POLITIET

Kriminalitet i og mot næringslivet

Trender og trusler

Sør-Øst politidistrikt 2018

Rapporten er utarbeidet av
Amund Rolseth og
Jarl Martin Pedersen

FORORD

Et av politiets fremtidsbilder i vår virksomhetsstrategi frem mot 2025, viser at vi skal forebygge målrettet med utgangspunkt i risikoanalyser og vurderinger. Vi skal ha god kunnskap om risiko og sårbarheter i samfunnet, kriminalitetsutvikling, fenomener og årsaker, både lokalt og nasjonalt. Vi skal samarbeide tett på tvers og med andre aktører, dele kunnskap og ha tilgjengelig kompetanse og virkemidler som benyttes fleksibelt og effektivt for å skape resultater.

Som politimester i Sør-Øst politidistrikt er jeg svært opptatt av, og stiller store krav til at vårt samfunnsoppdrag baserer seg på kunnskap på alle virksomhetsområder. Arbeidsmarkedskriminalitet, herunder næringskriminalitet er et av flere prioriterte området for 2018. Jeg er derfor svært fornøyd med at vi nå har fått utarbeidet denne rapporten som vil være et godt kunnskapsgrunnlag for det videre kriminalitetsforebyggende arbeidet innenfor næringslivskriminalitet.

For å gjennomføre gode risikovurdering er det nødvendig å ha oversikt over det faktiske trusselbildet. Som vi kan lese i rapporten er det derfor viktige at næringslivet selv kartlegger egne verdier og sårbarheter, slik at virksomhetene selv har oversikt over egen risikosituasjon. Dette blir faktisk det viktigste grunnlaget for å etablere gode strategier og tiltak for å styre risikoen.

Politiet skal frem mot 2025 komme i forkant av kriminaliteten. Kunnskapen vi tilegner oss gjennom risikoanalyser og vurderinger vil derfor være viktig kunnskap å dele for å mobilisere andre. Rapporten vil derfor ikke bare bli et godt kunnskapsgrunnlag for politiet, men også andre aktører innenfor næringslivet. Vi vil ved et slikt samarbeid uten tvil stå sterkere sammen i det kriminalitetsforebyggende arbeidet.

Jeg gleder meg til fortsettelsen til det beste for våre innbyggere og vårt næringsliv i Sør-Øst politidistrikt.

Christine Fossen
Politimester

Sør-Øst politidistrikt, Juni 2018

Innhold

SAMMENDRAG

Til tross for at næringslivet står for en veldig stor andel av Norges BNP og årlig blir utsatt for kriminelle handlinger som utgjør enorme summer, blir dette lite belyst i politiets egne kriminalitetsstatistikker. Dette skyldes ikke bare manglende mulighet i politiet til å hente ut hvor store verdier som har blitt stjålet/tapt, men fordi næringslivet selv i stor grad velger å ikke anmelde lovbruddene. Siden mørketallene er så store så har vi i denne rapporten valgt å sammenstille kunnskap som finnes utenfor politietaten.

Kriminalitet i og mot næringslivet er ikke et nytt fenomen, men vi ser likevel at det er i stor endring, og særlig da knyttet til digitalisering. Trussel- og sårbarhetsnivået knyttet til digitalisering gjelder for de aller fleste bransjer, og nevnes som et viktig tema i tiden fremover.[1] Kriminaliteten som skjer via digitale verktøy er i utgangspunktet ikke en ny type kriminalitet, men er tradisjonell kriminalitet med nye verktøy og ny modus. Som vi skal se senere i rapporten så er mørketallene veldig store, og politiet har lite oversikt over både kriminalitet i og mot næringslivet og IKT-kriminalitet generelt. Informasjonen som finnes i dag er veldig fragmentert, og fordelt på ulike enkeltvirksomheter eller paraplyorganisasjoner.

I rapporten fremheves seks trusler som vi vurderer som de mest aktuelle for næringslivet;

- Direktørsvindel
- Løsepengevirus
- Dataskadeverk/sabotasje
- Informasjonstyveri
- Innsidere
- Vold og trusler mot ansatte

De fire første truslene er digitale, mens de to siste har blitt trukket frem på grunn av deres viktighet knyttet til samfunnet (innsidere) og folks helse og trygghetsfølelse (vold og trusler).

Det er flere årsaker til at IKT-kriminalitet har blitt en så stor trussel. For det første er det veldig mye av kriminaliteten som forblir uoppdaget, og dette gjør at de kriminelle kan fortsette sin aktivitet lenge før de blir tatt. Hvis et lovbrudd blir oppdaget kan det ofte være vanskelig å gjøre noe når sporene går på kryss og tvers av landegrenser og dermed skaper utfordringer for politi og rettsvesen som må forholde seg til flere lands lovverk. For det andre bidrar lett tilgjengelig programvare for å begå kriminalitet med enkelt brukergrensesnitt til et økt trusselbilde. I motsetning til tidligere trenger man ikke særlig kompetanse for å drive med IKT-kriminalitet på et grunnleggende nivå. Samtidig har man de veldig kompetente kriminelle som har kapasitet til å gjennomføre store og kompliserte angrep. Selv om mange vil hevde at Norge er et land med jevnt over god beskyttelse, er det mange virksomheter som har manglende beskyttelse eller oversikt på potensielle trusler, noe som er med på å øke risikoen for å bli utsatt.

I et historisk perspektiv er kriminalitet med IKT-verktøy en forholdsvis ny disiplin, og en ser at mange kriminelle har veldig høy kapasitet, og tar i bruk stadig mer avanserte angrepsmetoder. I takt med utviklingen er det grunn til å tro at de kriminelle stadig kommer til å utvikle nye metoder for å tjene penger på kriminalitet, noe som betyr at virksomheter også må ta trusselen alvorlig.

For å gjennomføre en god risikovurdering er det nødvendig å ha oversikt over det faktiske trusselbildet. Denne rapporten bidrar til å beskrive trusselbildet. Like viktige er det at næringslivet selv kartlegger egne verdier og sårbarheter, slik at virksomhetene har oversikt over egen risikosituasjon. Det er det viktigste grunnlaget for å etablere gode strategier og tiltak for å styre risikoen.

Flere virksomheter har etterlyst en kanal hvor digitale hendelser kan rapporteres inn til politiet. I tillegg til å hjelpe næringslivet med å vurdere sin egen risiko, vil det også hjelpe politiet med å allokere sine ressurser på de områdene hvor det er størst behov. I så måte er denne rapporten bare et første steg for politidistriktet i retning av et oversiktsbilde.

[1] Finans Norge (2016)

DEL 1:
INTRODUKSJON

Samfunns- og kriminalitetsutvikling

Som med resten av samfunnet er kriminalitetsbildet i stadig endring. Ny teknologi åpner for nye metoder til å begå kriminalitet, noe som medfører at virksomheter og privatpersoner må endre sikkerhetsrutinene de har hatt før. Kriminelle på sin side tilpasser seg stadig de nye sikkerhetsrutinene, og utvikler kontinuerlig verktøy for å kunne begå lovbrudd. Den raske utviklingstakten krever at kompetanse oppdateres, og har medført at politiet og lovverket henger etter innen IKT-feltet. I en veldig stor andel av sakene hvor IKT har blitt brukt som verktøy finner man digitale spor som leder til utlandet, og mangelen på gode internasjonale avtaler og ulik lovgivning gjør at det er vanskelig både å etterforske samt avgjøre sakene. Manglende datalagringstid er også et aspekt som skaper utfordringer for etterforskningen, og ofte vil relevante spor være slettet før politiet har hatt mulighet til å hente ut relevant data.

Det er også en tendens til økt profesjonalisering av kriminalitet, hvor de kriminelle bruker utdannede fagfolk[2], som for eksempel revisorer, advokater, leger, og lignende for å bidra i kriminalitetsutøvelsen. Dette gjelder også for kriminalitet begått med IKT, som nå ikke lengre er forbeholdt personer med digital kompetanse. Det har blitt skapt et marked for utvikling av programvare som kun er til kriminelle formål[3], og som selges til personer som bruker verktøyene for å utføre kriminelle handlinger. En ser også at det er enklere enn noensinne å finne kompetente personer til å hjelpe seg med å utføre kriminalitet. Kriminelle fora og ulike kommunikasjonsplattformer fungerer som møte- og markedsplasser for kriminelle hvor de kan dele erfaringer og kunnskap, samt selge tjenester til hverandre.[4]

Kriminaliteten har det siste tiåret beveget seg fra den fysiske til den digitale verden, og det meste tyder på at denne utviklingen kommer til å fortsette, og sannsynligvis styrkes. Veksten i antall internettbrukere har vokst voldsomt siden årtusenskiftet fra omtrent 250 millioner brukere, via 1,8 milliarder brukere i 2010, og til 4,1 milliarder brukere i slutten av 2017[5]. Over halvparten av verdens befolkning er med andre ord tilkoblet til internett. Samtidig med økningen av brukere har det vært en enda større økning i enheter tilkoblet internett, og begrepet "tingenes internett"[6] er et mye brukt uttrykk. Mens de tilkoblede enhetene i begynnelsen av 2000-tallet gjerne var datamaskiner og mobiltelefoner, finnes det nå ingen grenser for hva som er koblet opp mot internett. Det er i dag mulig å ha lyspærer, vannkokere, teddybjørner, madrasser, og en hel del andre dagligdagse produkter samt industrirelaterte produkter tilkoblet internett. Dette gjør at antall tilkoblede enheter er mye større enn antall brukere, og i 2017 var det flere enn 27 milliarder tilkoblede enheter. Innen 2030 er det anslått at det kommer til å være over 125 milliarder enheter tilkoblet internett.[7]

Omfang og mørketall

På 2010-tallet har den registrerte kriminaliteten vært stadig synkende, og nådde et nytt lavpunkt med 318 617 anmeldelser i 2017, mot 394 137 i 2010. Nedgangen kan være reell – altså at det foregår færre kriminelle handlinger enn tidligere, men det kan også være at mørketallene er større i dag enn de var for noen år tilbake. Bruken av digitale produkter og internett har vært sterkt økende over lengre tid, og dermed også muligheten for å begå kriminelle handlinger i via nettet. Det er mye som tilsier at kriminaliteten har endret arena og forflyttet seg til den digitale sfæren. Flere virksomheter og organisasjoner rapporterer om øk-

[2] NTAES (2017a)
[3] Norsis (2017b)
[4] Europol (2017)
[5] Internet World Stats (2018)
[6] Også kjent som Internet of Things (IoT)
[7] IHS (2017)

ning i uønskede hendelser innenfor sin bransje, og bare en liten andel av disse anmeldes.

Ser vi på alle typer kriminalitet virksomheter blir utsatt for, så rapporterte kun ti prosent av virksomhetene at de har opplevd lovbrudd som de ikke har anmeldt. Fordelingen på hvilken type kriminalitet virksomhetene ikke anmelder er[8]:

- 63 prosent vinningskriminalitet
- 16 prosent økonomisk kriminalitet,
- 10 prosent IKT- kriminalitet
- 20 prosent annen type kriminalitet

Som vi kan se er mørketallene i *antall* lovbrudd størst blant vinningskriminaliteten. Det er ikke lett å estimere en sum hvor mye norske virksomheter taper på vinningslovbrudd i løpet av et år, men det er antakelig snakk om store summer. Samtidig er vinningskriminalitet en vedvarende trussel og har vært det i mange tiår, noe som gjør at stort sett alle virksomheter har gjennomført trusselvurderinger eller forebyggende tiltak for å forhindre den. I denne rapporten vurderer vi heller den digitale trusselen til å være større basert på omfang, mulige konsekvenser for virksomheter, og virksomhetenes sårbarhet for IKT-kriminalitet.

I tillegg til digitale trusler vurderer vi også innsidere samt vold og trusler mot ansatte som to viktige områder. Innsidertrusselen har i de senere årene blitt mer aktuell med korrupsjonssaker og økt fokus på trusselen fra sikkerhetstjenestens side. Dette er en trussel som har potensiale til å skade både folkets tillit til rettsstaten, rikets sikkerhet, og virksomheters lønnsomhet. Vold og trusler mot ansatte mener vi bør ha økt oppmerksomhet både på grunn av det store omfanget og på grunn av konsekvensene det kan ha for de ansattes personlige helse og arbeidsmiljø.

[8] NSR (2017). Prosentene er ikke kumulative, og en virksomhet kan være offer for flere enn én av de fire punktene.

Omfang av IKT-kriminalitet

Mørketallsundersøkelsen fra 2016 viser at 27 % av virksomhetene sa at de ble utsatt for uønskede digitale sikkerhetshendelser det siste året. Det er med andre ord liten tvil om at det er et stort avvik mellom antall lovbrudd næringslivet blir utsatt for, og hvor mange som blir anmeldt til politiet. Hvis man hadde tatt utgangspunkt i dette omfanget i Sør-Øst så ville dette tilsvart 3564 hendelser i 2017[9], og for landet som helhet 27455 hendelser.[10] Selv om politiet ikke har en egen statistikk over hvor mange lovbrudd næringslivet har blitt utsatt for, kan man sammenligne tallene med anmeldelser innenfor økonomikapittelet. I Sør-Øst ble det registrert 3403 saker innen økonomisk kriminalitet, og godt over halvparten av disse er lovbrudd begått mot privatpersoner. Politiet får med andre ord mange færre anmeldelser enn de kunne fått om alle lovbrudd hadde blitt anmeldt.

Et tegn på at mørketallene i Norge er store kan vi se når vi sammenligner antall anmeldelser på bedragerier i Norge med våre naboland. I 2017 ble det anmeldt 198 227 bedragerier i Sverige[11], 44 550 i Danmark[12], mens det i Norge ble anmeldt 19 097 saker. Selv om forskjeller i kriminalitetsrate, klassifisering av lovbrudd, og forskjeller i straffelovene nok forklarer en del av forskjellen, så utgjør den nok ikke alt. Ser vi på utvikling over tid har antallet bedragerianmeldelser i Norge vært lavest i Skandinavia. I perioden 2007-2017 økte antallet anmeldelser med 41 % i Norge, 118 % i Sverige, og 546 % i Danmark. Sør-Øst ligger lavere enn alle disse med 19 % økning.[13]

[9] Gitt at hver utsatte virksomhet kun blir utsatt for én hendelse. Sannsynligvis vil nok snittet være høyt over 1, og antallet hendelser derfor være tilsvarende høyere.

[10] Basert på henholdsvis 13 201 og 101 685 virksomheter med flere enn fem ansatte ifølge SSB (2018)

[11] BRÅ (2018)

[12] DST (2018)

[13] Det er noen problemer med de Norske tallene knyttet opp mot innføringen av den nye straffeloven i slutten av 2015 som også førte til endring av statistikkgrupper. Vi kan ikke

13 prosent har blitt utsatt for direktørsvindel det siste året, og for ni prosent av disse medførte det et økonomisk tap.[14] Om man ser overordnet på alle typer IKT-kriminalitet så uttalte syv prosent at deres virksomhet hadde blitt utsatt for digitale hendelser som hadde ført til tap av omdømme eller kontrakter, beslaglegging av interne ressurser, eller direkte økonomiske tap.[15]

Et annet eksempel på den enorme mengden lovbrudd som ikke blir anmeldt kan en se i et stort norsk programvareselskap som opplever omtrent 800 000 angrepsforsøk på hver av sine 300 tjenester per måned. Av disse angrepene er 2400 per måned så alvorlige at de selv bruker ressurser, og i utgangspunktet ønsker å anmelde. I et oppstartet samarbeid med Oslo PD foreslår de på grunn av kapasitetshensyn i politiet at de begynner med å anmelde 2-3 saker per måned.[16] Med andre ord betyr det at mørketallene fra denne virksomheten alene utgjør 28 000 saker per år – tilsvarende ni prosent av hele landets straffesaker. Legger man til andre virksomheter som har samme anmeldelsesrate så ser man at avviket mellom registrert kriminalitet innen den digitale sfæren og den faktiske kriminaliteten er så stor at politiet ikke er i nærheten av å ha kapasitet nok til å etterforske sakene.

46 prosent av virksomhetene sier at de oppdagede sikkerhetshendelsene ble oppdaget ved en tilfeldighet[17], noe som betyr at det sannsynligvis er et stort avvik mellom virksomhetenes faktiske utsatthet for IKT-kriminalitet og det de oppdager selv. Samtidig er det nok også en utfordring for virksomhetene å vite om det er snakk om en kriminell handling som skal anmeldes, eller kun en hendelse.

I følge mørketallsundersøkelsen er det virus og skadevare som forårsaker de verste IKT-relaterte hendelsene, hvor 32 % rapporterer at de ble rammet av uspesifiserte virus eller skadevare, med løsepengevirus som den verste hendelsen. Blant de som blir utsatt for de uønskede sikkerhetshendelsene er det ekstraarbeid i form av arbeidstimer som er den mest aktuelle konsekvensen. Kun 12 % oppgir derimot at de har hatt direkte kostnader knyttet til hendelsen(e).[18] Selv om fokuset til de fleste virksomheter er på de største hendelsene, og at man ikke har kapasitet til å ha fokus på alle de små, så utgjør også angrep med «high volume – low impact» en stor trussel fordi det totalt sett er snakk om store summer. Betalingssvindel er et eksempel på en slik problemstilling, og er et område hvor en ikke helt klarer å se hvor stort problem det er basert på lokal rapportering eller enkeltetterforskninger. [19]

Typer trusselaktører

Det er vanskelig å generalisere når en skal beskrive de typiske kriminelle som bruker IKT-verktøy i utførelsen av sin kriminalitet, og ut fra nåværende kunnskapsbilde gir det i et kriminalitetsforebyggende perspektiv ikke så mye mening å snakke om demografiske faktorer som alder, kjønn, utdanning, og lignende. Lovbruddene foregår gjerne der hvor de kriminelle holder til, noe som gjerne er veldig langt unna der hvor ofrenes server er. En vil med andre ord ikke nødvendigvis forebygge kriminalitet i Sør-Øst ved å kontakte aktuelle personer som sitter i politidistriktet. En kan likevel kategorisere IKT-kriminelle i et hierarki, som sett i Telenors rapport «Digital Sikkerhet». [20]Som tabellen på neste side viser, er det fem forskjellige kategorier, hvor kapasiteten er større jo høyere opp i hierarkiet man kommer.

utelukke at lignende endringer i Sverige og Danmark forklarer en del av deres økning.

[14] NSR (2017)

[15] BDO (2017)

[16] Internt notat i Oslo PD 9. april 2018

[17] NSR (2016)

[18] NSR (2016)

[19] Europol (2017)

[20] Telenor (2017)

Stater

- Stater (sammen med kontraktører) har ressurser og kapasitet til å drive avanserte og skjulte operasjoner over lengre tid

Kontraktører

- Kontraktørene utfører oppdrag på bestilling fra andre, og kan like gjerne utføres på vegne av stater (spionasje) så vel som næringsliv (industrispionasje)

Organiserte kriminelle

- De organiserte kriminelle driver med flere typer kriminalitet og gjerne veldig alvorlig kriminalitet som hvitvasking av penger fra narkotikaomsetning til menneskehandel og terrorfinansiering. Man ser at organiserte cyberkriminelle nå også har tilgang til verktøy som tidligere har vært forbeholdt stater og kontraktører.

Politisk motiverte "hacktivister"

- Hacktivistene har gjerne en politisk agenda som de prøver å presse frem ved å gjennomføre angrep på systemer, for eksempel nettsider som blir endret til å vise innhold hacktivistene ønsker å vise frem.

Enkeltkriminelle og svindlere

- Denne gruppen er utvilsomt den største - og kanskje den som øker mest, og består først og fremst av personer som er ute etter økonomisk profitt, eller personer som ønsker å vise frem som tekniske kompetanse for å få innpass høyere i hierarkiet.

DEL 2:
TRUSLER

Trusler i og mot næringslivet

Dataangrep blir nevnt som norske lederes største frykt, foran tema som konjunkturnedgang og finanskrise[21], og privatpersoner ser på digitale trusler som den største bekymringen de neste fem årene[22]. Frykten for cyberangrep er ikke helt ubegrunnet, og nasjonal sikkerhetsmyndighet har gjennom flere år sett en økning av antall målrettede angrep mot private og offentlige interesser. Samtidig som det skjer flere cyberangrep, ser man at disse blir stadig mer avanserte og profesjonelt utført, noe som fører til at store økonomiske verdier går tapt hvert år.[23] Når ledere og privatpersoner for øvrig nevner den digitale sfæren som en kilde til bekymring så er det paradoksalt at seks av ti bedrifter ikke har informasjons- og IKT-sikkerhet som en del av virksomhetens risikostyring, og én av fire mener de ikke er tilfredsstillende rustet mot dataangrep.[24]

Vi har vurdert seks trusler som de mest aktuelle for næringslivet:

- Direktørsvindel
- Løsepengevirus
- Dataskadeverk/sabotasje
- Informasjonstyveri
- Innsidere
- Vold og trusler mot ansatte

Arbeidslivskriminalitet er en av politiets prioriterte områder, og vi vurderer ikke dette under de seks ovennevnte punktene, men henviser heller til Sør-Øst akrim-rapport fra 2017, eller Nasjonalt tverretatlig analyse- og etterretningssenters situasjonsbeskrivelse fra samme år. Trusselbildet til næringslivet begrenser seg naturligvis ikke kun til disse seks punktene og akrim, men andre mer bransjespesifikke trusler kunne vært naturlig å ta med. Fraværet av andre trusseltyper betyr ikke at vi vurderer de som ubetydelige, men ønsket om en mindre omfattende og mer spisset rapport har veid tyngre i dette henseende.

[21] BDO (2017)
[22] DSB (2018)
[23] NSM (2017)
[24] BDO (2017)

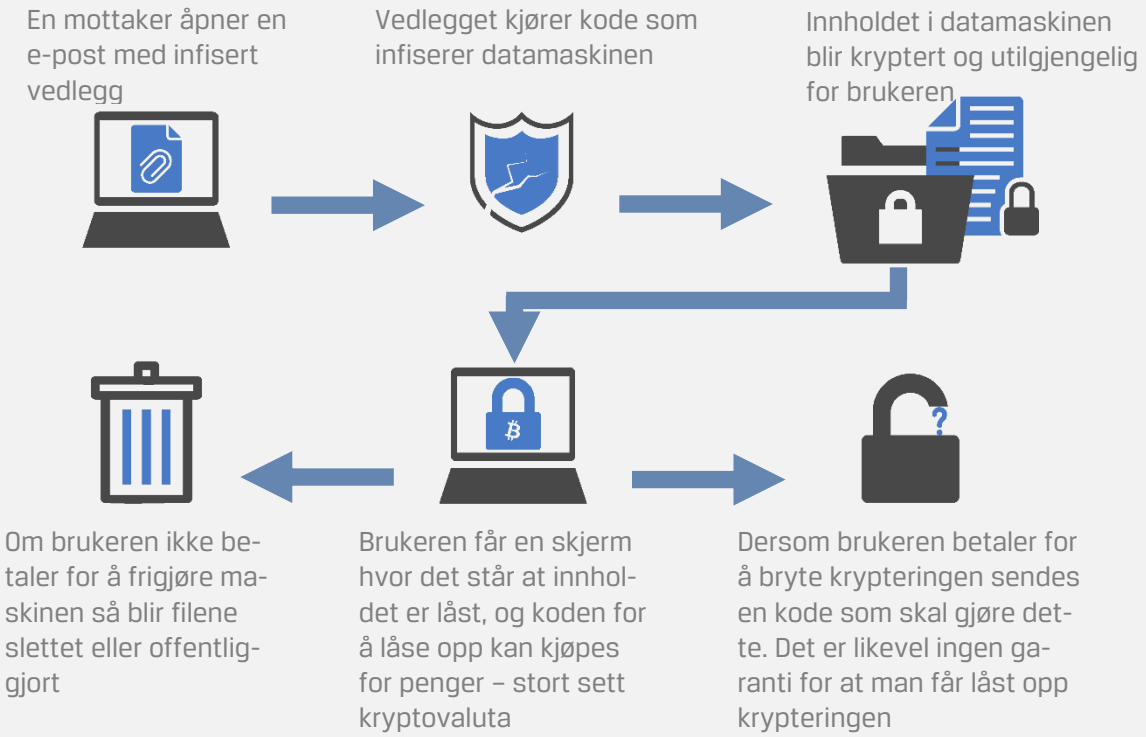
Direktørsvindel

Direktørsvindel – eller CxO-bedrageri[25] – er en bedragerityp som har blitt aktuell de siste årene, og kan ha et veldig stort skadepotensiale. I 2016 rapporterte norske bedrifter et tap på 294 millioner kroner knyttet til direktørsvindel, og gjennomsnitt rapportert tap per sak lå på 1,37 millioner kroner.[26] Til tross for at det allerede er innrapportert store tap anser man at mørketallene her er store.[27] Det groveste eksemplet på denne svindeltypen i Norge var da en bedrift i Oslo ble svindlet for over 500 millioner kroner[28]. Gjennomføring av direktørsvindel krever ofte sosial manipulering av de ansatte som utbetaler summer de ikke burde gjøre. En vanlig modus er å enten forfalske hvilket telefonnummer man ringer eller sender tekstmelding fra[29] eller e-postkonto en sender fra, sånn at det fremstår som at det er en direktør eller lignende i virksomheten som tar kontakt og krever en hurtig og konfidensiell overføring til en gitt konto.

Hovedpoenget med direktørsvindel er å utgi seg for å være en annen for å få penger overført til egen konto. Man har også lignende modi hvor svindlere utgir seg for å være en av virksomhetens leverandører som ønsker å oppgi ny kontoinformasjon, eller svindlere som utgir seg for å være IT-ansatt i virksomheten som varsler om et sikkerhetsbrudd og derfor ber om finansielle detaljer for å kunne sjekke om virksomheten har blitt kompromittert.

På grunn av bedragerityens natur er det mye arbeid for de kriminelle i forkant av et forsøk. Skal de lykkes må de gjennomføre undersøkelser og overvåkning av virksomheten, i tillegg til å skaffe organisasjonskart og en liste over hvilke ansatte det er naturlig å rette angrepet mot.[30] Ofte vil de kriminelle ha hacket organisasjonen i forkant for å få den ovennevnte informasjonen, i tillegg til et innblikk i hvordan direktørene kommuniserer med sine ansatte, samt hvilke samarbeidspartnere virksomheten har.

[25] Bedragerityen omtales også som den litt mer snevrere "CEO-bedragerier".
[26] Finanstilsynet (2017)
[27] E24 (2017)
[28] Norsis (2017a)
[29] Også kjent som «spoofing»
[30] Europol (2016)



Løsepengevirus

Løsepengevirus fremstod i 2017 som den sterkest voksende digitale trusselen, og det ble registrert angrep på en skala man ikke har sett tidligere.[31]

Løsepengevirus fungerer ved at skadevare blir spredd til ulike dataenheter – som oftest via e-post – hvor den installerer seg selv og krypterer innholdet. Krypteringene er gjerne så sterke at de ikke lar seg bryte, og hvis den infiserte personen eller virksomheten ikke har sikkerhetskopier må man skrive inn en nøkkel for å få tilgang på innholdet. Denne nøkkelen får man kun tilgang til om man betaler en gitt sum til gjerningspersonene.

Det er flere grunner til at løsepengevirus er så attraktivt blant kriminelle. Terskelen for å gjennomføre et angrep er lav fordi det krever forholdsvis lite kompetanse å gjennomføre et angrep ettersom man lett kan få tilgang på ferdigprodusert programvare som gjør det meste av jobben, mens organiserte kriminelle produserer egne – og ofte mer sofistikerte – virus.

De senere årene har antallet tilgjengelige løsepengevirusfamilier[32] eksplodert, og fra 2015 til 2016 økte kjente familier fra 29 til 247.[33] Løsepengevirus er også attraktivt fordi man lett kan kapitalisere kriminaliteten ved at pengene kommer direkte til de kriminelle. På grunn av betalingsformen (som oftest Bitcoin) er det det lettere å hvitvaske enn om illegalt ervervet fysiske penger. I motsetning til flere av de andre IKT-truslene så har løsepengevirus et stort nedslagsfelt, og stort sett alle privatpersoner og virksomheter med data de ønsker å ta vare på er potensielle ofre.

Det verste registrerte løsepengeviruset til nå er WannaCry[34], som i 2017 klarte å infisere over 300 000 ofre i over 150 land[35], og står som ett av de verste virusene i historien. Det som gjorde WannaCry så effektivt var at det spredde seg til andre enheter via lokalnettverk eller internett før det låste enheten det først infiserte.[36] Med andre ord krevde det mye mindre arbeid for bakmennene å gi viruset det omfanget som det fikk enn om det kun skulle spredd seg via e-post

[31] Europol (2017)

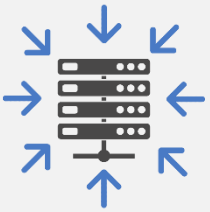
[32] «Familier» i denne sammenheng kan forenklet forstås som varianter.
[33] Trendlabs (2016)
[34] Viruset er antatt å ha blitt produsert av en statlig støttet nordkoreansk gruppe
[35] Europol (2017)
[36] Symantec (2017)

Tjenestenektangrep

En trojaner spres til enheter som er tilkoblet internett – alt fra vannkokere til datamaskiner

Sammen utgjør alle de infiserte enhetene et botnet, og kan bestå av flere millioner enheter

De som lagde botnettet leier ut bruken til andre for ganske små summer. Eventuelle kjøpere av tjenesten kan velge ut et mål de ønsker å angripe



De infiserte enhetene sender så mye trafikk til en gitt server at den blir overbelastet, noe som resulterer i ingen får tilgang til den

Dataskadeverk/sabotasje

Ikke alle dataangrep er direkte økonomisk motivert, og angrep som dataskadeverk og sabotasje vil ofte være motivert av andre grunner; Noen ønsker å angripe en virksomhet eller organisasjon på bakgrunn av politiske, ideologiske, eller religiøse idéer; noen har som mål å ødelegge for en konkurrent eller rival; noen gjør det for å vise frem sin kompetanse, mens andre gjør det kun fordi de ønsker å vandalisere. I enkelte tilfeller brukes tjenestenektangrep som et ledd i en større operasjon, hvor tjenestenektangrepet er et skalkeskjul som skal forlede IT-personell til å ha fokus på et annet sted enn der hvor angrepet foregår.

Tjenestenektangrep er en av de mest brukte angrepsformene som blir brukt av IKT-kriminelle, og kan brukes til flere formål.[37] Et tjenestenektangrep vil kunne knele en virksomhets datasystemer og gjøre data utilgjengelig. Det krever ikke nødvendigvis mye kompetanse for å gjennomføre det, og for enkle angrep trenger man ikke gjøre annet enn å betale en ganske liten sum til noen som tilbyr tjenesten, samt et mål som man ønsker å angripe. Et eksempel på hvor enkelt det er ble vist i en sak i Sør-Øst hvor en elleveåring betalte under 200 kroner for å utføre et angrep på en kompis mens de spilte spill, med den følgen at mange andre virksomheter og tjenester også ble angrepet og mistet tilgang. Store og ressurssterke organiserte kriminelle har andre verktøy og metoder enn de som kan kjøpes, og kan derfor gjennomføre større og mer sofistikerte angrep.

I forbindelse med det stadig voksende tingenes internett og manglende sikkerhet knyttet til disse komponentene så ser man at det kommer til å bli en økning i antall botnet[38] og dermed flere tjenestenektangrep i tiden som kommer[39].

[37] Europol (2016)

[38] Et botnet er en samling enheter som alle er infisert med samme virus/trojaner, og som kan brukes til å stjele informasjon, gjennomføre tjenestenektangrep, eller sende søppelpost

[39] Europol (2017); NSM (2018)

Informasjonstyvene bruker mye ressurser på å velge hvilket mål de skal gå etter, basert på sikkerhet og hva de kan få ut av informasjonen i etterkant

Ved bruk av innsidere, phishing, målrettet hacking, vannhull, eller andre metoder får tyvene en trojaner installert hos virksomheten

De kriminelle får informasjon ved at trojaneren selv samler inn informasjon og sender, eller at de manuelt kommer seg inn på nettverket og leter

Dersom informasjonen ikke er noe tyvene selv har behov for må de finne en eller flere interesserte kjø-

Spionasje/informasjonstyveri

Utenlandske statlige aktører gjennomfører jevnlig digitale spionasjeoperasjoner mot norske offentlige og private virksomheter.[40] Til tross for at aktiviteten fra de statlige aktørene først og fremst retter seg mot politiske og militære mål, ser man i tillegg at akademiske institusjoner, kraftselskaper og industribedrifter blir utsatt.[41] Trusselen gjelder særlig for teknologivirksomheter som utvikler og leverer varer som kan brukes militært.[42] Samtidig er det også mange ikke-statlige aktører som stjeler informasjon, men deres motiv er ofte finansielt.

Selv om informasjonstyveri kan være aktuelt hos flere typer virksomheter og privatpersoner er det finansinstitusjoner som er de mest utsatte virksomhetene.[43] Det er begrenset hvilke virksomheter som angripes, og dersom kriminelle angriper en spesifikk bank, må angrepet skreddersys til det målet, og kan ikke uten videre gjenbrukes hos andre virksomheter. Informasjonstyveri trenger dog ikke være direkte rettet mot inntjening. I tillegg til spionasje/industrispionasje og sabotasje, kan det også brukes som ledd i utpressing og svindel av privatpersoner.[44] Informasjonstyveri og påfølgende utpressing av strategisk viktige personer kan medføre en trussel mot virksomheter.

Der hvor løsepengevirus søker størst mulig nedslagsfelt og dermed får lavere andel som betaler og gjennomsnittssummen er relativt lav, treffer informasjonstyver få mål, men med høy utbetaling per mål de klarer å ta. Angrepsmetodene kan være som med løsepengevirus, men i hovedsak går angrepene mot utvalgte personer eller bedrifter via phishing[45] på e-post eller SMS.[46]

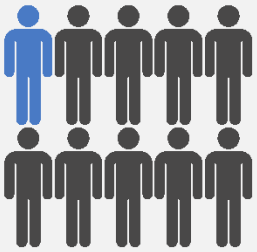
Informasjonstyveri har ikke like stort omfang som løsepengevirus blant annet fordi det krever mye mer arbeid og kompetanse. Samtidig krever informasjonstyveri mer arbeid i ettertid for å kapitalisere, ettersom de kriminelle må finne personer som er interessert i å kjøpe den stjålne informasjonen. For tyveri av kredittkortinformasjon og lignende krever det at man bruker tredjepersoner som bidrar til å hvitvaske gevinsten.[47]

[40] NSM (2017b)
[41] Etterretningstjenesten (2018)
[42] PST (2018)
[43] Europol (2017)
[44] Norsis (2017b)
[45] Fisking etter innloggingsinformasjon eller lignende
[46] Norsis (2017b)
[47] Europol (2017)

Innsidere

Den rekrutterte innsideren, som jobber frivillig eller under press for en tredjepart. Rekrutteringen skjer ofte etter at personen har fått tilgang til virksomhetens verdier. Dette er typisk den ansatte, som blir presset til å handle, gjerne fra kriminelle grupperinger eller fra fremmed stat.

Den selvmotiverte, ondsinnede innsideren, som gjennomfører den tilsiktede uønskede handlingen på eget initiativ - og i utgangspunktet ikke har kontakt med eller styres av en tredjepart. Dette er typisk betrodde ansatte som har motiv, utnytter mulighetene og rasjonaliserer sin adferd.



Infiltratøren er plassert i virksomheten av en tredjepart som ønsker å utnytte tilgangen han gis, på en måte som skader virksomheten. Vi kjenner dette igjen fra de klassiske "spionfilmene".

Den uforvarende innsideren som uten å forstå det, gjennomfører en handling som resulterer i økt sårbarhet, skade eller tap for virksomheten. Vedkommende kan ha blitt manipulert eller forledet eller har ikke kompetanse til å forstå konsekvensene av handlingen sin. Dette er typisk ansatte som ikke har god nok kompetanse. De store endringene i digitalisering utfordrer både vårt virkelighetsbilde og vår kompetanse.

Innsidere

En av ti virksomheter forteller at de har avdekket utro tjenere blant egne ansatte i løpet av de siste to årene. Avdekkingen er noe høyere i det offentlige enn det private, men det er ikke store forskjeller mellom ulike bransjer.[48] Mens de fleste virksomheter investerer beløp for å sikre seg mot eksterne trusler, blir de interne truslene glemt.[49]

Når det er så mange virksomheter som rapporterer om utro tjenere, burde dette ført til at en har gode rutiner på plass for å luke ut eventuelle problemer allerede ved ansettelsesprosessen. Det ser dog ut som at den interne trusselen ofte overses blant virksomheter, og en ser at mange enkle tiltak ved ansettelser ikke gjennomføres. Offentlige virksomheter har bedre rutiner på dette, men også her er det mye å hente.[50]

Det er dog ikke alltid en rekrutteringsprosess vil avdekke eventuelle innsidere. Utro tjenere kan deles i ulike grupper, hvor kun førstnevnte gruppe vil være mulig å oppdage i en rekrutteringsprosess: de som søker jobb i en virksomhet med det formål å bli innsider; de som i utgangspunktet ikke hadde planlagt det da de ble ansatt, men som velger å bli det; de som blir rekruttert eller utnyttet/utpresset;[51] og de som uforvarende er innsider uten å være klar over det selv.[52]

Det har vært flere tilfeller av innsidere og korrupsjon i media de senere år i forbindelse med økt fokus på arbeidsmarkedskriminalitet, senest med en dom i mars 2018 på grov korrupsjon i Drammen kommune.[53] Innsidertrusselen er ikke bare et konkurransevridende problem, men kan også være skadelig for demokratiet og befolkningens tillit til rettsstaten og myndighetene.

Samarbeidspartnere utgjør også en slags innsidertrussel, og også her ser man at norske virksomheter gjør en svak jobb med bakgrunnssjekk av samarbeidspartnere. 37 prosent sier at de alltid gjennomfører bakgrunnssjekk ved inngåelse av samarbeid i Norge, mens det kun er 24 prosent som gjør dette når de inngår internasjonale samarbeid. For land med høy risiko er andelen høyere – 62 prosent.[54] Men også dette må sies å være lavt.

[48] NSR (2017)
[49] Liljedahl (2017)
[50] NSR (2017)
[51] Benjaminsen (2017)
[52] NSM (2017b)
[53] NRK (2018)
[54] NSR (2017)

7,5% av ansatte utsatt for vold eller trusler – tilsvarende 200 000 personer (STAMI 2015)

2,6 prosent utsatt for vold som ga synlige merker (STAMI 2015)

11 prosent av kvinnelige ansatte utsatt for vold eller trusler (SSB 2013)

5 prosent av mannlige ansatte utsatt for vold eller trusler (SSB 2013)

Vold og trusler mot ansatte

Over 200 000 personer – tilsvarende 7,5 prosent av ansatte i norske virksomheter ble utsatt for vold og trusler på jobb i 2014. De mest utsatte yrkene er i offentlige virksomheter, og den verste er vernepleier/sosialarbeidere hvor flere enn 40 prosent ble utsatt for vold eller trusler det siste året. Politi og vaktvirksomhet er den nest mest utsatte yrkesgruppen med litt under 35 prosent. De private virksomhetene som skiller seg mest ut er servitører, sjåfører, og kundeserviceyrker – alle yrker hvor mer enn fem prosent av de ansatte utsettes for vold eller trusler. Selv om det er flest personer som blir utsatt for trusler, er det også en del som blir utsatt for vold som ga synlige merker (2,6 prosent) eller vold som ikke ga synlige merker (4 prosent). [55]

Hvis alle som ble utsatt for vold som ga synlige merker hadde anmeldt disse til politiet ville det ha tilsvart 63 000 anmeldelser nasjonalt, og 6 900 anmeldelser i Sør-Øst. Til sammenligning ble det anmeldt henholdsvis og 32 540 og 3 926 saker innen voldskapittelet.[56]

Det har vært en moderat økning i andelen personer som har blitt utsatt for vold i arbeidslivet. I tillegg til økning i vold mot polititjenestepersoner[57] så uttaler vektere det samme, og deres statistikker viser en økning i antall utløste alarmer til voldsepisoder som vektere blir utsatt for, og volden de blir utsatt for blir stadig styggere. Denne trenden gjelder ikke bare til spesielle bydeler i Oslo, men er noe man ser igjen i hele landet. Samtidig er det mange episoder som ikke blir anmeldt, og det er en gjengs oppfatning blant mange vektere at en må tåle å få seg et lite trøkk i jobbutførelsen.

Utviklingen med mer vold i arbeidslivet er ikke bare relevant for ansatte innenfor de utsatte virksomhetene, men kan i verste fall være et symptom på et større problem. Dersom terskelen for å begå voldelige handlinger i landet synker så øker risikoen for grove ran. Videre kan det øke omfanget av vold, trusler og sjikane mot politikere, journalister, redaktører, og andre meningsytrere i det frie rom og som igjen kan medføre press på ytringsfriheten og demokratiet.

[55] STAMI (2015)

[56] Voldskapittelet inkluderer også trusler, og er derfor en bredere definisjon enn vold med synlige merker. Mørketallene vil dermed være enda større enn det som kommer frem av disse tallene

[57] Dignes (2016)

«Nettet - Trygg havn for kriminelle»

I tillegg til å være en aktuell trussel for næringslivet, er IKT-kriminalitet minst like aktuelt for politiet. Omfanget er utvilsomt en god del av årsaken til dette, men også på grunn av den lave risikoen og de lave inngangskostnadene de kriminelle har ved å begå kriminalitet ved bruk av informasjons- og kommunikasjonsteknologi.

IKT-kriminalitet skiller seg fra tradisjonell kriminalitet ved at investeringskostnadene er mye lavere for førstnevnte. Ved tradisjonell kriminalitet er man begrenset av den romlige dimensjonen, det vil si at ens muligheter blir begrenset av fysisk nærhet til objektet en skal begå kriminalitet mot, mens IKT-kriminalitet begås på tvers av landegrenser. Tidsdimensjonen er også en faktor som gjør nettkriminalitet ekstra attraktivt, ettersom det ofte krever veldig lite tidsbruk, og ofte kan en kriminell tjene penger lenge etter at man utførte selve lovbruddet. For de som kjøper ferdigutviklede IKT-kriminalitetsprodukt krever det også lite investering i egen kunnskap og kompetanse.

I tillegg til interne faktorer hos de enkelte gjerningspersonene er det også en del eksterne faktorer som fasiliterer og forenkler IKT-kriminalitet, og som gjør at det skiller seg fra tradisjonell kriminalitet.

Risikominimering

Bruk av elektroniske verktøy på nett etterlater seg ofte spor om hvor brukeren befinner seg, hvilken maskinvare som brukes, og hva slags aktivitet som bedrives. Siden disse sporene kan føre til at brukeren kan identifiseres er det mange som tar i bruk programvare eller verktøy som bidrar til å skjule sporene.

Skjuling av elektroniske spor

En ser at mye av den kriminelle aktiviteten foregår på det mørke nettet, hvor tor-nettverket er det mest utbredte. Forenklet kan en si at det mørke nettet er et eget slags world wide web hvor man via det vanlige internettet bruker dedikert programvare for å komme inn. På grunn av måten det mørke nettet er bygd opp, hvor informasjonen mellom bruker og sluttserver krypteres og går gjennom mange forskjellige ledd, så er det mye vanskeligere å identifisere brukeren Selv om det mørke nettet ikke er helt anonymt, vanskeliggjør det identifisering av brukere, og i kombinasjon med andre metoder for å skjule seg[58] krever det store ressurser for å avdekke identiteten til brukerne.

[58] Som for eksempel bruk av VPN og virtuell maskin

Kryptovaluta

Kryptovaluta er en virtuell valuta som i motsetning til nasjonsstaters egne valutaer ikke er garantert eller utstedt av en offentlig aktør, og er som sådan fullstendig markedsstyrt. Det finnes et veldig stort antall kryptovaluta hvor den mest kjente er Bitcoin. Selv om det er få virksomheter i næringslivet som godtar betaling med Bitcoin, er det relativt lett å konvertere denne valutaen til for eksempel norske kroner eller andre lands valuta. I motsetning til banktjenester som vi har vært vant til historisk sett, er det mye enklere å kjøpe og selge tjenester anonymt med kryptovaluta. Når det tilbys debetkort som man kan fylle opp med kryptovaluta er det fullt mulig å leve på midler som kommer fra kriminell aktivitet uten å måtte hvitvaske penger. Anonymiteten og mange bruksområder har ført til at kryptovalutaer har blitt et populært blant kriminelle.[59]

Tingenes internett

En stadig større andel av hjelpemidlene vi bruker i hverdagen er koblet til internett, og utgjør det vi kaller «tingenes internett». Det har mange fordeler med seg å kunne ha mange av hjelpemidlene knyttet til internett, men det skaper også utfordringer. De enhetene som er koblet på nettverket kan misbrukes til avlytting, spredning av skadevare, bakdør inn til virksomhetens data samt flere andre mulige utnyttelser av virksomhetens digitale svakheter.[60] Disse enhetene har ofte mangelfull sikkerhet og man har allerede sett at disse blir brukt som et ledd i informasjonstyveri, og en antar at de i fremtiden vil fortsette å føre til at sensitive data kommer på avveie, og store innbrudd forventes å bli en vanlig forekomst. Enheter som er koblet til internett brukes ikke bare som et verktøy for å bedrive informasjonstyveri, men det har vært utstrakt bruk av disse som ledd i tjenestenektangrep, og denne trenden forventer man å se også i fremtiden.[61]

Mange virksomheter er nok ikke klar over hvor eksponert de blir for digitale trusler gjennom vanlige gjenstander som er koblet til nettet. Tankegangen blant mange når det kommer til IKT-sikkerhet er å sikre de enhetene som inneholder sensitiv informasjon, men glemmer alle andre enheter som kan være en inngang. Mange av tingene som er koblet opp mot nettet har dårlig sikkerhet fordi produsentene i utgangspunktet ikke er IT-selskap, og derfor ikke klarer å se for seg hvilke sikkerhetsutfordringer de utgjør. Samtidig har ikke produsentene incentiver til å gjøre noe med det

[59] Se for øvrig NTAES (2017b) for mer informasjon om hvordan kryptovaluta fungerer.

[60] Norsis (2017b)

[61] Europol (2017)

fordi mange av deres kunder ikke er klar over at de har blitt kompromittert.

Sosial manipulering

I tillegg til dårlig sikring av enheter som ikke inneholder viktig informasjon om virksomheten, kan en også si at virksomheter ikke er gode nok til å sikre egne ansatte mot «angrep» som for eksempel sosial manipulering. Sosial manipulering er på ingen måte noe som har kommet med internett, men i motsetning til tidligere hvor man var avhengig av direkte kontakt med personene man skal manipulere, er det i dag mulig å gjøre det med mindre arbeid og på mye større skala. Der hvor hacking er utnyttelse av svakheter i datasystemer, er sosial manipulering utnyttelse av svakhet i mennesker. På grunn av nedgang i markedet for utnyttelsesverktøy[62] for å spre skadevare, så har utviklere måttet bruke andre metoder for å infisere datamaskiner, som for eksempel spam botnet og sosial manipulering.[63] Nedgangen i bruken av utnyttelsesverktøy skjer ikke nødvendigvis bare fordi de ikke er like effektive som før, men også fordi de mest avanserte aktørene, i motsetning til hva en skulle tro, ikke ønsker å bruke denne type teknisk kompetanse eller verktøy for å komme seg inn i virksomheters nettverk. Avanserte aktører ønsker heller å skaffe seg virkelige tilganger gjennom sosial manipulasjon, fordi de på denne måten har anledning til å være lengre inne på virksomhetenes nettverk uten å bli oppdaget.[64]

Sosial manipulering er en ofte brukt metode i den digitale kriminaliteten ved at ansatte i virksomheter overtales, misledes, eller trues til å gjøre ting de normalt sett ikke ville gjort. Det blir ofte spilt på frykt, fristelser, eller tillit for å påvirke den ansatte, og ved bruk av den ansatte omgår de teknisk beskyttelse.[65] Siden sosial manipulering er utnyttelse av menneskelige svakheter betyr det at forebygging må foregå ved opplysning og opplæring av de ansatte. Dessverre er det store mangler på opplæring av ansatte. Når en vet at ansattes uforsiktige eller uvitende handlinger medfører en stor risiko for virksomheter er det lite tvil om at opplæring bør være en prioritet. Kun 21 prosent av befolkningen sier at de har mottatt opplæring om effektive sikringstiltak innen digital sikkerhet de siste to årene. Mange personer har for dårlige ferdigheter og gjør ikke grunnleggende ting som gir effektiv beskyttelse. [66]

[62] Exploitation kits
[63] Europol (2017)
[64] Telenor (2017)
[65] Norsis (2017b)
[66] Norsis (2017c)

DEL 3:
RISIKOSTYRING

Risikostyringen i virksomheten

Kriminalitet er en av mange interne og eksterne trusler for virksomheten. Vi anbefaler at virksomheten vurderer risiko på en helhetlig måte. Det å ta risiko er en naturlig del av å drive enhver virksomhet, og krever kunnskap om risikoene. I denne rapporten har vi valgt å ikke gå nærmere inne på de ulike standardene og rammeverkene for risikostyring,[67] men valgt å vektlegge det vi mener er viktig for å forebygge kriminalitet.

Risikostyring defineres gjerne som systematiske, koordinerte og proaktive aktiviteter som er rettet mot vurdering og håndtering av usikkerhet og hendelser/handlinger som kan påvirke måloppnåelsen.

Det omfatter blant annet virksomhetens evne til å:

- Påvirke sårbarhet/sannsynligheten og den positive eller negative konsekvensen av hendelser
- Følge med på risikobildet over tid.
- Initiere tiltak som endrer utviklingen i ønsket retning.
- Bygge opp en organisasjonskultur som sikrer implementering av tiltak og bidrar til god risikostyring
- Forstå og utnytte korrelasjoner mellom ulike typer risiko.

Målet med helhetlig risikostyring er å holde risiko på et ønsket nivå samt sikre best mulig balanse mellom trusler og muligheter. Dette krever at et helhetlig perspektiv på tvers av organisasjonsenheter, funksjoner og risikokategorier[68] legges til grunn, blant annet for å unngå silotenking og suboptimalisering.

Styret skal påse at virksomheten har etablert en forsvarlig risikostyring og har et generelt forvaltningsansvar for virksomheten[69] og bør stille tydelige krav til risikostyringen[70], mens administrerende direktør (daglig leder) har overordnet operativt ansvar for risikostyringen[71], noe som innebærer å "sette tonen fra toppen" gjennom å demonstrere viktigheten av god risikostyring, herunder at kriminalitet er tema på ledermøter. Virksomheter etablerer gjerne en risikostyringsfunksjon[72] som kan være en del av oppgavene til daglig leder, en ansatt eller en enhet i virksomheten. Funksjonen bør blant annet identifisere, vurdere og håndtere risiko, samt overvåker risikobildet og flagger trender i risikobildet. Funksjonen bør blant annet ha ansvaret for å følge opp fremdriften i det samlede risikostyringsarbeidet, bistå linjeledelsen i å kommunisere risikoinformasjon i hele virksomheten, overvåke at risikostyringsprosesser etterleves og reagere dersom det avdekkes forhold som ikke er tilstrekkelig håndtert.

Krav til risikovurdering av securityhendelser

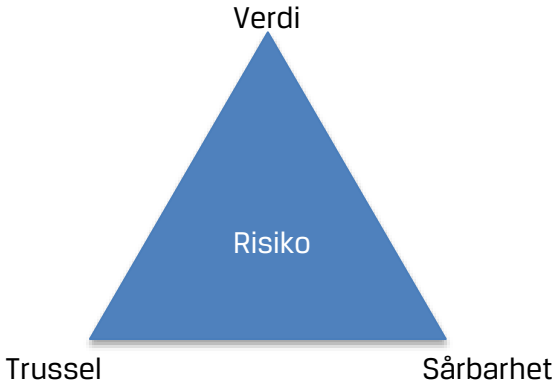
Endringer i internkontrollforskriften innebærer at HMS-arbeidet i virksomheter skal være både safety- og security-rettet ved at de har et generelt krav om å forebygge «uønskede tilsiktede hendelser».[73] Terrorisme, dataangrep, underslag, vold mot ansatte, vandalisme og grove tyverier er eksempler på slike uønskede tilsiktede hendelser. Virksomhetens forbedringsarbeid gjennom systematiske tiltak inkluderer å forebygge slike uønskede tilsiktede hendelser, eller handlinger. Endringen innebærer blant annet å vurdere risiko ved hjelp av sikringsrisikoanalyse og utarbeide planer og tiltak for å redusere kriminalitetsrisikoen.[74]

Risikoanalyse for sikring

Vurdering eller analyse av risiko kan gjennomføres på en rekke ulike måter. Trusselvurderingen i denne rapporten forsøker vi å tilpasse til NS5832,

[67] COSO ERM, ISO 31000, m.fl.
[68] Strategiske, finansielle, operasjonelle risikoer, eksterne vs. interne risikoer, mv.
[69] Aksjeloven § 6-13
[70] Kjørstad (2016)
[71] Aksjeloven § 6-14
[72] Veileder for Risikostyringsfunksjonen, IIA Norge
[73] Internkontrollforskriften § 1
[74] Internkontrollforskriften § 5

«Krav til sikringsrisikoanalyse», hvor politiets rolle primært er å presentere et trusselbilde. Vi tar ikke stilling i diskusjonen om hvordan man skal gjøre risikovurderinger, og spesielt hvordan man estimerer sannsynlighet.[75, 76] Vi mener imidlertid at denne analysemetoden kan benyttes på en grovvurdering av de fleste typer uønskede tilsiktede hendelser/handlinger.



NS5832 baserer seg på at virksomheten vurderer tre faktorer; verdi, trussel og sårbarhet og samspillet mellom disse. Dette innebærer at virksomheten kartlegger de verdier den eier, forventer å eie eller forvalter for andre eiere. Videre gjennomfører virksomheten en trusselvurdering og beskriver scenarioer for hvordan trusselaktører kan påvirke de valgte verdiene negativt. Politiets trusselvurderinger er et av flere innspill til denne. Virksomheten gjør deretter en vurdering av i hvilken grad verdiene er sårbare sett opp mot scenarioene. Til slutt sammenstilles informasjonen i en egen, selvstendig vurdering av risiko for hvert scenario.

Dette innebærer i korte trekk å besvare følgende spørsmål:
1) Hvilke kritiske verdier har virksomheten?
2) Hvilke trusler kan ramme disse verdiene?
3) På hvilken måte er verdiene sårbare overfor truslene?

[75] Busmundrud et. al (2015)
[76] Barane (2014)

Den tradisjonelle vurderingen av risiko[77] er som oftest som en kombinasjon av sannsynligheten for at noe kommer til å skje, basert på trusler og sårbarheter, og konsekvensen av en hendelse. Risikoen kan angis i en matrise. Analyse basert på NS5832 vil gi innspill til både angivelse av sannsynlighet og konsekvens i en slik matrise.

Risikoanalysen[78]

Risikoanalysen må sees i sammenheng risikostyringsprosessen i virksomheten. Vi anbefaler at analysen starter med en planlegging og organisering av arbeidet, og i forkant bør en vurdere følgende punkter:

- Avklare omfang og mål for analysen
- Forankring hos beslutningstaker – typisk ledelse
- Informere andre interessenter
- Vurdere behov for beslutninger underveis
- Avklare hvordan analyseresultatene skal dokumenteres og hvorvidt det er behov for å skjerme noe av informasjonen
- Planlegge de ulike stegene i analysen

Sett gjerne høyeste og laveste i skalaen som brukes i analysen, og fyll deretter på midten. Hver enkelt virksomhet er unik.

Nedenfor er en figur som viser stegene i sikringsrisikoanalysen.[79]

Verdivurdering

Formålet med verdivurderingen er å identifisere, vurdere og rangere de viktigste verdiene i virksomheten. Virksomhetens skal vurdere egne verdier – både nåværende og mulige fremtidige – samt verdier virksomheten forvalter for andre. Verdier kan måles i f.eks. liv og helse, miljø, øko-

[77] ROS-analyse, ISO31000:2018, ISO27001, COSO Fraud Risk Assessment, Difi-modellen, etc.
[78] Norsk Standard 5832
[79] Roy Stranden - foredrag presentert på Nasjonal sikkerhetsmyndighets sikkerhetskonferanse 19. mars 2013.

nomi, omdømme eller handlingsfrihet. Som en del av prosessen fastsettes sikringsmål, dvs. ønsket og akseptabel tilstand for verdien.

Virksomheten beskriver på en hensiktsmessig måte slik at den kan identifisere hva som er verdifullt for virksomheten. Det kan være nyttig å beskrive virksomheten som f.eks. et prosesskart (IDEF0-diagram)[80] eller som en verdikjede[81], slik at man får oversikt over hva virksomheten egentlig driver på med. Deretter identifiseres ressurser som har verdi for de kriminelle (eller andre potensielle angripere) som f.eks. data/informasjon, kunnskap hos nøkkelmedarbeidere, kunderegister, varelager, patenter eller gjenstander med høy økonomisk verdi. Det kan være lurt å skaffe seg oversikt over de ti mest kritiske verdiene i virksomheten og prioritere disse først, noe som bidrar til oversikt og forenkling av prosessen. Det anbefales heller å gå i detalj ved senere gjennomganger. [82] Det er viktig å forankre sikringsmålene og rangering av verdier hos eier eller forvalter av verdiene.

Trusselvurdering

Trusselvurderingen beskriver det gjeldende trusselbildet for de verdier som ønskes beskyttet, samt en vurdering av hvordan trusselbildet kan utvikle seg.

Det er viktig å forsøke å identifisere og beskrive eventuelle trusselaktører, deres intensjon (vilje) og kapasitet (evne) og andre relevant faktorer. Intensjon kan sies å være vilje eller et ønske om å ramme de kritiske verdiene som ble prioritert i verdivurderingen. Kapasitet dreier seg om evne til å utføre de tilsiktede handlinger.

Deretter utarbeider man scenarioer basert på vurdering av verdier og trusselaktører. For å få frem scenarioene identifiseres og vurderes hvordan de ulike trusselaktørene som er identifisert og vektet vil gå frem for å negativt påvirke verdiene (modus operandi). Det er viktig å være detaljert på hvordan dette kan skje. Om dette ikke er eksplisitt så vil det være svært vanskelig å vurdere sårbarheten på en god måte. Scenarioene som velges ut til å være med i den videre prosessen er også de som til slutt vurderes i risikovurderingen.

[80] Stranden (2017)
[81] Porter (1985)
[82] Bergsjø & Windvik (2018)

Sårbarhetsvurdering

For hvert scenario gjøres en sårbarhetsvurdering. Sårbarhetsvurderingen avdekker i hvilken grad de valgte verdiene er sårbare i scenarioene, og dermed medføre en konsekvens for virksomheten. Ut i fra dette vurderes det i hvilken grad det eksisterer tiltak som forhindrer uønsket handling. Man får da frem eventuelle gap mellom innførte forebyggende tiltak og en trusselaktørs intensjon og kapasitet.

Risikovurdering

I risikovurderingen sammenstiller man verdi, trussel og sårbarhet til en vurdering av risiko. Hensikten er å få frem en beskrivelse av og en bedømmelse av risikonivået for hver enkelt risiko. Ved hjelp av scenarier og sårbarheter beskriver man hver enkelt risiko. Man bestemmer risikonivået basert på klassifisering av verdi, trussel og sårbarhet for hver enkelt risiko. Risikonivået velges og begrunnes, samt usikkerhet i vurderingen tas med.

Vurdering og valg av strategi og tiltak

Vurdering og valg av strategi vurderes for hver enkelt risiko. Det er ulike strategier for styre risiko; å unngå, å overføre, å akseptere, og/eller å fjerne/redusere risiko. Hver enkelt strategi har gjerne flere tiltak, som følges opp over tid og sees i sammenheng med andre tiltak. Etter at ulike strategier og tiltak er vurdert og konsekvensen ved disse løsningen er kartlagt, skal sikringsmålene revurderes. Beslutningstaker skal avgjøre hva som er akseptabelt risikonivå. Valg av tiltak besluttes.

Nyttige kilder for forebygging

De vanligste tiltakene for å forebygge og som virksomheter mener reduserer kriminalitetsrisikoen er blant annet[83]:

- Presisering av styrets påse- og forvaltningsansvar og administrerende direktørs (daglig leder) overordnede operative ansvar for risikostyringen
- Klargjøring av roller, ansvar og oppgaver for risikostyringsfunksjoner, compliancefunksjoner og andre nøkkelfunksjoner i virksomheten.
- Etablere etiske regler og "sette tonen fra toppen"
- Etablere et rammeverk og standard for utøvelse av risikostyring og internkontroll, og risikoanalyser/-vurderinger
- Prinsipper og rutiner for å forebygge, avdekke og styre risikoen,
- Transparens og varslingskanal
- Opplæring av ledere og medarbeidere
- Intern og ekstern kommunikasjon
- Kunnskapsdeling og læring ved hendelser
- Oppfølging av kontraktsmotparter og leverandører
- Styrets og linjeledelsens oppfølging
- Bekreftelser fra intern- og/eller eksternrevisor

Oversikten er ikke uttømmende. I det videre har vi nevnt noen nyttige kilder relatert til risikoanalyse og forebygging av de truslene vi har omtalt i vurderingen.

Nasjonal sikkerhetsmyndighet (NSM) har utarbeidet håndboken «Risikovurdering for sikring» som gir virksomheter mer detaljert beskrivelse om hvordan slike risikovurderinger kan planlegges og gjennomføres.[84] På deres hjemmeside er det også veiledninger og råd.[85]

Det er også kommet en ny bok hvor det beskrives hvordan en risikovurdering/-analyse i samsvar med NS5832 kan gjennomføres innenfor datasikkerhet, og hvor verdier er knyttet til data og datasystemer.[86] Forfatterne driver også nettstedet instituttforcybersikkerhet.no som har en visjon om å samle relevant informasjon om cybersikkerhet.

[83] Report to the Nations, Global study on occupational fraud and abuse, ACFE http://www.acfe.com/report-to-the-nations/2018/

[84] NSM (2016b),

[85] https://nsm.stat.no

[86] Bergsjø og Windvik (2018)

Det er også utgitt en veileder mot økonomisk kriminalitet i energibransjen[87] og som følger i all hovedsak prinsippene i COSO-rammeverket[88] og anbefalingene fra organisasjonen Association of Certified Fraud Examiner.[89] De samme prinsippene for forebygging av økonomisk kriminalitet kan være anvendelig også på andre kriminalitetsområder.

Norsk senter for informasjonssikring (NorSIS) har på deres hjemmeside[90] en kontakttjeneste for informasjon om trusler, råd om forebygging og hjelp i forbindelse med kriminalitet og krenkelse på nettet.

NSM har også utarbeidet Grunnprinsipper om IKT-sikkerhet[91] og en rekke publikasjoner hvert år, fra kvartals- og årsrapporter til veiledninger og temahefter innenfor en rekke fagområder, og skjemaer,[92] samt en uformell blogg.[93]

Direktoratet for forvaltning og IKT (Difi) jobber for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen. Deres hjemmeside[94] inneholder veiledninger og råd som også er relevant for næringslivet.

På siden Nettvett.no[95] er det informasjon, råd og veiledning i bruk av internett. Informasjonen er rettet både mot enkeltpersoner fra barn til voksne, forbrukere og små og mellomstore bedrifter.

Næringslivets Sikkerhetsråd, PST, NSM og Politidirektoratet med har utgitt en veileder Sikkerhet ved ansettelsesforhold som er et hjelpemiddel for å redusere sannsynligheten for innsidervirksomhet.[96]

Temaet vold og trusler mot ansatte er beskrevet på hjemmesiden til Arbeidstilsynet.[97] Etaten har også utgitt en veileder.[98] Veilederen gir råd om hvordan virksomhetene kan arbeide med å fore bygge og håndtere vold og trusler som skjer i forbindelse med arbeidet. Varslingsutvalget har avgitt sin innstilling, NOU 2018: 6 Varsling – verdier og vern, hvor man foreslår å styrke varslervernet.[99] Arbeidstilsynet har også egne sider om varsling.[100] Varsling er også tema i siste nummer av Magma.[101]herunder forholdet mellom den ulovfestede styringsretten og det særskilte rettsvernet arbeidstaker har ved varsling,[102] regler om forbudet mot trakassering og seksuell trakassering, arbeidsgivers plikt til å forebygge trakassering samt regler om varsling og oppfølging av varsel,[103] varslingsrutiner på arbeidsplassen som redskap for åpenhet og trygghet, [104] varslingens ettervirkninger blant personer med varslererfaring i og utenfor arbeidslivet,[105] og erfaringer fra en leder som selv var varsler.[106] Vi anbefaler også en hjemmeside med råd både til arbeidsgivere[107] og varslere.[108]

[87] Energi Norge (2017)
[88] https://www.coso.org
[89] http://.acfe.com
[90] https://.norsis.no
[91] https://nsm.stat.no/globalassets/dokumenter/nsm_grunnprinsipper_ikt-sikkerhet_enkeltside_3008.pdf
[92] https://nsm.stat.no/publikasjoner/
[93] https://nsm.stat.no/blogg/
[94] https://www.difi.no/fagomrader-og-tjenester/informasjonssikkerhet
[95] Nettside drevet av blant annet NSM og NorSIS
[96] https://www.nsr-org.no/aktuelle-saker/sikkerhet-i-ansettelsesforhold-article1098-110.html
[97] https://www.arbeidstilsynet.no/tema/vold-og-trusler/
[98] https://www.arbeidstilsynet.no/contentassets/0cbb3bc6069a4008a3e4873900177c2f/veileder---vold-og-trusler-i-forbindelse-med-arbeidet.pdf
[99] http://varslingsutvalget.no/rapporter
[100] https://www.arbeidstilsynet.no/tema/varsling/
[101] https://www.magma.no/varsling-som-aktuelt-fenomen-i-norge2
[102] https://www.magma.no/forholdet-mellom-arbeidsgivers-styringsrett-og-arbeidstakers-varslervern-jf-arbeidsmiljoloven-2a-22
[103] https://www.magma.no/arbeidsgivers-ansvar-ved-trakassering-og-seksuell-trakassering2
[104] https://www.magma.no/varslingsrutiner-pa-arbeidsplassen-som-redskap-for-apenhet-og-trygghet2
[105] https://www.magma.no/innenfor-eller-utenfor
[106] https://www.magma.no/dette-larte-lederen-som-selv-var-varsler2
[107] https://www.governance.no/single-post/2018/01/04/varsling-rad-til-arbeidsgivere
[108] https://www.governance.no/single-post/2017/12/20/Har-du-tenkt-a-varsle-om-kritikkverdige-forhold-pa-

Referanser

Barane, Joakim Eike (2014): "Risikohåndtering krever analyser", *Teknisk ukeblad*, Oktober 2014

BDO (2017): *Risikoundersøkelsen 2017*

Benjaminsen (2017): *The Norwegian Downsizing Approach in Terms of the Insider Threat* (Masteroppgave), NTNU: Trondheim

Bergsjø, Håkon, & Ronny Windvik (2018): *Datasikkerhet for ledere – hvordan beskytte din virksomhet*, Oslo: Universitetsforlaget

BRÅ (2018): «Anmälda brott de senaste 10 åren», sist sjekket 13.04.18 på https://bra.se/brott-och-statistik/kriminalstatistik/anmalda-brott.html

Busmundrud, Odd, Maren Maal, Jo Hagness Kiran & Monica Endregard (2015): *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*, FFI-rapport 2015/00923

Dignes, Ingunn M. Grude (2016): *Vold mot politiet*

DST (2018): Straf20: Anmeldte forbrydelser og sigtelser efter overtrædelsens art og anmeldte og sigtede», sjekket 21.03.18 på http://www.statistikbanken.dk/STRAF20

E24 (2017): *Bare toppen av et isfjell*, sjekket 21.03.18 på https://e24.no/digital/datakriminalitet/bedrifter-svindles-for-hundrevis-av-millioner-bare-toppen-av-et-isfjell/24152475

Energi Norge (2017): *Veileder: Økonomisk kriminalitet i energibransjen*

Etterretningstjenesten (2018): *Fokus 2018*

Europol (2016): *Internet Organised Crime Threat Assessment 2016*

Europol (2017): *Internet Organised Crime Threat Assessment 2017*

Finans Norge (2016): *Finansnæringens arbeid mot kriminalitet – Trusler og sårbarheter*

Finanstilsynet (2017): *Risiko- og sårbarhetsanalyse (ROS) 2016*

IHS (2017): *The Internet of Things: a movement, not a market*, sist sjekket 20.04.18 fra https://cdn.ihs.com/www/pdf/IoT_ebook.pdf

Internet World Stats (2018): *Internet Growth Statistics*, sist sjekket 20.04.18 fra https://www.internetworldstats.com/emarketing.htm

Justis- og beredskapsdepartementet (2017): IKT-sikkerhet (Meld. St. 38 2016-2017)

Kjørstad, Ole Martin (2016): "Hvorfor bør styret stille tydeligere krav til risikostyringen?", *SIRK* (2): 39-43

Liljedahl, Dag (2017): Innsidetrussel: Den største utfordringen for mange [blogginnlegg], sist sjekket 29.04.18 på https://www.bdobloggen.no/2017/03/19/innsidetrussel-den-storste-utfordringen-for-mange/

NRK (2018): Dømt for grov korrupsjon mot Drammen kommune, sjekket 21.03.18 på https://www.nrk.no/buskerud/domt-for-grov-korrupsjon-mot-drammen-kommune-1.13972605

Norsis (2017a): *Politi spilte direktør og rundlurte svindlere*, sist sjekket 13.04.18 på https://norsis.no/politi-spilte-direktor-rundlurte-svindlere/

Norsis (2017b): *Trusler og trender 2017-18*

Norsis (2017c): *Nordmenn og digital sikkerhetskultur*

NSM (2016a): *Fire tiltak stopper opp mot 90 prosent av dataangrep*, sist sjekket 13.04.18 på https://www.nsm.stat.no/virksomhetssikkerhet/fire-enkle-tiltak-stopper-90-prosent-av-dataangrep/

NSM (2016b): Håndbok: *risikovurdering for sikring*

NSM (2017a): *Risiko 2017 – Risiko og sårbarheter i en ny tid*

NSM (2017b): *Helhetlig IKT-risikobilde*

NSM (2018): *Risiko 2018 – Verdifulle individer – Verdifulle virksomheter – Verdifull infrastruktur*

NSR (2014): *Mørketallsundersøkelsen 2014*

NSR (2016): *Mørketallsundersøkelsen 2016*

NSR (2017): *Kriminalitets- og sikkerhetsundersøkelsen i Norge 2017 (KRISINO 2017)*

NTAES (2017a): *Situasjonsbeskrivelse 2017*

NTAES (2017b): *Nyere betalingstjenester - grunnlagsdokument*

Porter, Michael E. (1985): *The Competitive Advantage: Creating and Sustaining Superior Performance*, New York: Free press

PST (2018): *Trusselvurdering 2018*

SSB (2018): Tabell 07091: Virksomheter, etter næring (SN2007) og antall ansatte (K) 2009 - 2018

STAMI (2015): *Faktabok om arbeidsmiljø og helse 2015 – Status og utviklingstrekk*

Stranden, Roy (2017): "Sikringsrisikoanalyse: Bruk rett verktøy til rett job", sist sjekket 07.05.18 på https://www.beredskapsbloggen.no/sikringsrisikoanalyse-bruk-rett-verktoy-til-rett-jobb

Symantec (2017): *Internet Security Threat Report: Ransomware 2017*

Telenor (2017): *Digital sikkerhet 2017*

Trendlabs (2016): *TrendLabs 2016 Security Roundup*