyggande rådet (2016), *Bedrägeribrottsligheten i Sverige*, s. 93–94

Kredittbedrageri ved bruk av kapret foretak

Tre menn ble i 2016 dømt i Oslo tingrett for identitetskrenkelse overfor to personer samt et aksjeselskap som en av de fornærmede eide. De ble også dømt for en rekke grove bedragerier og forsøk på bedragerier overfor finansinstitusjoner og leverandører av varer og tjenester, ved bruk av stjålne identiteter. Identitetstyveriet av aksjeselskapet ble gjort ved å inngi opplysninger til Brønnøysundregisteret om at selskapet ikke skulle oppløses som planlagt, og at en av de tre var innsatt som styreleder og daglig leder for selskapet. De endret videre selskapets adresse, og endret selskapets postadresse til den oppgitte «styreleders» privatadresse.

Over en periode på 15 måneder tok mennene opp lån og søkte om kredittkort ved misbruk av en av person-identitetene. Identiteten tilhørte en av de dømtes samboer. De gjorde videre en lang rekke disposisjoner i kraft av å være daglig leder og styreleder i selskapet, herunder kjøp av diverse elektronisk utstyr, og kjøp av luksusbiler med finansiering fra ulike finansieringsinstitusjoner. Blant annet lånefinansierte de en Audi, en Aston Martin, kjøpte klær og utstyr fra Ferner Jacobsen for 66 000 kroner, åtte iPhone 5 fra tre forhandlere, i tillegg til diverse elektronisk utstyr verdt over 100 000 kroner fra Eplehuset og Elkjøp. Alt ble gjort under påskudd av å være daglig leder og styreleder i selskapet.

Mennene var tidligere dømt en rekke ganger for tilsvarende forhold. To av dem ble i denne saken idømt fengselsstraff i hhv. 2 år og 9 måneder, den siste ble idømt 300 timer samfunnsstraff. Én mistet retten til å drive næringsvirksomhet i tre år. To ble fradømt retten til å drive selvstendig næringsvirksomhet for alltid.

93

7.4.2 Gjerningspersonene har tilknytning til Norge

Ved kreditt- og lånebedragerier befinner gjerningspersonen seg som oftest i Norge. I mange tilfeller er det enkeltpersoner eller mindre grupper som står bak, men det kan også være organiserte miljøer. Ofte er dette personer som er tidligere domfelt for tilsvarende forhold. Kredittbedrageriet omfatter ofte også andre forhold som for eksempel identitetstyveri og dokumentfalsk. Svært ofte blir identiteten til gjerningspersonens tidligere partnere utnyttet ved inngåelse av låneavtale i annens navn.[94]

Kredittbedragerier krever en viss tilknytning til Norge i form av norsk bankkonto, norsk adresse og bank-ID. Utenlandske personer som arbeider i Norge har anledning til å ta opp lån etter tre måneder. Det er en utfordring for kreditt- og finansinstitusjoner at utenlandske arbeidstakere ved en rekke tilfeller har fått innvilget billån for så å ta kjøretøyet med til hjemlandet uten å nedbetale billånet.[95]

93 De tre tiltalte ble i lagmannsretten (LB-2016-180744) frifunnet for at de ved selve identitetstyveriet av aksjeselskapet samtidig gjorde seg skyldig i bedrageri overfor selskapet

94 Brottsförebyggande rådet (2016), *Bedrägeribrottsligheten i Sverige,* s. 93

95 Justis- og beredskapsdepartementet (2018), *Nasjonal risikovurdering*, s. 20

Bestilling av kredittkort med stjålet identitet

I mai 2018 ble en 40 år gammel mann dømt til fengsel i seks måneder i Agder lagmannsrett, for å ha medvirket til bestilling og avhenting av kredittkort utstedt til en uvitende tredjepart som var utsatt for et identitetstyveri. Kortene ble hentet ut ved hjelp av et pass som hadde fornærmedes navn og tiltaltes bilde. Domfelte hadde medvirket til både å lage passet, og til misbruk av kredittkortene. I tillegg til fengselsstraff, ble mannen dømt til å betale erstatning til fire ulike kredittinstitusjoner, i solidarisk ansvar med en annen gjerningsperson. Lovbruddene inngikk i et større sakskompleks hvor flere gjerningspersoner systematisk hadde begått bedragerier.

96

Det er også eksempler på at personer blir presset av kriminelle til å oppta bil- og forbrukslån i eget navn.[97] Når lånet innvilges, blir pengene umiddelbart spredt til flere kontoer og personer. Personer knyttet til mistanke om terrorfinansiering er ofte omtalt i bedragerier med dette moduset, ofte som en av flere som får overført pengene til egen konto. Det kan være uklart om tredjepersonen som tar opp lån i slike tilfeller har medvirket til bedrageriene, eller er utsatt for identitetstyveri.[98]

7.5 KORTBEDRAGERI

Ved kortbedrageri benytter gjerningspersonen en annen persons betalingskort eller kortopplysninger til å gjennomføre et kjøp eller kontantuttak. Bedrageriformen har en rekke ulike fremgangsmåter og medfører ofte andre kriminelle handlinger i tilknytning til bedrageriet.

Kortbedrageri kan deles inn i to kategorier: kjøp eller uttak der betalingskortet er tilstede *(card present – CP)*, og kjøp eller uttak der betalingskortet ikke er til stede (*card not present – CNP)*. Hvis kortet ikke er tilstede, er det stjålne eller falske kortopplysninger som benyttes for å gjennomføre transaksjonen. Transaksjoner hvor det ikke er behov for at kortet er fysisk til stede er for eksempel ved netthandel.

Stjålne kortopplysninger kan også benyttes i produksjon av falske kort.

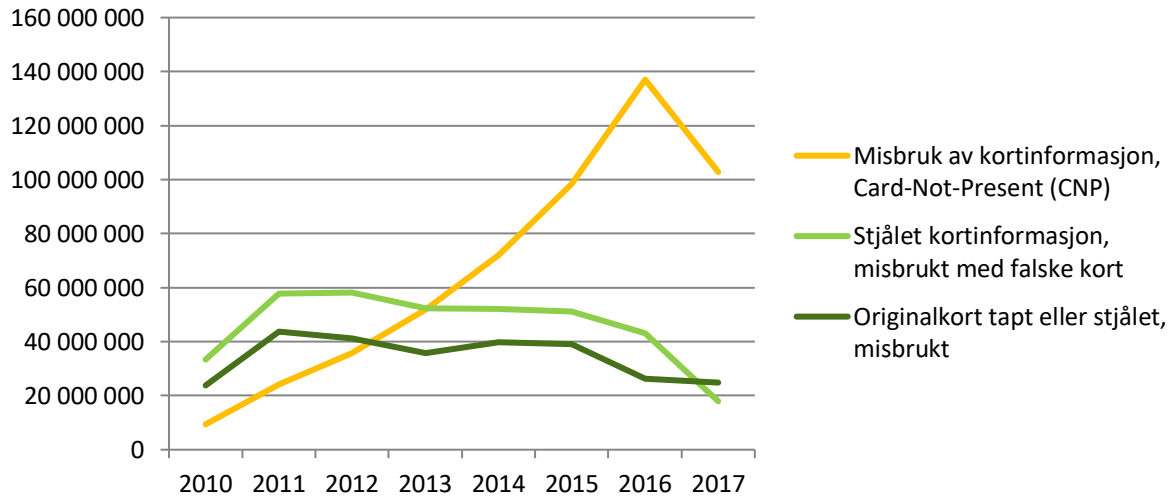
7.5.1 Utvikling

Etter mange år med økning, spesielt av misbruk av stjålne kortopplysninger, observerte Finanstilsynet i 2017 en nedgang i kortsvindel, se figur 12.[99] Nedgangen skyldtes antakelig økte krav fra kortutstedere, kortinnløsere og brukersteder til sterk autentisering av kortholder ved bruk av betalingskort.[100]

Selv om EU-landene observerer samme synkende trend, er kortbedragerier der betalingskortet ikke er til stede fortsatt den dominerende formen for svindel mot betalingstjenester ifølge Europol.[101]

---

96 LA-2018-206
97 TOSLO-2016-203957 (Zalo), TOSLO-2015-105037-3 (Lime – ikke rettskraftig)
98 Justis- og beredskapsdepartementet (2018), *Nasjonal risikovurdering,* s. 20-21
99 Finanstilsynet, *Risiko- og sårbarhetsanalyse (ROS) 2010* s. 28, 2011 s. 21 og 2017 s. 19
100 Finanstilsynet, *Risiko og sårbarhetsanalyse (ROS) 2017*, s. 18
101 Europol, Internet organised crime threat assessment 2018, s. 7



Figur 12: Tap som følge av kortbedrageri 2010–2017

7.5.2 Tilgang på stjålne kortopplysninger

Kortopplysninger kan tilegnes på ulike måter. Ifølge Europol er skimming[102] av kort fortsatt en utfordring, om enn mindre utbredt enn det var for noen år siden.[103] Kortopplysningene blir brukt til å lage falske kort, som benyttes til uttak i områder – hovedsakelig utenfor Europa – der EMV chip-teknologi[104] ikke er tatt i bruk og magnetstripen fortsatt benyttes.[105] I 2017 rapporterte EU-landene tilfeller av «shimming» til Europol. *Shimming* innebærer at kortopplysninger blir kopiert fra kortets EMV-chip. Opplysningene kan benyttes til å lage falske kort med magnetstripe, men det kan ikke lages en kopi av kortets chip.[106] Uttak med falske kort laget med kortopplysninger stjålet ved shimming, kan derfor kun skje i områder der magnetstripen fortsatt benyttes.

En annen måte å tilegne seg kortopplysninger på er gjennom phishing-kampanjer. Kjente merkevarer blir misbrukt i forsøk på å lure personer til å oppgi sine kortopplysninger. Gjerningspersonen utgir seg for å være et kjent selskap som mange har et kundeforhold til. Vedkommende tar kontakt med mange, ofte tilfeldig utvalgte mennesker, med en likelydende henvendelse. Personene oppfordres her til å oppdatere sine betalingsopplysninger overfor selskapet. Henvendelsen skjer ofte via e-post, men også ved popup-annonser på internett, tekstmeldinger eller oppringninger. Apple og Netflix er eksempler på merkevarer som stadig misbrukes i slike kampanjer.

Kortopplysninger kan også tilegnes gjennom datainnbrudd hos aktører som lagrer sine kunders betalingsopplysninger. De siste årene har det vært en rekke tilfeller av datainnbrudd, blant annet hos leverandører av software til ulike booking-tjenester, som har

102 Skimming innebærer at kortopplysninger blir kopiert fra kortets magnetstripe ved bruk i minibank eller betalingsterminaler (Points of Sale – POS)

103 Europol, *Internet organised crime threat assessment 2018,* s. 40

104 EMV står for Europay, MasterCard og Visa, som er de tre kortselskapene som utviklet standarden for bruk av chip til å lagre opplysninger i kortet og autentisere korttransaksjoner

105 Europol, *Internet organised crime threat assessment 2018*, s. 40

106 Europol, *Internet organised crime threat assessment 2017*, s. 45

medført at person- og betalingsopplysninger for svært mange mennesker har kommet på avveie. I 2018 ble en andel av Ticketmasters britiske kunder rammet, da en underleverandør til Ticketmaster ble utsatt for datainnbrudd og bruk av skadelig programvare som skaffet tilgang til kundenes person- og betalingsopplysninger. Det franske selskapet Fastbooking, som tilbyr bookingløsninger til 4 000 hoteller i hundre land, ble utsatt for tilsvarende angrep sommeren 2018.[107]
Det er et stort marked for stjålne kortopplysninger på det mørke nettet.

7.5.3 Gjerningspersoner

Der stjålne kort blir misbrukt direkte er det gjerne lokale grupperinger eller enkeltpersoner som står bak, og det dreier seg ofte om mindre beløp. Kortsvindel ved misbruk av stjålne kortopplysninger bærer preg av organisert kriminalitet, og ofte er det utenlandske grupperinger som står bak. Ifølge Europol er det i hovedsak kriminelle grupper i Øst-Europa og Balkan som står bak skimming av kortopplysninger.[108]

7.5.4 Fornærmede

I 2017 ble 65 000 norske kort misbrukt i kortsvindel, med et direkte tap på 145 millioner kroner.[109] Prognosen for 2018, basert på tall fra første halvår, er et tap knyttet til kortbedrageri på 94 millioner kroner.[110] Dette tilsvarer en nedgang på 35 prosent sammenlignet med 2017.

Det er først og fremst eier av kortet som privatperson som rammes av bedrageriet, men tapet som oppstår dekkes i svært mange tilfeller av aktører i verdikjeden, så som kortutsteder eller brukerstedet, og rammer på den måten også næringslivet. Hvem som dekker tapet avhenger av de konkrete forholdene i den enkelte sak.

7.6 INVESTERINGSBEDRAGERIER

Investeringsbedrageri innebærer at privatpersoner eller foretak blir forledet til å investere i prosjekter eller produkter som er verdiløse eller ikke-eksisterende. Investeringene kan være i aksjer eller andre finansielle instrumenter, eiendomsprosjekter, varer eller råvarebørs, eller påstått verdifulle gjenstander, som kunst og antikviteter. De siste årene har bedragerier tilknyttet investeringer i kryptovaluta blitt svært utbredt. Sosial manipulasjon av fornærmede står sentralt i bedrageriformen.

Både privatpersoner og foretak utsettes for investeringsbedragerier. Foretak med ledig likviditet blir manipulert til å investere i et prosjekt eller i aksjer, motivert av forventningen om høy avkastning forbundet med liten risiko. Ifølge Nordea var investeringssvindel den bedrageriformen deres kunder var hyppigst utsatt for i 2018.[111] Estimert potensielt tap som følge av investeringsbedrageri utgjorde 309 millioner kroner på landsbasis i 2018.[112]

---

107 http://www.digi.no/artikler/mange-billett-og-hotellkunder-berort-av-nye-datainnbrudd/441054 (Lesedato: 8.1.2019)

108 Europol, *Internet Organised Crime Threat Assessment 2018*, s. 40

109 Finanstilsynet, *Risiko og sårbarhetsanalyse (ROS) 2017*, s. 18

110 www.finansnorge.no/aktuelt/nyheter/2019/01/kraftig-nedgang-i-svindel-med -kort/ (Lesedato: 25.2.2019)

111 Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018,* s. 51

112 Beløpet er et estimat basert på rapportert angrepssum fra DNB i 2018. *Angrepssum* innebærer at dette er summen av forsøk og gjennomførte investeringsbedragerier (person og foretak) som er registrert i 2018. Ev. mørketall kommer i tillegg.

7.6.1 Salg av investeringsobjekter og -prosjekter

Aksjeinvesteringsbedragerier innledes ofte med en oppringning fra en operatør i et såkalt «boiler room», eller call-senter. Slike call-sentre er bemannet med selgere som benytter pågående salgsteknikker for å overbevise- eller manipulere potensielle investorer til å foreta aksjeinvesteringer som senere viser seg å være verdiløse eller ikke-eksisterende.[113] Oppringningen er ofte første kontakt mellom selgeren og den potensielle investoren, og omtales som «cold-calling».

ØKOKRIM omtaler denne første kontakten som salgsfasen.[114] Deretter starter tilbakekjøpsfasen hvor fornærmede blir kontaktet og får tilbud om å selge aksjene. Henvendelsen kommer ofte flere år etter at vedkommende har avskrevet aksjene som tap. Ofte følger det krav om å betale skatter og avgifter på aksjene. Avslutningsvis kommer redningsfasen, hvor fornærmede blir kontaktet av selskap som angivelig vil hjelpe fornærmede med å vinne tilbake tapt kapital.

De fem flaggs teori

Bedragerne innretter seg gjerne etter det ØKOKRIM kaller "De fem flaggs teori". Ifølge teorien sprer bedragerne spor etter sine aktiviteter over fem land. Dette gjør de ved å jobbe i land 1, ha kunder i land 2, ha produkter i land 3, motta betaling i land 4 og bo i land 5. Praksisen gjør bedrageriene krevende å etterforske.

115

En annen form for investeringsbedragerier er såkalte «Ponzi-bedragerier» som kjennetegnes ved at bedragere tiltrekker seg en gruppe investorer med løfter om høy avkastning på kort tid. Bedragerne bruker midler fra investorer som kommer inn på et senere tidspunkt, til å betale den første gruppen investorer for å rekruttere andre investorer. Midlene blir aldri investert, og etter en tid forsvinner bedragerne. Pengene er da hvitvasket gjennom et stort antall bankkonti i flere land.[116]

7.6.2 Falske handelsplattformer på nett

I de senere år har det vært en økning i investeringsbedrageri ved salg av kryptovaluta gjennom falske handelsplattformer på nett. Bedragerne bruker sosiale medier eller oppringningskampanjer (*cold-calling*) til å markedsføre plattformene.[117] Navn og bilder av kjente personer blir ofte misbrukt i kampanjer på sosiale medier, med oppdiktede historier om deres suksess med investeringer i kryptovaluta gjennom plattformen. Markedsføringen av *The Crypto Revolt* er et eksempel dette, hvor også norske kjendisnavn har blitt utnyttet.[118] I forbindelse med opprettelse av konto på handelsplattformen gir fornærmede fra seg kort- og personopplysninger til bedragerne. Bedrageriet medfører derfor ofte at fornærmede også blir frastjålet sin identitet.

---

113 Europol, *Serious and Organised Crime Threat Assessment 2017*, s. 43

114 https://www.okokrim.no/?cat=422488 (Lesedato: 1.2.2019)

115 Ibid

116 Europol, *Serious and Organised Crime Threat Assessment 2017*, s. 43

117 http://www.actionfraud.police.uk/ *Cryptocurrency Investment Fraud*

118 http://www.dn.no/medier/kryptovaluta/idar-vollvik/teknologi/fortviler-over-kryptosvindel-klager-pa-henleggelse/2-1-526204 (Lesedato: 1.2.2019)

Den siste tiden har det vært et skifte fra bruk av falske handelsplattformer til bruk av konto i legale kryptobørser. Bedragerne manipulerer fornærmede til å gi fra seg personopplysninger, for så å benytte opplysningene til å opprette konto på en kryptobørs. Et beløp overføres fra kunden til den digitale lommeboken som er opprettet i kundens navn, hvorpå beholdningen blir stjålet.

7.6.3 Investeringsbedrageri og kjærlighetssvindel

Investeringsbedragerier kan innledes ved en oppringning fra en selger, eller gjennom kjærlighetssvindel. Gjennom romantiske relasjoner knyttet i sosiale medier eller på datingsider, blir fornærmede manipulert til å investere- og til å rekruttere andre investorer til tvilsomme prosjekter i utlandet. Fremgangsmåten blir omtalt som Nigeriasvindel. Ofte blir den som utsettes for kjærlighetssvindel også bedt om å stille sin konto til disposisjon til pengeoverføringer, en såkalt «muldyrkonto». Fornærmede gjør seg da skyldig i hvitvasking.

7.7 TELEKOMMUNIKASJONSBEDRAGERI – MANIPULERING AV ANROPSTRAFIKK

Europol ser en økende trend innen enkelte modus av telebedrageri. International Revenue Share Fraud rettes spesielt mot næringslivet og krever at myndigheter i flere land samarbeider med telebransjen i kriminalitetsbekjempelsen.[119]

Sakseksempel: Bedrageri av norsk teleselskap

En 37 år gammel mann ble av Borgarting lagmannsrett i 2017 dømt for grovt bedrageri og forsøk på grovt bedrageri etter å ha svindlet og forsøkt svindlet to norske teleselskap. Den domfelte opprettet et NUF under et dansk selskap han var direktør i. Han bestilte 33 mobilabonnement gjennom det norske selskapet, men fikk avslag etter en kredittsjekk av det nyetablerte selskapet. Domfelte bestilte 34 kontantkortabonnement hos et datterselskap av det forrige teleselskapet. Etter å ha mottatt SIM-kortene kontaktet domfelte utstederen og fikk omgjort kontantkortene til mobilabonnement. Tiltalte reiste så til utlandet og benyttet SIM-kortene til å ringe en rekke numre i åtte ulike land. I løpet av den fire timers perioden dette pågikk hadde anropene en varighet på 417 timer og 20 minutt. Handlingen medførte et tap for telefonselskapet på 636.166 kroner. I dommen påpekes det at bedrageriet og forsøket fremsto nøye og målrettet planlagt over tid, at de bar preg av å være profesjonelt gjennomført og at flere personer må ha vært involvert.

120

7.7.1 International Revenue Share Fraud (IRSF)

Målet ved International Revenue Share Fraud (IRSF-bedrageri) er å manipulere anropstrafikken i telekommunikasjonsnettverket. Anropstrafikk styres til høyt takserte telefonnumre som for eksempel teletorgtjenester, eller det roames i utlandet. Bedrageren mottar en andel av inntekten fra eieren av den kostbare telefontjenesten eller operatøren som samtalen rutes gjennom. Bedrageriene utføres hovedsakelig ved én av to fremgangsmåter.

---

119 Europol: *Internet organised crime threat assessment 2018*, s. 44

120 Borgarting lagmannsrett – Dom – LB-2017-125960

Den ene innebærer å kjøpe, overta eller kapre SIM-kort og ringe til kostbare telefonnummer. For å generere mest mulig trafikk settes det opp konferansesamtaler som gjør det mulig å foreta flere anrop samtidig ved bruk av ett SIM-kort. SIM-kortets tilbyder må betale operatører i utlandet for medgått trafikk uten at tilbyderen selv får betalt.

En annen måte er hacking av et privat telefonnettverk (Private Branch Exchange system (PBX))[121] for så å anrope kostbare nummer. Dette utføres gjennom utnytting av feilkonfigurerte brannmurer, dårlige sikkerhetsinnstillinger eller manglende vedlikehold i nettverket. Når bedragerne først er på innsiden av nettverket kan mobilsvartjenester eller viderekobling av telefoner til høyt takserte nummer fra en bedriftstelefon enkelt foretas. Slike handlinger medfører høye kostnader for utnyttede foretak, men kan også føre til at foretaket blokkeres av teletilbyder fordi foretaket feilaktig anses som utøveren av handlingen.[122]

7.7.1.1 Omfang og utvikling

Telekommunikasjonsbedrageri har eksistert i mer enn ti år. Nå anser Europol denne type bedrageri for å være økende. I Norge er det flere eksempler på at personer har fått tilgang på flere SIM-kort og ringt kostbare utenlandske teletorgtjenester. Det er også et eksempel på bedrageri hvor bedragerne har fått tilgang til sentralbordet i et foretak og generert 400 samtaler til en totalkostnad på i overkant av 160 000 kroner.

Estimater tilsier at halvparten av medlemslandene i EU har vært utsatt for telekommunikasjonsbedrageri og at det økonomiske tapet er på rundt 7 milliarder amerikanske dollar årlig.[123] Enkelte teleoperatører mener at 18 prosent av omsetningen deres er komponert av trafikk generert ved organisert kriminalitet.[124]

Overgangen til Voice over Internet Protocol (VoIP)[125] gir bedragerne tilgang til å foreta flere simultane anrop og raskere generere høye regninger enn hva som er tilfelle ved PSTN-nettet.[126] Kommunikasjon som går over internettapplikasjoner har de samme sårbarheter som andre applikasjoner.[127] Dersom kriminelle først har tilgang til PBX nettverket er de også knyttet til en lengre sammenkoblet kjede av teknologiavhengige enheter, også kalt the Internet of Things (IoT), med de potensielle skadevirkningene dette kan medføre.

I 2017 omtalte Europol PBX bedrageri som et økende problem og estimerte at fremgangsmåten sto for 20 prosent av alle rapporterte telebedrageri.[128]

---

121 Private telefonnettverk brukes av foretak til å kommunisere både internt og eksternt til det offentlige telefoninettet (PSTN), VoIP tilbydere og SIP trunks.

122 Europol og Trend Micro (2018): *Toll Fraud, International Revenue Share Fraud and More: How criminals monetise hacked cellphones and IoT devices for Telecom fraud* samt http://www.actionfraud.-police.uk/news/the-threat-of-pbx-dial-through-fraud

123 Europol: *Internet organised crime threat assessment 2018*, s. 44

124 Europol og Trend Micro (2018): *Toll Fraud, International Revenue Share Fraud and More: How criminals monetise hacked cellphones and IoT devices for Telecom fraud,* s. 2

125 VoIP er kommunikasjon over IP nettverk slik som internett, til forskjell fra over det offentlige svitsjede telefonnettverket (PSTN).

126 PSTN står for public switched telephone network og er et svitsjet telefonnettverk. Det omtales noe misvisende som analog telefoni. Et moderne PSTN nett er ofte digitalisert med unntak fra endesentralen og ut til abonnenten.

127 http://www.blog.ipswitch.com/voip-and-the-wild-world-of-toll-fraud. (Lesedato 16.1.2019)

128 Europol: *Internet organised crime threat assessment 2017*, s. 28

7.7.1.2 Gjerningspersoner – varierende grad av kompetanse kreves

Hacking av PBX-nettverk krever teknologisk kompetanse og kan utføres fra hvor som helst i verden. Telebedrageri ved bruk av SIM-kort krever på sin side ingen særskilt teknologisk kompetanse. Felles for bedragerne bak begge fremgangsmåtene er at de kan ha en knytning eller et samarbeid med den høyt takserte teleoperatøren eller teletorgtjenesten. Disse tjenestene befinner seg gjerne i land med generelt høyt takserte anropspriser og gjerningspersonen kan derfor sannsynligvis ha en forbindelse til utlandet.

7.7.1.3 Fornærmede – teleselskaper

International Revenue Share Fraud rammer primært teletilbydere og teleoperatører ved å utnytte transaksjonsflyten i telekommunikasjonskjeden. Teletilbydere må betale for alle samtaler som settes opp eller startes i sitt nettverk, uavhengig av om det er bedrageri eller ikke. Foretak med dårlig sikret nettverk rammes av PBX bedrageri. Bedrageriet foregår oftest utenfor foretakets kontortid, og oppdages ikke før neste arbeidsdag.

7.8 MANIPULERING AV STRØMMETJENESTER

75 prosent av inntektene i musikkindustrien i 2018 stammet fra strømmetjenester.[129] [130] Strømmetjenesters betalingsmodell fungerer slik at inntektene fordeles mellom strømmetjenesten og rettighetshavere til innholdet i tjenesten.

I musikkstrømmetjenester genereres inntekter etter antall avspilte sanger, spillelister eller album. Jo flere avspillinger desto høyere inntekter får rettighetshaverne utbetalt i royalties. Tjenestene kan manipuleres gjennom økt strømmetrafikk eller ved at det genereres inntekter til falske artister. Oppskrifter for enkle former for strømmemanipulering kan kjøpes over internett.

Automatiserte kontoer, eller robotkontoer konstrueres for å strømme utvalgte sanger eller spillelister kontinuerlig døgnet rundt for å generere høyt antall avspillinger og royalties. Lydsporene som strømmes kan enten være legitime artisters musikk eller konstruerte generiske lydspor uten tydelige vers og refreng og som bedrageren har opphavsrettigheter til.[131] Det kan også benyttes ordinære og legitime abonnementskontoer til å generere økt strømmetrafikk ved å spille samme sang gjentatte ganger en måned i strekk. Hvorvidt sistnevnte er et lovbrudd er omdiskutert da abonnementet er betalt for.

En tredje fremgangsmåte for å manipulere strømmetjenester er at brukere med gratisabonnement benytter illegale applikasjoner som blokkerer reklamer på tjenesten. Denne formen for bedrageri rammer primært selve strømmetjenesten og foretak som betaler for annonsering.[132]

Manipulering av strømmetjenester påvirker inntektsdelingen mellom rettighetshavere slik at inntekter basert på urettmessig tilegnelse av avspillinger begrenser inntekten til reelle artister. Fordelingen blir skjev fordi potten å fordele på de rettmessige artistene

---

129 Kategorien strømmetjenester inkluderer abonnementstjenester som Spotify, Apple music og Tidal, digitale radiotilbud som Pandora og reklamefinansierte tjenester som YouTube og gratisversjonen av Spotify.

130 http://www.riaa.com/wp-content/uploads/2018/09/RIAA-Mid_Year-2018-Revenue-Report.pdf. (Lesedato 5.2.2019)

131 Dagens Næringsliv 29.1.19, s. 30: *Bergenulo Five finnes ikke, men spilles på Spotify*

132 http://www.variety.com/2018/music-streamin-sites-fraud-1202905665. (Lesedato: 6.2.2019)

blir mindre. Strømmetjenesten rammes ved utbetaling av beløp til falske artister eller artister som urettmessig har tilegnet seg volumavspillinger og derav høyere inntekter. Det er knyttet stor usikkerhet til omfang av bedrageriformen. Strømmetjenestene ønsker ikke å bekrefte at dette er et problem.

Selskaper bak sosiale medier har blitt oppmerksomme på manipulering av «trafikk» i sosiale medier. Falske følgere og likerklikk påvirker popularitet, som kan øke eller redusere markedsverdi og fortjeneste til personer, foretak og varer.[133] Falske profiler har fått tilgang til brukerkonto for øke antall følgere og likerklikk.

Manipulering av spillelister
I februar 2018 avslørte Music Business Worldwide at en person eller gruppe i Bulgaria mest sannsynlig hadde manipulert Spotify for en million amerikanske dollar. Fremgangsmåten besto i å lage en tredjepartsspilleliste med musikk de selv eide rettighetene til, som genererte nok inntekter til å bli innlemmet på Spotify sin globale topp 100 oversikt. Spillelisten, med bare 1800 følgere og 467 sanger genererte 1200 månedlige lyttere hver. Tross det noe beskjedne antall lyttere utkonkurrerte spillelisten plateselskap som Sony, Universal og Warner.

Fremgangsmåten var sannsynligvis å betale for 1200 abonnement, som spilte de 467 sangene i loop. 1200 abonnement koster om lag 12.000 dollar i måneden totalt. Inntektene derimot kan fordeles slik: Sangene varte i gjennomsnitt på noe over 40 sekund. Det er 86.4000 sekunder i løpet av ett døgn. Dersom sangene ble spilt kontinuerlig av de 1200 kontoene i 30 dager utgjør det 72 millioner avspillinger. Et konservativt anslag av utbetaling per sang er 0.004 dollar. Ganget med 72 millioner utgjør det 288.000 dollar per måned. Dersom bots ble brukt til å skippe sangene etter 30 sekunder (Spotify sin grense for pengeutbetaling) ville profitten være på 415.000 dollar. Og dette er bare ved å spille sanger fra én spilleliste i én måned. Det er usikkert om handlingen var ulovlig da abonnementene var betalt for.

134

133 Instagram-press.com/blog/2018/11/19 (Lesedato: 14.2.2019).
134 http://www.musicbusinessworldwide.com/great-big-spotify-scam-bulgarian-playlister-swindle-way-fortune-streaming-service. (Lesedato 6.2.2019)

8 DIGITALE ANGREP – IKKE ALT ER BEDRAGERI

Datakriminalitet inngår ofte i en kjede av handlinger som til sammen utgjør et bedrageri. Det er imidlertid mange typer digitale angrep som mangler elementet av forledelse av en person, eller manipulasjon av data, og dermed ikke oppfyller kriteriene til et bedrageri.

For et foretak som opplever et sikkerhetsbrudd er det hverken enkelt eller særlig interessant å skille mellom bedragerier og andre digitale angrepsformer. Manglende bevissthet rundt forskjellen, gjør at bedragerimodus og en rekke datakriminalitetsmodus ofte omtales om hverandre. Under følger en beskrivelse av enkelte digitale angrepsformer som i stor grad rammer næringslivet, men som ikke er bedrageri.

8.1 UTPRESSING ETTER DATAINNBRUDD

Stjålet informasjon som følge av et datainnbrudd kan brukes til å drive utpressing overfor foretaket. Utpressing kan også skje i form av et angrep med løsepengevirus (ransomware). Ved slike angrep blir foretakets datafiler kryptert eller gjort utilgjengelig av gjerningspersoner som krever betaling for å dekryptere dem.[135] I mange tilfeller kreves betalingen utført i kryptovaluta. Angrepet skjer ofte via skadevare i e-post. I 2017 omtalte Europol løsepengevirus som den mest fremtredende trusselen innen skadevare.[136]

Til tross for Wanna-Cry (se faktaboks), stagnerte økningen i antall angrep med løsepengevirus i 2017, men angrepsformen fortsatte å dominere trusselbildet for kriminalitet rettet mot datasystemer i Europa.[137]

Ifølge Nordic Financial Cert har det ikke vært rapportert tilfeller av løsepengevirus blant deres medlemmer i 2018. Løsepengevirusangrep har ifølge Nordic Financial Cert forandret karakter fra å være ikke-målrettede angrep mot tilfeldig utvalgte systemer som in-

135 Kripos, *Trusler og utfordringer innen IKT-kriminalitet (2017)* s. 9
136 Europol, *Internet Organised Crime Threat Assessment 2017*, s. 19
137 Europol, *Internet Organised Crime Threat Assessment 2018*, s. 7

neholdt svakheter, til å være mer målrettede angrep mot ressurssterke mål hvor løsepengesummen som kreves i etterkant er større.

«Wanna-Cry»

Angrep med løsepengevirus ble for alvor allment kjent 12. mai 2017, da skadevaren «Wanna-Cry» spredte seg til datamaskiner over hele verden. Europol estimerer at opp til 300.000 maskiner, i over 150 land ble infisert i angrepet.[1] Skadevaren skiller seg fra tidligere kjente løsepengeviruskampanjer ved at den sprer seg automatisk i nettverket ved hjelp av en kjent sårbarhet i programvaren fra Microsoft.

En type ikke-målrettede angrep som er i fremvekst i Europa er «cryptojacking».[138] Cryptojacking skjer ved at maskiner søker etter sårbarheter på systemer verden over, og stjeler CPU-kapasitet der de kommer til. Den stjålne datakapasiteten blir benyttet til å utvinne kryptovaluta. Det har vært tilfeller av cryptojacking i Norge i 2018 ifølge Nordic Financial Cert.

8.2 DATATRAFIKK SOM VERKTØY

En annen angrepsform som benyttes hyppig er tjenestenektangrep. Ifølge Europol er dette en av de vanligste angrepsformene, bare overgått av bruk av skadevare.[139] Distribuert tjenestenektangrep eller *Distributed-Denial-of-Service (*DDoS) er angrep som har til hensikt å hindre andre å få tilgang til en tjeneste, ressurs eller lignende på internett. Angrepet gjennomføres ved at offerets datasystem utsettes for så stor datatrafikk eller belastning at legitim trafikk ikke kommer gjennom, eller at systemet bryter sammen.[140] Formålet med angrepet kan være utpressing, aktivisme, eller å skaffe seg anerkjennelse. DDoS-angrep er lett tilgjengelig på nett for en billig penge.

Ofte trues det med å gjennomføre tjenestenektangrep såfremt ikke offeret betaler løsepenger. Mange av de som står bak slike trusler har ikke evnen til å gjennomføre de angrep som det trues med.[141]

Operasjon Power OFF

I april 2018 tok Europol, i samarbeid med nederlandsk og engelsk politi, ned det som skal ha vært verdens største markedsplass for kjøp av tjenestenektangrep. Markedsplassen, webstresser.org, hadde omtrent 151 000 registrerte brukere, og det var registrert fire millioner tjenestenektangrep fra nettstedet. Målene for angrepene var alt fra statlige institusjoner, banker, private virksomheter og aktører innenfor online-spill. Som følge av operasjonen har Kripos mottatt informasjon om en rekke norske brukere. Flere av brukerne er mindreårige.

142

138 Ibid, s. 8
139 Ibid, s.7
140 Kripos, *Trusler og utfordringer innen IKT-kriminalitet (2017),* s. 11
141 *Ibid,* s. 12

9 KJENNETEGN VED GJERNINGSPERSONER

9.1 EN TYPISK BEDRAGER

En typisk bedrager av næringslivet[143] kan sies å være en ugift mann på 36 år, uten arbeid og uten ledende rolle[144] i næringsliv, dersom vi legger medianverdier[145] til grunn. Figur 13 viser en oversikt over profiler av personer anmeldt for ulike typer lovbrudd, målt gjennom medianverdier.[146] Til sammenlikning er medianpersonen i Folkeregisteret en 42 år gammel ugift mann, med ansettelsesforhold, men uten ledende roller i næringslivet.

Vinningskriminelle og bedragere av næringsliv og privatpersoner er tilsynelatende de yngste og mest uetablerte, både når det gjelder sivil status, knytning til arbeidslivet og formelle ansvar. De ulike gruppene kan plasseres langs en akse hvor aktørene blir eldre og mer etablerte.

---

142 http://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2019/01/29/op-power-off-2/ (Lesedato: 30.1.2019), http://www.europol.europa.eu/newsroom/news/authorities-across-world-going-after-users-of-biggest-ddos-for-hire-website (Lesedato: 30.1.2019).

143 I kjennetegnsanalysen skilles det ikke på bedrageri av private og offentlige foretak. Med «næringsliv» menes her både foretak i privat og offentlig sektor.

144 *Ledende roller* er tatt fra Enhetsregistret og består av: Bestyrende reder (BEST), bobestyrer (BOBE), daglig leder (DAGL), deltaker med delt ansvar (DTPR), deltaker med fullt ansvar (DTSO), innehaver (INNH), kontaktperson (KONT), styrets leder (LEDE), styremedlem (MEDL), nestleder (NEST), observatør (OBS), norsk representant for utenlandsk enhet (REPR).

145 Medianverdi er verdien av variabelen som ligger midt i det statistiske materialet. Det vil si at like mange individer i materialet har verdier over medianen som under.

146 Økonomisk kriminalitet og vinningskriminalitet er overordnede kriminalitetstyper. Kategorien økonomisk kriminalitet inneholder blant annet korrupsjon, økonomisk utroskap, ulike bedragerier, hvitvasking og underslag. Kategorien vinningskriminalitet består av mer tradisjonelle lovbrudd som for eksempel tyveri av person på offentlig sted, biltyveri og innbrudd.

De som gjennomfører bedrageri av privatpersoner og næringsliv likner dermed på de vinningskriminelle, men er noe eldre. Videre har de økonomisk kriminelle blitt eldre og innehar ledende roller i næringslivet, i motsetning til de som bedrar privatpersoner og næringsliv. Til sist følger de som gjennomfører bedragerier av det offentlige, begår utroskap og står bak korrupsjonskriminalitet. I følge medianverdiene er sistnevnte gruppe eldre, ofte gift og er både i ansettelsesforhold og innehar ledende roller.

9.1.1 Kjennetegn er nært knyttet opp til modus

Medianverdier er et godt mål ved profilering av gjerningspersoner fordi det beskriver det typiske. Kjennetegnene viser klare forskjeller hos gjerningspersoner i de ulike kriminalitetsformene. Profileringen beskriver kjennetegn til de fleste som er anmeldt for bedrageri. Det innebærer allikevel ikke at de mer komplekse profilene ikke eksisterer, noe de kvalitative funnene underbygger. Uansett peker funnene i retning mot hva som kreves for å utføre kriminalitet i de oppsatte grupperingene. Kontaktnettverk, posisjon eller forståelse av samfunn og systemer virker å være elementer av betydning, eller muligheter som kan følge av slike knytninger. Bedragerier synes likevel å være mulig å utføre uten de store kontaktnettverkene og posisjonene.

Figur 13 Kjennetegn målt som medianverdier fordelt over utvalgte kriminalitetsformer

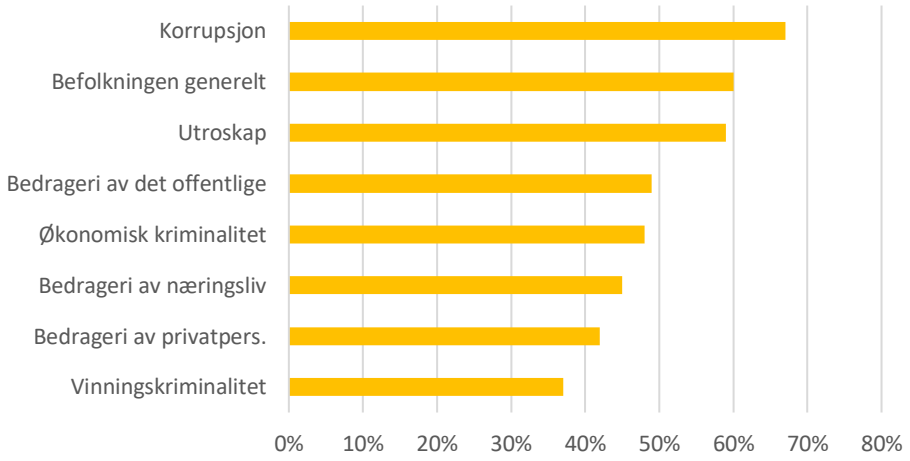
Bildet av den typiske bedrager som relativt ung og uetablert, kan sees i sammenheng med at bedrageriformer som utføres av norske gjerningspersoner, utføres uten bruk av store ressurser, med løse og uformelle nettverk. Det finnes eksempler på mer etablerte og profesjonelle bedrageri-aktører, men disse utgjør sannsynligvis en mindre andel av totalen. Den kvalitative analysen viser at ulike typer aktører gjerne utfører ulike typer av bedragerier. Eksempelvis utføres kortbedrageri (*Card Present*) uten de store ressursene, mens nettbankbedrageri krever mer kunnskap og ressurser.

9.2 LØS TILKNYTNING TIL ARBEIDSLIVET

En typisk bedrager av næringsliv eller privatpersoner har en løsere tilknytning til arbeidslivet enn «folk flest». Figur 14 viser gjennomsnittlig andel personer med et eller flere ansettelsesforhold per 1.oktober 2018 fordelt over «kriminalitetsformer» (grupper av personer anmeldt for kriminalitetsformene). Blant folkeregistrerte i Norge (i aldersgruppen 16–70 år) er i snitt 60 prosent registrert ansatt i minst én stilling per 1. oktober 2018. Blant bedragere av næringsliv og privatpersoner (i samme aldersgruppe) er de samme andelene 45-46 prosent. De fleste gruppene av anmeldte personer har i gjennomsnitt svakere tilknytning til arbeidslivet enn «folk flest». Dette kan til en viss grad være påvirket av avbrutte arbeidsforhold som følge av avdekket kriminalitet mot

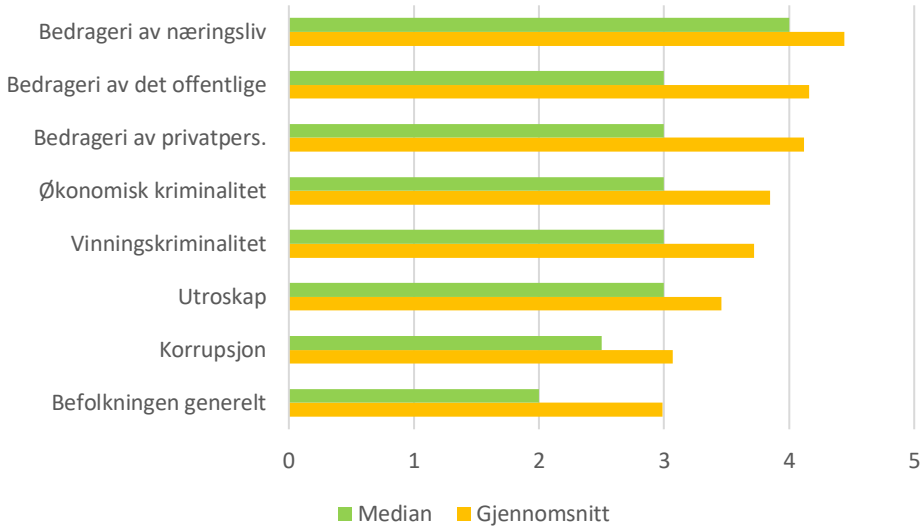
arbeidsgiver eller gjennom foretaket gjerningsperson er ansatt i. Resultatet kan også være påvirket av eventuelle soningsopphold.

Figur 14 og 15 viser at en typisk bedrager av næringsliv ikke er knyttet til arbeidslivet i form av en ansettelse.



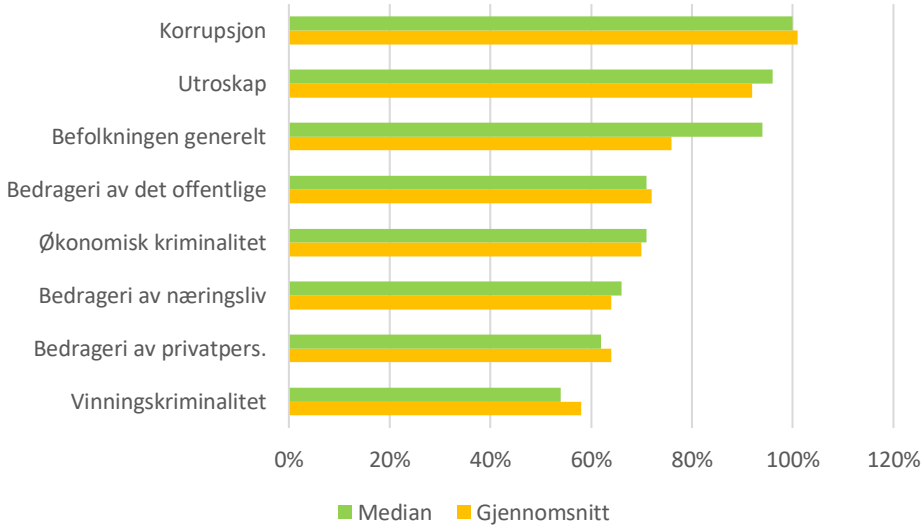
Figur 14 Andel i ansettelsesforhold per 1. okt. 2018

Figur 15 viser gjennomsnittlig antall arbeidsgivere (samt median) blant personer som er i arbeid, fordelt over de ulike kriminalitetsformene. Blant personer som *er* i arbeid, har bedragere typisk det høyeste antallet arbeidsgivere. Av de som *er* i arbeid, har medianen blant bedragere av næringslivet dobbelt så mange arbeidsgivere som befolkningen generelt, men likevel i sum en lavere stillingsprosent. De andre gruppene med kriminelle har også typisk flere arbeidsgivere. I motsetning til bedragere som ofte har flere arbeidsgivere men lav stillingsprosent totalt, har utro og korrupte personer nokså høye stillingsprosenter.



Figur 15 Antall arbeidsgivere, dersom i arbeid

Figur 16 viser gjennomsnittlig prosent stilling for personer som er i arbeid, fordelt over de ulike kriminalitetsformene. Vinningskriminelle og bedragere tilhører de gruppene med gjennomsnittlig lavest stillingsprosent (hvis i arbeid).

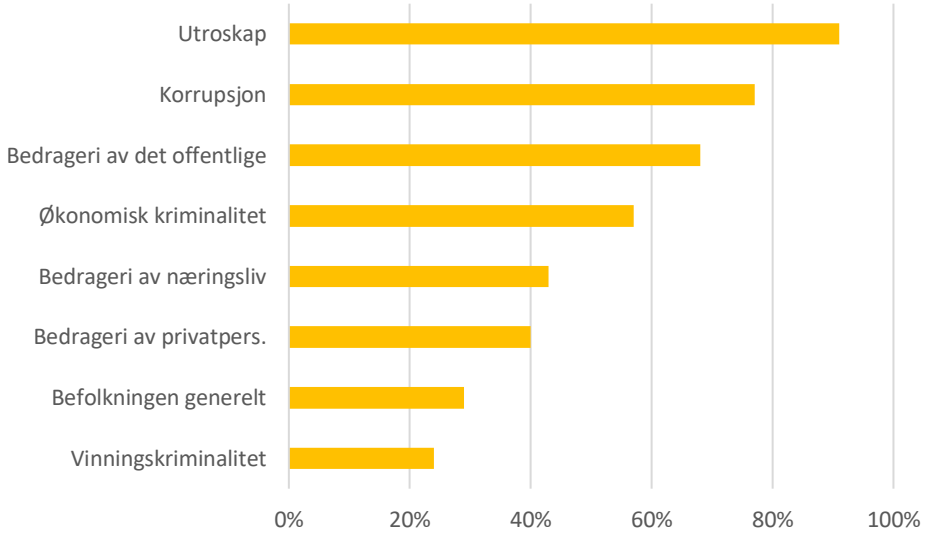


Figur 16 Prosent stilling, dersom i arbeid

Figur 14, 15 og 16 viser at bedragere har en løsere tilknytning til arbeidslivet på flere ulike måter. Enten ved at de ikke har noe formelt ansettelsesforhold, eller ved at de har mange stillinger med lav stillingsprosent, spredt på flere ulike arbeidsgivere.

9.3 LEDENDE ROLLER

Medianpersonen som er anmeldt for bedrageri av næringsliv eller privatpersoner har typisk ikke ledende roller i næringslivet. Det samme gjelder i befolkningen generelt og blant vinningskriminelle. På den annen side fremgår det at medianpersonen blant de som er anmeldt for økonomisk kriminalitet, bedrageri av det offentlige, korrupsjon og utroskap typisk *har* en ledende rolle i næringslivet. Figur 17 viser andelen med ledende roller i næringslivet i tidsperioden.



Figur 17 Gjennomsnittlig andel med ledende roller i næringslivet

De fleste gruppene av anmeldte personer, inkludert bedragere, har oftere enn «folk flest» ledende roller i næringslivet. Blant gjennomsnittspersoner i Norge (Folkeregisteret, i aldersgruppen 16-70 år) er 29 prosent registrert i minst en nåværende eller historisk ledende rolle i næringslivet. Blant bedragere av næringsliv og privatpersoner (i samme aldersgruppe) er de samme andelene henholdsvis 43 og 40 prosent. Blant personer anmeldt for økonomisk kriminalitet, bedrageri mot det offentlige, utroskap eller korrupsjon er tallene enda høyere (fra 57 til 91 prosent). Disse kriminelle gruppene har altså i større grad enn folk flest ledende roller i næringslivet. Dette funnet kan sees i sammenheng med at noen kriminelle bruker foretak som et skalkeskjul for kriminalitet.[147]

147 Nasjonalt tverretatlig analyse- og etterretningssenter 2017, *Situasjonsbeskrivelse av arbeidslivskriminalitet i Norge*, s. 7 og Nasjonalt tverretatlig analyse- og etterretningssenter 2018 *Kriminelle i arbeidslivet*, s. 13

I befolkningen generelt er den typiske ledende rollen styremedlem (både median og gjennomsnitt), dersom man har en ledende rolle. De vanligste rollene blant personer anmeldt for bedrageri av næringsliv, privatpersoner eller det offentlige, utroskap eller korrupsjon er innehaver av enkeltpersonforetak, daglig leder og leder.

- 29 prosent av de som er anmeldt for bedrageri av næringsliv har hatt rolle som innehaver, 21 prosent som daglig leder og 16 prosent som leder
- 37 prosent av de som er anmeldt for økonomisk kriminalitet har hatt rolle som innehaver
- 69 prosent av de som er anmeldt for utroskap har hatt en rolle som leder
- I befolkningen generelt har 11 prosent hatt en rolle som styremedlem, 10 prosent som innehaver og 6 prosent som leder

10 KJENNETEGN VED FORNÆRMEDE

Noen grupper av virksomheter peker seg ut med høy tilbøyelighet til å anmelde bedragerier. Høy tilbøyelighet til å anmelde er ikke nødvendigvis det samme som høy sårbarhet for bedragerier. Noen virksomheter har i større grad enn andre ressurser og rutiner på plass som bidrar til at bedragerier i større grad anmeldes, mens andre virksomheter kan være like utsatt, men unnlate å anmelde.

Resultatene under baserer seg på to ulike regresjonsmodeller, som i noe ulik grad kan antas å fange opp forskjellen mellom tilbøyelighet til å anmelde og reell sårbarhet.[148]

Bransjer som peker seg ut som mer sårbare er finanssektoren, overnatting, produksjon av tekstiler og produksjon av nærings- og nytelsesmidler. Det er ikke overraskende at finanssektoren skiller seg ut, da de forvalter attraktive ressurser. Når det gjelder foretaksstørrelse målt som antall ansatte, fremkommer ingen lineær effekt (gradvis økning av sannsynligheten med høyere eller lavere foretaksstørrelse). Imidlertid skiller de aller største foretakene seg ut (mer enn 100 ansatte) med både høy anmeldelsestilbøyelighet og -intensitet. I intervjuer pekes små foretak ut som særlig sårbare, og det kan ikke utelukkes at den kvantitative analysen ikke i tilstrekkelig grad fanger opp disse.

Når det gjelder foretaksalder, synes eldre foretak å ha en sterkere tilbøyelighet til å anmelde bedragerier enn yngre foretak. Ved kun å se på foretak som har anmeldt minst ett bedrageri, blir det imidlertid tydelig at yngre foretak skiller seg ut med høyere antall anmeldelser enn eldre foretak (høyere anmeldelsesintensitet). En mulig forklaring er at eldre foretak i større grad anmelder bedragerier, mens yngre foretak oftere bedras, men sjeldnere anmelder. Nyetablerte foretak er attraktive mål for blant annet katalogsvindel, hvor bedragere frister med markedsføring på nettsider som viser seg å ha lave besøkstall. Nyetablerte har sjeldent rukket å etablere tilstrekkelig med rutiner, og kan dermed være mer sårbare for bedragerier på generell basis.

148 I hovedmodellen sammenliknes virksomheter som anmelder bedragerier med virksomheter som ikke anmelder i en *logit*-modell (anmeldelses*tilbøyelighet*). I den alternative modellen analyseres *antallet* anmeldelser gitt at virksomheten er registrert med én eller flere anmeldelser, i en lineær regresjonsmodell (anmeldelses*intensitet*). I sistnevnte modell har virksomhetene som er inkluderte i analysen allerede illustrert at de har en positiv tilbøyelighet til å anmelde, imidlertid introduseres andre svakheter, eksempelvis ved at størrelsen på datasettet reduseres. Resultater som nevnes her er resultater som følger av begge modellene.

11 NÆRINGSLIVETS ROLLE

Systemene som muliggjør handel er de samme som muliggjør bedragerier.[149] Ved å unnlate å sørge for tilstrekkelige kontrollmekanismer i sine systemer, legger næringslivet til rette for at bedragerier kan utføres. Dette gjør næringslivet ikke bare til *offer* for bedrageri, men også til en *arena* for bedrageri. I hvilken grad man prioriterer slike kontrollmekanismer, avhenger blant annet av hvor sterk salgskulturen i foretaket er, i forhold til sikkerhetskulturen.[150]

I dagens samfunn forventes det brukervennlige og raske løsninger hva gjelder betalingsløsninger, registrering av kundeforhold og levering av varer og tjenester. Vegen fra en utviklet idé til et produkt unnfanges og leveres på markedet skal være rask og effektiv («Time to market»). Dette kan bidra til at foretaket tar både snarveier og beslutninger som øker sårbarheten for bedrageri og dataangrep. Foretaket må foreta en avveining av brukervennlighet mot kontrollmekanismer.

Det er store mørketall knyttet til bedragerier og sikkerhetsbrudd overfor foretak i næringslivet. Lave anmeldelsestall fra næringslivet kan antageligvis skyldes at omtale av bedrageriet vil avsløre for omverdenen at foretaket har svake interne rutiner, noe som igjen kan svekke foretakets omdømme.

11.1.1 Der bedrageriforsøk mislykkes

Ved hjelp av gode interne rutiner og sikkerhetsbevisste medarbeidere kan forsøk på bedrageri avverges av foretaket. De store foretakene har ofte gode sikkerhetsrutiner, men små og mellomstore foretak har i mange tilfeller ikke kompetanse og/eller ressurser til å prioritere dette.

Foretakets revisor eller regnskapsfører kan også, gjennom kunnskap om indikatorer på bedragerier, bidra til å avverge forsøk. Foretakets samarbeidspartnere kan også spille en rolle ved avdekking av bedrageriforsøk. For eksempel når en kunde oppdager at et kontonummer i faktura er endret, og melder fra til foretaket om dette.

---

149 Brottsförebyggande rådet, *Bedrägeribrottsligheten i Sverige, Rapport 2016:9*, s. 174
150 Ibid.

Foretakets bankforbindelse kan spille en viktig rolle i å avverge tap i forbindelse med bedrageriforsøk. Bankenes elektroniske overvåkningssystemer gjør de i stand til å oppdage mistenkelige transaksjoner, og i mange tilfeller stanse disse. Dersom transaksjonen er utført, kan banken reklamere på transaksjonen til mottakerbanken, med bedrageri som begrunnelse. Transaksjonen stanses, og kontoen i mottakerbanken kan sperres. Indikatorer på mistenkelige transaksjoner for banken kan være endring av kontonummer til en mottakerkonto som banken tidligere har identifisert som mistenkelig, eller overføring fra en bedriftskunde til en privatperson i et høyrisikoland.

Ifølge Enheten for finansiell etterretning (EFE) i ØKOKRIM, blir bankene stadig dyktigere i å stanse mistenkelige utenlandstransaksjoner. Som en konsekvens har antall norske muldyrkontoer økt betraktelig.[151] Når en muldyrkonto avdekkes, avslutter banken kundeforholdet til innehaveren av denne. På dette området er det større etterlevelse hos de store bankene enn de mindre – noe som medfører at muldyr flytter kontoene sine til mindre banker.

151 Betegnelsen muldyrkonto benyttes om bankkonto som tjener som mellomstasjon for utbyttet av en straffbar handling, med formål å tilsløre pengesporet av utbyttet.

12 POLITIETS STRAFFESAKSBEHANDLING AV BEDRAGERI

Ti prosent av virksomheter har i løpet av siste år opplevd lovbrudd som de ikke har anmeldt. De to mest utbredte forklaringene er at politiet som regel henlegger saken, og at det for tid- og ressurskrevende å anmelde.[152] I tillegg oppgir aktører fra næringslivet at de ikke anmelder bedragerier fordi de ikke har tiltro til at en etterforskning vil skaffe tilveie det tapte beløpet.

Norsk politi sin innsats mot bedrageri er, med noen få unntak, i stor grad basert på reaktiv innsats, som sentreres rundt straffeforfølgning. Lovbrudd anmeldes, etterforskes og gjerningspersoner straffeforfølges, se figur 18. I andre land ser man imidlertid at det brukes ressurser på å bekjempe teknologiske, finansielle eller kommunikative drivere bak bedrageri og datakriminalitet, fortrinnsvis i samarbeid med internettilbydere, banker og teletilbydere. Samarbeid med disse tjenestetilbyderne gir mulighet til å respondere og iverksette tiltak raskt.

Figur 18: Reaktiv modell

152 Næringslivets sikkerhetsråd. Kriminalitets- og sikkerhetsundersøkelsen i Norge 2017, s. 35.

12.1.1 Anmeldelser

I Intervjuene fremkom det at det opplevdes unødvendig ressurskrevende å anmelde et lovbrudd. Et intervjuobjekt forklarte det slik:

> «(..) det er ressurskrevende å skulle levere anmeldelse til politiet. En må ta seg fri en dag for å reise til stasjonen og sitte i vakta der. Politiet trenger masse info som ikke kan leveres i skranken.»

Antakelsen om at det kreves oppmøte hos politiet for å levere anmeldelse var utbredt blant intervjuobjektene. Fysisk oppmøte er tidkrevende fordi det må påregnes venting på politistasjonen og tapt arbeidstid. I tillegg kreves det dokumentasjon på det straffbare forholdet som ikke kan leveres der og da. I praksis innebærer dette at fornærmede må innhente og ettersende dokumentasjon.

Det er imidlertid ikke krav om personlig oppmøte på politistasjon ved innlevering av anmeldelse til politiet. Politiet plikter å ta imot anmeldelser uavhengig av hvilken form den inngis i. En anmeldelse kan altså leveres per post, e-post eller til og med muntlig.[153] Det kan likevel være hensiktsmessig med dialog med politiet i komplekse saker slik at hendelsesforløpet gjøres forstått og at politiet kan iverksette eventuelle tiltak.

Digital kriminalitet krever digitale løsninger. I Sverige og Danmark er det åpnet for å anmelde bedrageri og datakriminalitet over internett. Det antas å være tidsbesparende. I Norge er det foreløpig mulig med mindre alvorlige forhold som tyveri og skadeverk. I Storbritannia kan foretak kontakte politiet på telefon det etterfølgende døgnet etter at de er utsatt for dataangrep eller digitalt bedrageri.[154]

12.1.2 Å se saker i sammenheng

De som utsettes for systematiske bedrageri er bosatt over hele landet, noe som medfører at sakene registreres i ulike politidistrikt. Slik blir bedragerisaker med fellesnevnere gjerne registrert hos politiet uten at eventuelle likhetstrekk avdekkes. En ansatt i politiet forklarer det slik:

> «Vi ser ikke, eller i svært liten grad, etter sammenhenger – blir målt på restanser og har derfor ikke anledning til å se etter sammenhenger mellom saker.»

Intervjuobjekter både i politi og næringsliv etterlyser nasjonal koordinering av bedragerianmeldelser og anmeldelser av datakriminalitet, for bedre å se saker i sammenheng. For å avdekke anmeldelser med fellestrekk er det viktig at;

- det straffbare forholdet registreres med riktig straffesakskode (STRASAK-kode)
- informasjon om nye modus og trender deles med politiet for øvrig, slik at politiansatte har kunnskap til å finne likhetstrekk mellom saker.

I Sverige ble Nationellt bedrägericenter (NBC) opprettet i 2014 som et tiltak i den svenske satsingen mot bedrageri. Senteret er underlagt politiet i Stockholm, men har som formål å identifisere bedragerilovbrudd med nasjonale forgreninger og samordne politiets ressurser i bekjempelsen av bedragerier. I sitt arbeid prioriterer NBC metode-

---

153 Tidligere var det også krav om at styreleder i et foretak måtte begjære offentlig påtale av straffbare handlinger til politiet, med mindre det var gitt fullmakt til styremedlem, daglig leder eller medelt prokura. Denne bestemmelsen er nå opphevet ved innføring av straffeloven av 2005.

154 www.actionfraudpolice.uk/campaign/24-7-live-cyber-reporting-for-businesses. (Lesedato: 10.2.2019)

utvikling, forebygging og politioperativt arbeid som identifiserer bedragerilovbrudd med nasjonale forgreninger. NBC har mulighet til å delegere ansvar for etterforskning i bedragerisaker med fellestrekk til andre politidistrikt. Selv om senteret ikke har mandat til å følge opp distriktets håndtering av saken, er det av avgjørende betydning at NBC ser saker i sammenheng på et nasjonalt nivå.

12.1.3 Oppklaringsprosent og henleggelser

Bedragerier har lavere oppklaringsprosent enn gjennomsnittet av alle lovbruddstyper. Av de 15 169 bedrageriene som ble etterforsket i 2017 ble 26 prosent oppklart. Til sammenligning var gjennomsnittlig oppklaringsprosent for alle lovbruddstyper 51 prosent samme år. Grovt bedrageri har imidlertid oppklaringsprosent på 71 prosent. Oppklaringsprosenten for ID-krenkelser og inntrengning i data- og kommunikasjonssystem ligger mellom 10 og 17 prosent.[155]

Den forholdsvis lave oppklaringsprosenten tilsier at flertallet av bedragerisaker, datainnbrudd og ID-krenkelser blir henlagt av politiet. Årsakene er sammensatte.

Bedragerier er ofte komplekse lovbrudd. Fremgangsmåtene er kreative. Det kan være krevende å definere hva slags lovbrudd som har blitt begått, eller om det har blitt begått lovbrudd i det hele tatt. Det er eksempler på at ansatte manipuleres til å overføre penger fra arbeidsgivers konto, og så mistenkes for å ha underslått penger selv, eller er en utro tjener som har medvirket til lovbruddet. Grensene for hva som er bedrageri, og hva som er villedende markedsføring kan også oppleves uklare.

Politiet er også opptatt av å etterforske de *riktige* sakene. Fornærmede i bedragerisaker forventes å bidra med dokumentasjon av ulik karakter. IP-logger, e-poster, betalingsinformasjon og skjermbilder er eksempler på slik dokumentasjon. En annen faktor som kan være avgjørende for om saken blir etterforsket er størrelsen på beløpet som er tapt.

Bedragerier begått fra utlandet, som mange av bedrageriene er, er spesielt krevende å etterforske. «Jeg tror ikke det er mange politidistrikt som etterforsker mot utlandet.», forklarer en etterforsker. «Etterforsking på tvers av landegrenser er ikke bare avhengig av kompetanse eller om det ligger en avtale til grunn, men et spørsmål om ressurser.»

12.1.4 Identifisere saker med økt sannsynlighet for oppklaring

I Storbritannia viser undersøkelser at oppklaringsprosent er høyere ved bedragerier hvor politiet responderer umiddelbart. Årsakene til at politiet agerer raskt kan være flere, men gjelder i hovedsak når bedrageriet er utført av en gjerningsperson som er fysisk til stede under bedrageriet. For eksempel var 37 prosent av bedrageriene politiet responderte raskt på uført av en ansatt, mens kun tre prosent var bedrageri utført ved IT-support. Ved sistnevnte type bedrageri har gjerningspersonen i hovedsak tilhold i utlandet og oppklaringsprosenten forventes i slike tilfeller å være lav. Dette illustrerer viktigheten av kategorisering av sakene på anmeldelsesstadiet.

Det anses mest hensiktsmessig å identifisere saker med indikatorer som tilsier økt oppklaringsprosent, og ikke bruke unødvendige ressurser på saker der gjerningspersonen er meget krevende å identifisere. Saker hvor gjerningspersonen befinner seg i utlandet

155 SSB: Tabell 09406

har lavere oppklaringsprosent. Her kan en proaktiv tilnærming til bedragerier være fornuftig.[156]

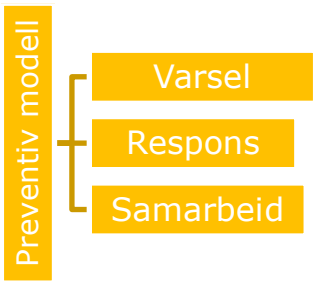
12.1.5 Rask respons ved digitale bedragerier

Digitale bedragerier er grenseløse og begås ofte fra utlandet. Ved hjelp av internett kan bedrageri begås i et stort omfang og hyppighet. Rask respons fra politiet sin side krever tydeliggjorte tiltak og et velfungerende samarbeid med relevante aktører.

> «Vannlekkasje gav umiddelbar utrykning, men nettsvindel for 730 000 kroner kunne ingen hjelpe med.»

Utsagnet fra en politiansatt belyser utfordringer ved politiets håndtering. Politiet responderer raskt på fysiske hendelser og har en klar idé om hvilke tiltak som må iverksettes. De har ikke tilsvarende kompetanse eller beredskap for hendelser i det digitale rom.

De lave anmeldelsestallene og oppklaringsprosenten for bedragerier og utvalgte former for datakriminalitet, tyder på at bedrageri har lav oppdagelsesrisiko, potensialet for stor økonomisk gevinst er stor for kriminelle og risikoen er lav for å bli straffeforfulgt. Suksessfaktoren i bekjempelse av bedrageri og datakriminalitet beskrives i å kunne supplere straffesakshåndteringen med proaktive tiltak. Ved en proaktiv tilnærming, som illustrert i figur 19, kreves det utstrakt samarbeid med private aktører og rask respons i tidskritiske saker. Dette er avgjørende for å sikre, stanse eller forfølge transaksjoner og digitale spor.



Figur 19: Preventiv modell

12.1.6 Forebygging

«Bedrageri kan ikke etterforskes bort. Til det er problemet for stort og ressursene for små.» Sitatet er fra en ansatt ved NBC. Også medarbeidere i politiet og næringslivet understreker at bedrageri i økende grad må forebygges. Forebygging kan utføres ved å;

- redusere mulighetene for at bedrageri blir begått
- øke oppdagelsesrisikoen ved bedrageri
- redusere vinningen[157]

Ved å informere næringslivet om fremgangsmåter og trender kan politiet sette næringslivet i stand til å sikre virksomheter mot bedrageri og datakriminalitet. Informasjon og samhandling vil redusere de kriminelles handlingsrom og øke oppdagelsesrisikoen. Fo-

156 The police foundation (2018), *More than just a number: Improving the police response to victims of fraud,* s. 33.

157 Ibid, s. 56

rebyggende virksomhet forutsetter tidsriktig kunnskap om hvilke bedragerimodi og dataangrep som opptrer til en hver tid.

En konsekvens av mørketallene innen bedrageri mot næringslivet er at politiet ikke er oppdatert på aktuelle modus og trender i Norge. Ingen aktører i Norge, hverken i politiet eller næringslivet innehar en fullstendig oversikt over antall utførte bedragerier. Det finnes heller ingen nasjonal oversikt over hvor mange som utsettes for de ulike formene for bedrageri, eller hvem som i størst grad utsettes for bedrageri.

Næringslivet besitter egne oversikter over dataangrep og bedrageri de utsettes for, men volumet er så stort at det er krevende å rapportere alle tilfeller til politiet. Politiet på sin side har informasjon basert på anmeldelser. Å samle denne kunnskapen er en forutsetning for å kunne informere publikum om hvilke typer bedrageri som er dagsaktuelle. Politi og næringslivsaktører er med andre ord gjensidig avhengig av hverandres informasjon om pågående trusler for å kunne forebygge fremtidige angrep.

12.1.7 Koordinert innsats mellom politi og næringsliv

Det er allerede etablert samarbeidsordninger mellom politi, næringslivet, finansbransjen og datasikkerhetsmiljøer. Politiet har opprettet næringslivskontakter i samtlige politidistrikt som skal sørge for et velfungerende samarbeid mellom politi, næringsliv, sikkerhetsmyndigheter og andre aktører i samfunnet. Gjennom forebyggende arbeid har de som mål å bidra til velrettede tiltak i næringslivet og sørge for en kunnskapsbasert kriminalitetsbekjempelse i politiet.[158]

FinansCERT og NorCert er eksempler på slike samarbeid. I Nordisk FinansCert utveksles det informasjon om modus og muldyr-kontoer, IP-adresser og variabler for å avdekke trojanere. De fleste nordiske banker er tilkoblet samarbeidsforumet.

Næringslivet påpeker at små og mellomstore foretak, som utgjør 90 prosent av norsk næringsliv, ikke har kapasitet og ressurser til å ta del i slike samarbeidsfora og dermed går glipp av viktig informasjon. Foretak har behov for tidsriktig informasjon for å iverksette sikkerhetstiltak. Det etterlyses derfor en form for varslingssystem.

Flere aktører i politiet og næringslivet knytter store forventninger til opprettelsen av politiets cyberkrimsenter (NC3) som skal bistå norsk politi i konkrete etterforskninger og videreutvikle spisskompetanse innenfor cyberområdet.[159]

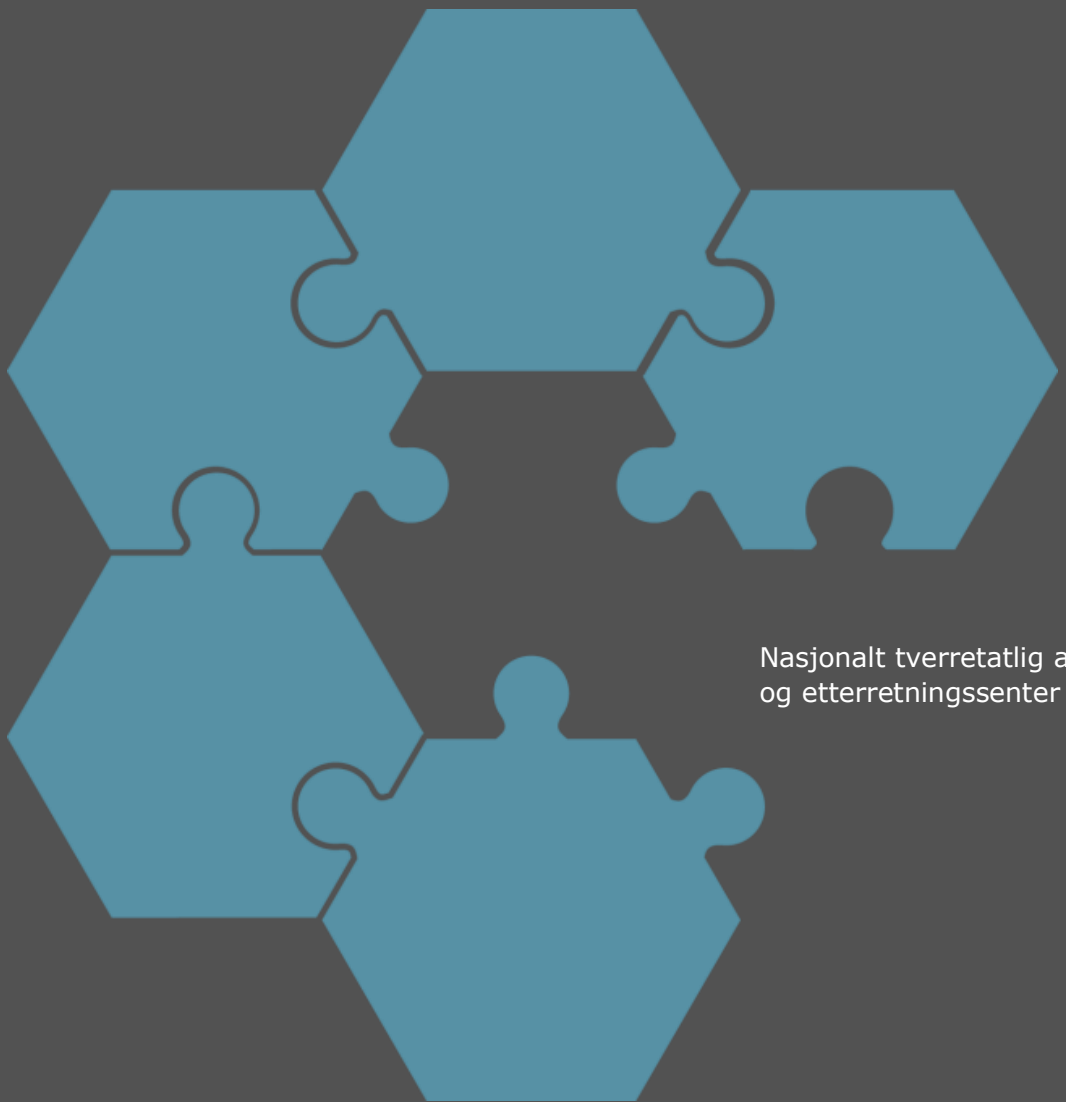
158 https://www.politiet.no/kontakt-oss/naringslivskontakter. (Lesedato: 12.2.2019).

159 https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2019/01/24/apning-nc3/. (Lesedato 12.02.2019).

Bedrageribekjempelsen i Storbritannia ble tidligere oppfattet som fragmentert og med manglende samarbeid mellom aktører. **The Joint Fraud Taskforce** ble etablert i 2016 for å bedre koordineringen mellom politiet og finanssektoren.

Politiets registrering av bedrageri var mangelfull fordi de ikke hadde god nok kompetanse, og dette var noe av årsaken til at det sentraliserte rapporteringssenteret **Action fraud** ble opprettet i 2013. Formålet med senteret var å redusere underrapporteringen av bedrageri og kvalitetssikre registrering både av anmeldelser og informasjon som tilfløt politiet. Dette skulle gi bedre etterretning og oversikt over kriminalitetsbildet, og dermed også et bedre grunnlag for å identifisere og delegere saker for etterforsking. Bedragerier kan rapporteres både digitalt og til et call-senter med utvidet åpningstid. Gjennom call-senteret åpnet politiet for en dialog med fornærmede slik at sistnevnte fikk en bedre forståelse av hva de var utsatt for og kunne videreformidle kontakt til aktører som kunne informere dem om tiltak som bør iverksettes.

The National Fraud Intelligence Bureau er etablert for å analysere innrapportert informasjon og distribuere det i ettretningspakker til lokale politidistrikt. (The police foundation 2018: More than just a number: Improving the police response to victims of fraud, s. 42–43.)



Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES)