Trusselvurdering 2022

TRUSSELVURDERING 2022

Årlig trusselvurdering 2022 er utarbeidet av Group Security og Financial Cyber Crime Center med bidrag fra DNB Livsforsikring. Trusselvurderingen består av vurderinger av trusselnivået for DNB innenfor syv ulike kategorier og seks artikler som omhandler generelle tema. Rapporten tar sikte på å gi en bredest mulig vurdering av relevante sikkerhets-trusler mot DNBs virksomhet i en tids-ramme av ett til tre år frem i tid.

Group Security koordinerer arbeidet og ansvarlig for utgivelsen er Anders Hardangen, Sikkerhetsdirektør DNB.

Innhold

Om årlig trusselvurdering

Å forstå trusselbildet er avgjørende for å kunne forstå sin sikkerhetsrisiko.
Ved å se på hendelser og angrep kan man forstå hvordan trusselaktørene opererer, og hvilke verktøy og metoder de benytter for å oppnå det de ønsker.
Forståelsen av eksterne drivere er instrumentell i å prioritere riktig sikkerhetsnivå balansert opp mot brukervennlighet og effektivitet. For DNB er dette et viktig virkemiddel for å planlegge hvordan vi skal forsvare våre og kundens verdier.
I år er et annerledes år, med en storkrig i Europa. Mens vi de siste årene har sett et relativt stabilt europeisk trusselbilde i det fysiske rom har dette endret seg drastisk med krig mellom Russland og Ukraina. Vi er kun i startfasen av en økt spenning mellom vår nærmeste nabo Russland og den vestlige verden, og det er for tidlig å si hvordan dette vil utvikle seg. Det som imidlertid er sikkert er at vi fremover må ta høyde for mulige trusler i det fysiske domenet også i våre nærområder.

Den digitale trusselen er fortsatt høy, og nå også videre forhøyet i en mer polarisert verden. Vi ser at digitale angrep brukes som virkemiddel i konflikter og et mulig utfall er at dette vil øke i takt med den sikkerhetspolitiske spenningen.

I tillegg til enorme ødeleggelser og menneskelig lidelse får konflikten i Ukraina mange økonomiske og finansielle implikasjoner. I sikkerhetsdomenet medfører den endrede sikkerhetssituasjonen for DNB først og fremst endringer i trusselen i det digitale rom.
Utviklingen i Ukraina, europeisk og global sikkerhet blir gitt omfattende behandling i media. Kapitlene om digitale trusler og bedrageri tar for seg hvordan den endrede situasjonen påvirker trusselbildet for DNB.
For DNB er det viktig å beskytte våre samfunnsviktige finanstjenester.
Vi fortsetter å bruke trusselinformasjon for å forstå hva som skjer rundt oss og for å kunne styrke intern kunnskap for å lettere ta de riktige beslutningene.
Sammen med våre rapporter over observerte cyberangrep og bedragerier publiserer vi også i år vår trusselvurdering offentlig for å øke bevisstheten i samfunnet om truslene vi står overfor. Vårt formål er som alltid å øke bevissthetten både rundt det vi observerer der ute og hva vi opplever av ulike angrep mot DNB og våre kunder.

Jeg vil gjenta fjorårets budskap om at vi står i sammen mot de som vil skade eller stjele fra oss.

Anders Hardangen,
Sikkerhetsdirektør, DNB

Forord

Kriminalitetstrusselen i det digitale rom øker. Digitaliseringen av det norske samfunnet har også tiltatt, delvis drevet av to år med pandemi, og vår totale sårbarhetsflate har ekspandert i takt med den. I tillegg er det nå krig i Europa – en krig som også utkjempes digitalt. Alt dette har gitt både vinningskriminelle og andre kriminelle trusselaktører større handlingsrom. Hverdagen for alle sikkerhetsmiljøene der ute består av skarpe trefninger og kontinuerlig oppdragsløsning. Løsepengevirus, datainnbrudd, datatyveri og bedragerier rammer norske borgere og virksomheter bredt, og forårsaker store økonomiske tap. Kryptovaluta, anonymiseringstjenester, kryptering og nye betalingstjenester legger til rette for hvitvasking og annen kriminalitet. Vi trenger gode analyser som grunnlag for effektive tiltak for å forebygge og håndtere slike tap og trusler.
Vi trenger et sterkt offentlig/privat samarbeid for å møte utfordringene.

Teknologi er en betydelig driver for så godt som alle kriminalitetsutfordringer og trusler mot norske verdier. Den teknologiske utviklingen bidrar til at alle prosesser i samfunnet kan gå raskere, og påvirker samtidig selve endringshastigheten. Den fører med seg en akselerasjon som er betegnende for vår tid og våre utfordringer, og stiller nye krav til tidlig varsling om oppdukkende trusler og snar respons. Åpenhet, delingsvilje og evne til koordinering er avgjørende for om vi lykkes.

Vi må tenke på hvilke sårbarheter som oppstår samtidig som vi tenker utvikling, slik at sikkerhet ikke kommer halsende etter nye løsninger.

Norsk næringsliv er et attraktivt mål for kriminelle i utlandet. Vår geografiske plassering langt nord er ingen beskyttelse i det digitale rom. Truslene er sammensatte og grenseoverskridende, og verktøyene og virkemidlene som rettes mot oss er i stadig utvikling. Slagkraftig bekjempelse av kompleks kriminalitet i kontinuerlig endring fordrer at også vi utvikler oss, våre metoder og våre sektorovergripende samarbeid.
En forutsetning for det, og for et helhetlig svar på truslene vi står overfor, er at vi deler kunnskap mellom alle gode krefter i samfunnet. Sammen forvalter vi et mangfold av kilder og sensorer som alle bidrar til motstandsdyktighet og forsvarsevne i det private så vel som i det offentlige.

I Kripos ser vi at det internasjonale samarbeidet er helt sentralt for å forebygge, avverge og etterforske kriminalitet i det digitale rom. Vi opplever at norsk politi er en ønsket samarbeidspartner i internasjonale operasjoner, og vi må sette av ressurser til å være aktivt med i utviklingen av det internasjonale samarbeidet fremover.

Det er ikke gitt at morgendagens trusler består av elementer som er kjente i dag. Men for å produsere gode vurderinger om framtiden er vi nødt til å forstå samtiden, både overordnet og i detalj. Trusselvurderinger som DNBs årlige rapport er en viktig del av å bygge denne forståelsen, og å sikre at vi alle er informerte og omforente i vår innsikt om truslene mot oss. Rapporten er en viktig byggesten i vår felles innsats for trygghet, sikkerhet og det vernet om verdier som samfunnet vårt har behov for. Gjennom slik kunnskapsdeling setter vi både hverandre og oss selv i stand til å utgjøre en forskjell.

Politiet deler nå for andre år på rad kunnskap gjennom vår åpne trusselvurdering. Politiets trusselvurdering skal være et bidrag til felles situasjonsforståelse, så både hver enkelt av oss, næringsliv og myndigheter, kan forstå trusselbildet bedre, gjøre gode valg og dermed forebygge kriminalitet best mulig.

Kristin Kvigne,
Sjef Kripos

Nøkkelfakta

Terrorisme: Like truet som samfunnet rundt oss

Bankran forekommer sjelden i Norge

Ansatte utsettes enkelte ganger for grove trusler

Mobiltelefonen, er den sikker som banken?

Norske forsikringsselskap svindles hvert år antakelig for flere milliarder kroner

DNB Livsforsikring tar i bruk kunstig intelligens for å avdekke svindel

130 falske DNB-nettsider forsøkt brukt i svindel oppdaget og stengt ned

Rundt 40 millioner e-poster som utgir seg for å være DNB stoppet på internett

Ingen norske selskaper er immune mot innsidetrusselen

Massiv økning i phishingangrep mot privatpersoner

Kryptovaluta brukes for å sikre utbytte fra svindel

Antallet bedragerisaker har økt med 66 % siden 2021

Organiserte kriminelle i Sverige knyttes til omfattende lånebedragerier

Løsepengevirus utgjør en økende trussel mot norske bedrifter

Cyberkriminelle grupper tar side i statlige konflikter

Private selskaper kan rammes som ledd i hybrid krigføring mellom nasjonsstater

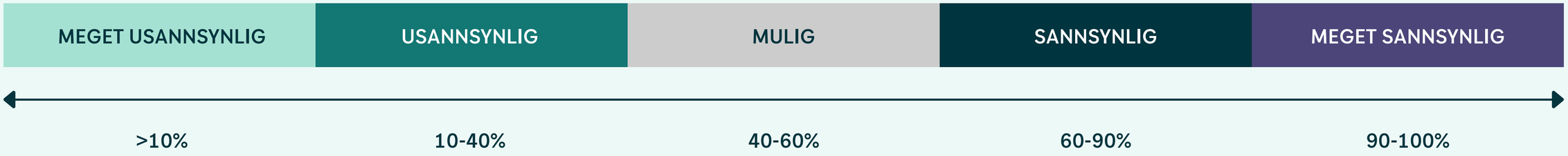
Tiden fra en sårbarhet blir kjent til den blir aktivt utnyttet, er stadig kortere

Digitale trusler fortsatt den største risikoen

Trusselnivå

DNB BENYTTER FØLGENDE KRITERIER FOR VURDERING AV TRUSSELNIVÅ:

TRUSSELNIVÅ / SANNSYNLIGHET FOR HENDELSE	BESKRIVELSE AV TRUSSELNIVÅ
KRITISK	Det er meget sannsynlig at DNB vil bli angrepet av avanserte *eller* koordinerte *eller* flere sammenfallende trusselaktører med intensjon *og* kapasitet til å påføre betydelig skade.
HØYT	Det er sannsynlig at DNB vil bli angrepet av trusselaktør(er) med intensjon *og* kapasitet til å påføre betydelig skade.
MODERAT	Det er mulig at DNB vil bli angrepet av trusselaktør(er) med intensjon *og* kapasitet til å påføre betydelig skade.
LAVT	Det er usannsynlig at DNB vil bli angrepet av trusselaktør(er) med intensjon *og* kapasitet til å påføre betydelig skade.
UBETYDELIG	Det er meget usannsynlig at DNB vil bli angrepet.



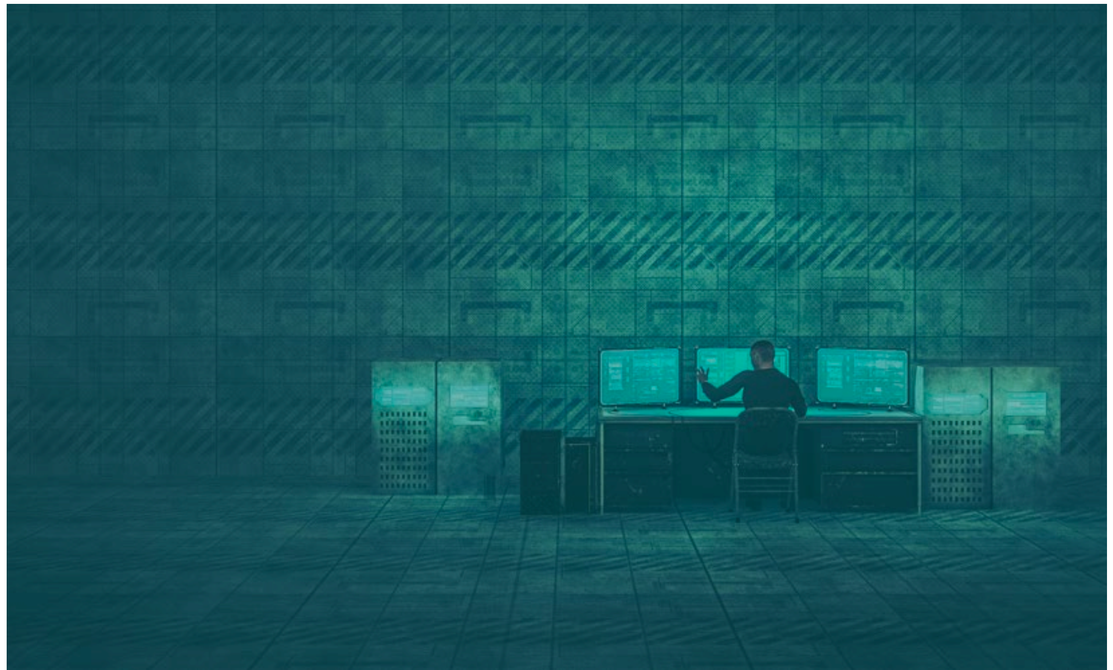
Digitale trusler

De digitale truslene mot DNB vedvarer. Hver dag forsøker trusselaktører å trenge inn i DNBs digitale infrastruktur i den hensikt å få tak i informasjon, sabotere eller å oppnå økonomisk vinning. I 2021 håndterte DNB 27 slike saker som hadde et alvorlig skadepotensial for konsernet. Dette representerer en liten nedgang fra året før. Trusselbildet er i stadig endring og har i økende grad blitt et samfunnsproblem. Cyberangrep kan medføre stor skade med konsekvenser for både renommé, tapte inntekter, forpliktelser mot kunder og tilgjengelighet til finansielle tjenester. Som følge av dette er sikkerhet et samfunnsansvar som DNB tar på alvor og et tema som angår alle ansatte på alle nivåer i organisasjonen. Årlig trusselvurdering understøtter dette og har til hensikt å forbedre sikkerhetsmessige vurderinger i organisasjonen.

ENDRET SIKKERHETSSITUASJON I EUROPA

Krigen i Ukraina har skapt en ny sikkerhetssituasjon i Europa. Selv om det ikke er rapportert om cyberangrep mot vestlige finansinstitusjoner gjør situasjonen at cyber-domenet har blitt enda mer uoversiktlig. Blant partene i krigen er det Russland som besitter kapabiliteter som i ytterste konsekvens kan bli brukt slik at de kan skade DNBs drift. I forbindelse med krigen har det blitt observert at både hacktivist-miljø, og cyberkriminelle har utført cyberangrep til støtte for det disse miljøene oppfatter som enten Russlands eller Ukrainas interesser. I cyberdomenet har vi ikke den samme typen grenser som vi har geografisk – en trusselaktør kan sitte hvor som helst i verden og utføre sine operasjoner.

Et scenario som kan utspille seg, er at skadevare eller angrep ment for krigen sprer seg og får utilsiktede konsekvenser andre steder. Dette skjedde i 2017 ved spredning av «NotPetya» skadevare i Ukraina, og igjen ved krigens utbrudd 24 februar 2022.



Samme dag som invasjonen startet rapporterte det amerikanske kommunikasjonsselskapet Viasat at en «cyberhendelse» hadde medført operasjonelle utfordringer for en satellitt som leverer bredbåndstjenester i Ukraina og omliggende land i Europa. Angrepet medførte nedetid i leveranser av bredbåndstjenester i Ukraina, men også tjenester i andre land fikk problemer. For eksempel mistet noen kunder i Frankrike internett, og man mistet kommunikasjonsmulighet med 5800 vindturbiner i Tyskland da de benyttet samme satellitt.

For både NotPetya-angrepet og angrepet mot satelitten KA-SAT har flere pekt på at det mest sannsynlig er russisk etterretning som står bak cyberangrepene. Det er vanskelig å vurdere hvordan situasjonen og cybertrusselen kan utvikle seg, og informasjonsutveksling for å forstå trusselbildet fremstår som enda viktigere enn tidligere.

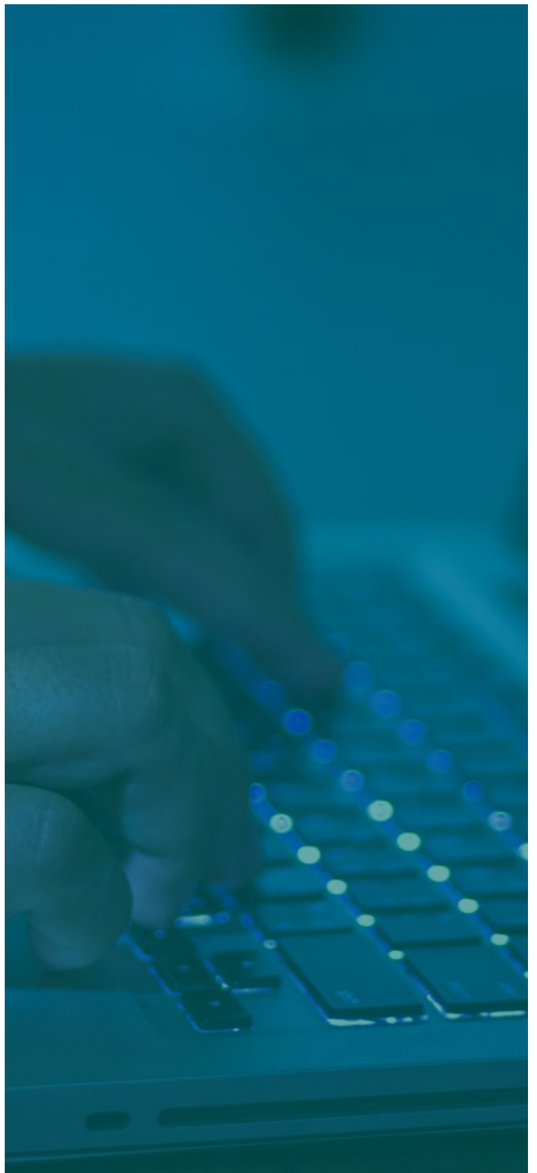
ORGANISERTE KRIMINELLE UTGJØR DEN STØRSTE TRUSSELEN

Det er først og fremst økonomisk motiverte kriminelle trusselaktører som har som mål å utføre cyberangrep mot DNB. Disse gruppene har cyberkriminalitet som profesjon og fungerer i økende grad som profesjonelle bedrifter – med stillingsannonser, arbeidstider og ansattgoder. Lønnsomheten og formaliseringen til disse gruppene gjør at virksomheten deres blir mer sofistikerte, og de investerer i utvikling og forskning. Dette fører til at trusselen blir mer kompleks – og virksomheter som beskytter seg mot disse må stadig heve sikkerheten sin for å operere på samme risikonivå som tidligere. Slike kriminelle organisasjoner har ofte tilholdssted i Øst-Europa og Afrika.

E-POST OG SÅRBARHETER I INTERNETT-EKSPONERT INFRASTRUKTUR SOM ANGREPSVEKTOR

E-post er fortsatt mye brukt av cyberkriminelle som et ledd i angrepskjeden. Da forsøker aktøren å lure den ansatte til å trykke på lenker eller åpne skadelige vedlegg som kan plassere ut skadevare eller bakdører på datamaskinen dette åpnes fra. I andre tilfeller forsøker de å få den ansatte til å oppgi sin innloggingsinformasjon for å få tilgang til datamaskinene på egenhånd. I DNB ser vi mange kampanjer hvor aktører sender ut et stort antall e-poster med generisk tematikk, som for eksempel falske lønnsslipper, hentemeldinger eller deling av filer. Disse aktørene er opportunistiske, og håper å nå ut til så mange som mulig med visshet om at ikke så mange av de som mottar e-posten kommer til å la seg lure.

Andre aktører jobber mer målrettet og har utpekt DNB som et mål. Disse bruker som regel mer tid på å tilegne seg kunnskap om DNB og konsernets ansatte før de sender e-post. På den måten kan de skreddersy tematikken tilpasset målet.I 2021 så vi flere kampanjer hvor porteføljeforvaltere fikk denne typen e-post med svært målrettet tematikk. For eksempel fikk forvaltere med geografiske ansvarsområder e-post fra fiktive avsendere i nettopp denne regionen. DNB bruker tid på å kartlegge aktørene som går målrettet mot oss i hensikt å kunne forstå hvordan de opererer, for så å kunne detektere og stanse inntrengingsforsøk.



Det er sannsynlig at trusselaktøren som sto bak e-postene til porteføljeforvalterne våre søkte tilgang til DNBs datasystemer for å installere en bakdør som kunne benyttes for innlogging.

En annen vanlig metode som trusselaktørene benytter seg av for å få fotfeste i en organisasjons datasystemer, er å utnytte sårbarheter i digital infrastruktur som er eksponert på internett. All digital infrastruktur kan inneholde iboende sårbarheter, og når disse oppdages må man raskt gjøre tiltak eller installere sikkerhetsoppdateringer for å fjerne sårbarhetene.

En trend DNB har sett er at tiden det tar fra en sårbarhet blir kjent til trusselaktører utnytter den blir kortere.

Det vil si at virksomheter har mindre tid til rådighet for å iverksette tiltak og installere sikkerhetsoppdateringene enn man har hatt tidligere.

Hvis ikke kan konsekvensen bli at uvedkommende får tilgang til nettverket.

STATLIGE AKTØRER

Selv om cyberangrep for økonomisk vinning er effektive og vurderes som den største trusselen mot DNB, er det på ingen måte forbeholdt cyberkriminelle å gjennomføre slike angrep. Statsaktører fortsetter å utvikle kapabiliteter for å støtte opp under landets ambisjoner og informasjonsbehov.

Kampanjene deres er ofte svært sofistikerte, vanskelige å oppdage, de har lang utholdenhet og retter seg kontinuerlig mot både kommersielle og statlige interesser. Selv om det finnes unntak, skiller statsaktører seg normalt ut ved å ha fokus på å få tilgang til informasjon eller understøtte sine lands politiske agenda fremfor økonomisk vinning.

Det kan være økonomisk informasjon, informasjon om personer eller om IT-infrastruktur. En fellesnevner for disse trusselaktørene er at de er godt finansiert, tålmodige og vil strekke seg langt for å nå målet sitt selv om det innebærer å påvirke eller utnytte andre virksomheter for å nå sitt sluttmål. Også DNB har opplevd at statsaktører har forsøkt å få tilgang til bankens datasystemer, men dette forekommer langt mer sjelden enn forsøk fra kriminelle aktører.

DESTRUKTIVE ANGREP OG DIGITAL UTPRESSING

Angrep med krypteringsvirus er fortsatt den største digitale trusselen mot DNB. Formålet med krypteringsvirus er å få tilgang til offerets datamaskiner og kryptere filene slik at de blir utilgjengelig for brukeren. For at offeret skal få tilgang til filene sine igjen, krever angriperen løsepenger. Disse ønskes ofte betalt i kryptovaluta, og beløpet som ofrene må betale har økt jevnlig. I nyhetene ser vi store selskaper tape hundrevis av millioner dollar i kostnader og tapte inntekter som følge av krypteringsvirus.

Dersom man ikke betaler løsepenger for å få tilbake de krypterte filene, krever det ofte at den rammede virksomheten har sikkerhetskopi (backup) av dataene sine. Mange virksomheter har også opplevd at sikkerhetskopien blir rammet av krypteringsvirus hvis den ikke er helt adskilt fra datasystemene. Hvis virksomheten har sikkerhetskopi av sine data, er det å tilbakestille denne som regel en krevende og svært omfattende jobb. Å få installert krypteringsvirus i sitt nettverk får derfor sannsynligvis alvorlig påvirkning på normal drift.

I 2021 har vi sett en markant trend hvor trusselaktørene ikke nøyer seg med å kryptere filene alene. I tillegg til at dataene gjøres utilgjengelige, truer aktørene med å publisere informasjonen offentlig dersom virksomheten ikke betaler. Noen trusselaktører går enda lenger: De kontakter partnere og kunder og truer med å ramme dem også hvis de ikke betaler, eller kombinerer krypteringsvirus med tjenestenektangrep (se forklaring på neste side). Krypteringsvirus har de siste årene i økende grad blitt en profesjonalisert industri. Cyberkriminelle selger tjenesten på markedsplasser på «Darknet» (se faktaboks). Aktører som mangler de tekniske ferdighetene for å utføre denne typen angrep selv kan bestille dem.

Når cyberangrep kommersialiseres som tjenester reduseres terskelen for gjennomførelse. Dette fører til at flere virksomheter blir utsatt for angrep. Aktørene går målrettet til verks i sine operasjoner, og bruker tid på å kartlegge målene sine. I november 2021 utstedte FBI en advarsel om at aktørene «bruker betydelige økonomiske hendelser, som fusjoner og oppkjøp, for å målrettet utnytte offerselskaper for krypteringsvirus».

MYNDIGHETER SKJERPER INNSATSEN

Å bedrive cyberkriminalitet har i lang tid vært tilnærmet risikofritt og trusselaktørene har kunnet operere uten å risikere straffeforfølgelse. De siste årene har man sett flere eksempler på internasjonalt samarbeid i kampen mot cyberkriminalitet. Flere land har innført sanksjoner mot kriminelle cyberaktører.

Darknet er en liten del av internett som kun er tilgjengelig ved hjelp av å bruke spesielle nettverk.

Sanksjonene innebærer at bankkontoer har blitt fryst, og det blitt innført innreiseforbud og forbud mot handel med personene og grupperingene. Virksomheter som betaler løsepenger til sanksjonerte grupperinger risikerer store konsekvenser i form av bøter, utestengelse fra valutahandel eller fengsel hvis dette forbudet brytes.

I 2021 førte internasjonal innsats tilrettelagt av Europol til arrestasjonen av syv individer tilknyttet en organisert kriminell cyberaktør, og to andre grupper ble fratatt utstyr benyttet i cyberangrep. Dette er viktige tiltak som bidrar til at risikoen øker for de kriminelle grupperingene, og de kan i mindre grad operere uten at det kan få konsekvenser for dem. Dette vil forhåpentligvis virke avskrekkende på de eksisterende grupperingene, og hindre at volumet av cyberkriminelle øker.

TJENESTENEKTANGREP

Tjenestenektangrep, populært referert til som DDoS (Distributed Denial of Service), er en form for destruktivt angrep hvor en angriper sender så mye datatrafikk mot en nettside eller infrastruktur at denne blir overbelastet og utilgjengelig. Dersom en angriper utfører tjenestenektangrep mot nettbanken vår, betyr det at denne kan bli utilgjengelig for kundene våre. Vi opplever fortsatt at tjenestenektangrep utføres mot DNB ved jevne mellomrom, og har i den forbindelse opplevd å få utpressing via e-post der trusselaktøren krever at DNB skal betale penger for at de skal slutte å sende trafikk mot oss. DNB har ikke betalt løsepenger for å stanse tjenestenektangrep, men blokkerer trafikken i samarbeid med tjenesteleverandører. Vi forventer at tjenestenektangrep fortsetter på samme nivå fremover.

INFORMASJONSTYVERI

DNB besitter store menger kundeinformasjon, markedsinformasjon og teknisk informasjon som er av interesse for enkelte aktører. Kortdetaljer, pengeoverføringer, informasjon om hvor innkjøp gjøres og oppkjøp av selskaper er eksempler på informasjon som kan si mye om personer eller selskaper.

Det finnes eksempler på finansinstitusjoner som har vært kompromittert over svært lang tid, i noen tilfeller flere måneder, hvor trusselaktøren i prasis har hatt tilgang til slik informasjon. Likevel ser vi at de aller fleste forsøkene på å trenge inn i DNBs IT-systemer ikke handler om spionasje, men er motivert av kriminell økonomisk vinning.

DIGITALE BANKRAN

De siste årene har vi sett en nedgang i forsøk på digitale bankran hvor trusselaktørene forsøker å få illegitim tilgang til bankens datasystemer og overføre penger ut av banken. Å gjennomføre digitale bankran er teknisk krevende, og har blitt enda vanskeligere de siste årene. Samtidig ser vi at det har vært en økning innenfor krypteringsvirus og digital svindel. Vår vurdering er at det er en sammenheng mellom nedgangen i digitale bankran og at aktørene har tatt i bruk andre metoder for å oppnå økonomisk vinning.

LEVERANSEKJEDEANGREP

I leveransekjedeangrep infiltrerer trusselaktøren et datasystem eller nettverk via en partner eller leverandør som har rettmessig tilgang. Da kompromitterer trusselaktøren tredjeparten først, og så utnyttes den allerede etablerte tilliten mellom tredjeparten og sluttmålet. Det kan være flere grunner til at trusselaktøren velger denne løsningen.

En kan være at tredjepartsleverandøren har dårlige sikkerhet enn sluttmålet. En annen kan være at tredjeparten, gjerne en tjenesteleverandør, kan ha tilgang til mange virksomheter, og på den måten får trusselaktøren tilgang til disse virksomhetene gjennom tredjepartsleverandøren. Da kan trusselaktøren fokusere på å kompromittere én virksomhet, og gjennom den få tilgang til mange. Det finnes flere metoder trusselaktøren kan velge for å tilnærme seg sluttmålet sitt gjennom en tredjepart:

- Det har blitt observert flere tilfeller der sikkerhetsoppdateringer inneholder en bakdør. Når virksomheter oppdaterer sine systemer, får de også installert bakdøren i systemene sine.
- En annen metode er å ta over en e-postkorrespondanse og sende ondsinnede vedlegg som mottakeren forventer, og sånn sett ikke vekke mistanke.
- En tredje metode er hvis tredjeparten har direkte tilgang inn i nettverket til sluttmålet – da kan denne tilgangen utnyttes direkte.

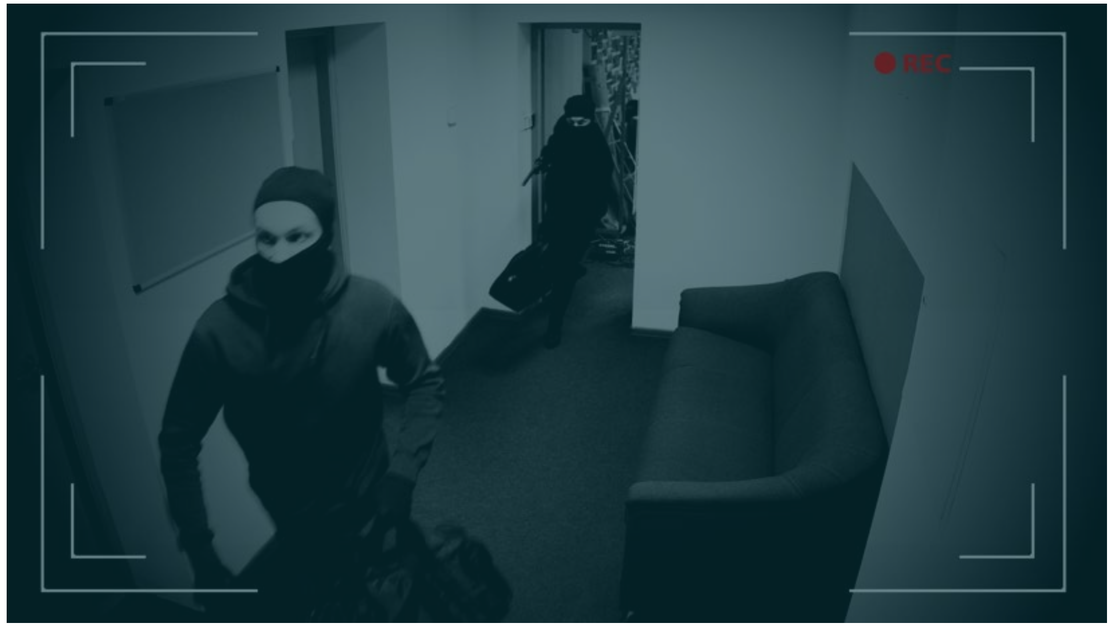
Mange virksomheter er avhengige av å kjøpe tjenester og programvare fra underleverandører. Dette gjelder også DNB. Vi vurderer denne trenden å være økende og trolig blir den mer utbredt i kommende år. I lys av dette blir håndtering av tredjepartsrisiko viktigere enn før, og sikkerhetsmessige vurderinger ved integrasjon av tredjeparter må gjøres i større grad som et forebyggende tiltak. Vi må forvente angrep via tredjeparter, og derfor være i stand til å forsvare oss mot det når det skjer.

Ran og voldelig utpressing

ETT RAN AV BANK- OG POSTKONTOR I NORGE I 2021, SVENSKE RANERE PÅGREPET.

I mai 2021 ble Etterstad postkontor i Oslo ranet av tre personer for et mindre beløp. To ansatte ble ved åpning av postkontoret tvunget inn gjennom bakdøren av to ranere. Gjerningspersonene forlot åstedet i en personbil med stjålne skilter. Etterforskning avdekket etter hvert at bilen med ranerne hadde krysset inn fra Sverige. I starten av august ble tre personer med bosted i Sverige arrestert i stocksholmsområdet. Den lave trafikken inn og ut av Sverige som følge av restriksjoner knyttet til Covid-19 var sannsynlig medvirkende til at politiet kunne identifisere bilen.

Antallet ran av bank og postkontor i Norge har de siste årene sunket til noe under ett ran per år. Siste "sjokkbrekk" med tyveri av en komplett minibank i Norge skjedde tilbake i 2019. Ran av minibanker under tømming eller fylling, samt "sjokkbrekk" mot minibanker forekommer meget sjelden. Gjennom 2021 er vi ikke kjent med tilfeller av gisseltaking av nærstående eller andre former for voldelig utpressing mot bankansatte i Norden. Før det seneste ranet omtalt over må vi tilbake til 2017 for å finne et ran utført av flere gjerningspersoner. Øvrige ran i Norge har vært utført av enkeltpersoner og har vært preget av dårlig organisering. I Sverige er det fortsatt aktive ransligaer med bedre organisering. Det er mulig at en del av ranene i Sverige har vært utført av østeuropeiske kriminelle. Trenden i svenske bank- og postran har vært synkende de siste årene. Det ventes at antallet ran mot bank- og postkontor i Norge i 2022 og inn i 2023 fortsetter på et nivå på noe under ett ran per år.



Vold og trusler mot ansatte

DET HENDER AT DNBS ANSATTE BLIR TRUET AV KONSERNETS KUNDER.

I løpet av 2021 opplevde DNB i Norge tre hendelser hvor ansatte ble utsatt for vold og 29 hendelser hvor ansatte ble truet med voldelige handlinger. Tallet er veldig nært tallet for 2020 og den totale trenden er stabil. Det er et skifte over til at 70 prosent av truslene er per telefon mot tidligere omtrent 50 prosent. Dette skiftet skyldes sannsynlig Covid-19 nedstengninger med redusert tilgang til banklokaler. Vi er kjent med at det av forskjellige årsaker er mørketall i innrapportering av hendelser. Sannsynlig ligger det totale antallet hendelser i området 40-50.

De som truer DNB-ansatte er privatkunder og de opptrer som enkeltpersoner. Ingen av hendelsene med vold eller trusler kan spores til organisert kriminalitet eller noen form for systematisk utpressing. I noen få tilfeller skjer hendelsene i forbindelse med eiendomstransaksjoner. Eksempler på utløsende årsaker inkluderer kunder som truer når de ikke får tilgang til midler fordi kontoen er tom, fordi minibankkortet er låst i en minibank, fordi de ikke får sin BankID til å virke, eller fordi de på grunn av Covid-19 tiltak ikke får slippe inn uten forhåndsavtale. Eksempler på hva ansatte har opplevd: trusler om fysisk skade, kunder som sier de vil ta med en pistol i banken, bråk i inngangspartiet når ansatte skal hjem, og ansatte som har blitt fysisk angrepet og endt opp i slåsskamp på gulvet med kunde som trengte seg inn i banklokalet. En person kom til samme bankkontoret og opptrådte truende/utagerende tre dager på rad. Fire ganger har kunder truet med å komme hjem til ansatte, men dette har ikke materialisert seg.

Heldigvis har voldshendelsene kun endt med mindre skader. Voldshendelser, utagerende adferd i banklokalene og trusler er likevel psykisk belastende for ansatte, ikke bare for den som blir direkte rammet, men også for kollegaer i nærheten.

Ved hendelser med trusler eller vold utløses det en rekke tiltak. Det er ofte varsling, oppfølging på stedet, leders oppfølging og oppfølging fra sikkerhets-avdelingen. En del ganger blir politiet tilkalt. I ettertid skal ansatte som har blitt eksponert følges opp med støtte-samtaler og lokale sikkerhetsprosesser blir gjennomgått. Det må brukes tid på sikring av bevis og politianmeldelse. En enkelt hendelse krever ofte mye ressurser i oppfølging.

DNB har kun egne tall å støtte oss på, men vi observerer en økning av hendelser i 2020 og 2021, samtidig med at Covid-19 pandemien har medført nedstengninger. Det er usikkert om endringen skyldes bedre rapportering eller nedstigningen i samfunnet. I mange av hendelsen er det tegn på at personene som truer er ruset og/eller har psykiske problemer.

Den gjennomgående trenden i samfunnet er at anmeldt voldskriminalitet (unntatt seksualforbrytelser) går sakte nedover. Utover sammenfallet med Covid-19 ser vi ingen spesifikk trend i samfunnet som kan ha virket inn på nivået av hendelser.

UTSIKTER MOT 2023

I 2022 og inn i 2023 er det vår vurdering at vi vil stå overfor 40-50 hendelser med trusler eller vold mot ansatte. Det store flertallet av hendelser vil være utagerende/truende adferd eller trusler, men med noen få tilfeller av vold. Det er moderat sannsynlighet for at en eller noen få ansatte kan komme til skade som følge av en voldshendelse.

Terrorisme og politisk motivert vold – en indirekte trussel

NORGE

I sin åpne trusselvurdering for 2022 vurderer PST det som mulig at høyre-ekstremister så vel som ekstreme islamister vil forsøke å utføre terrorhandlinger i Norge i 2022. Det knyttes særlig bekymring til at høyreekstrem aktivitet i stor grad finner sted i det digitale rom. PST viser til økt aktivitet blant personer med en antistatlig overbevisning i Norge. Det vurderes som lite sannsynlig at personer motivert av slikt tankegods vil forsøke å utføre terrorhandlinger.

De siste årene har det imidlertid vært en økning av volds- og sabotasjehandlinger motivert av antistatlige tankegods i flere vestlige land. Disse handlingene har primært vært rettet mot statlige mål, vaksinesentre og enkeltpersoner knyttet til håndteringen av pandemien. Det vurderes videre som svært lite sannsynlig at venstreekstremister og klima- og miljø-vernaktivister vil begå terrorhandlinger. Det vurderes som mer sannsynlig at slike aktører vil kunne begå skadeverk eller ordensforstyrrelser.

DNB I UTLANDET

Flere av landene DNB er til stede i har vært utsatt for terrorangrep de senere årene. DNB faller inn under den over-ordnede terrortrusselen i landene vi opererer i, og kan rammes indirekte av en eventuell terrorhandling. De fleste terrorangrepene som har rammet vestlige land har vært rettet mot folkerike steder og symbolmål som terroraktørene definerer inn i kjernen av sitt fiendebilde.

De siste to årene har antallet terror-angrep mot mål i Europa holdt seg stabilt. Europol rapporterer om en betydelig nedgang i antall terrorrelaterte arrestasjoner i EU-landene i 2020, og setter dette i sammenheng med pandemi-situasjonen. Det er uklart hvorvidt dette indikerer redusert aktivitet blant terror-aktører eller om det skyldes endret operasjonell kapasitet hos offentlige myndigheter og sikkerhetstjenester som følge av pandemien.

UTSIKTER MOT 2023

Det er ingen informasjon som tilsier at DNB er del av fiendebildet til høyreek-stremister eller ekstreme islamister verken i Norge eller i utlandet. Det vurderes som usannsynlig at DNB vil utgjøre primærmål for en terrorhandling. DNB vil imidlertid kunne rammes indirekte av en terrorhandling rettet mot mål i nær-heten av våre lokasjoner, eller ved at DNBs ansatte oppholder seg på feil sted til feil tid.

Bedrageri som organisert kriminalitet mot DNB – både nytenkende og tradisjonell

LÅNEBEDRAGERIER

DNB opplevde i 2021 et betydelig omfang av lånebedragerier rettet mot DNB Finans' bilfinansieringsprodukter. I likhet med prediksjonen fra fjorårets trusselvurdering, har organiserte kriminelle grupperinger med tilknytning til land som Sverige, Litauen, Romania, Syria og Albania fortsatt å systematisk misbruke bankens låneprodukter. Det er sannsynlig at disse gruppene begår økonomisk kriminalitet for å finansiere narkotikakriminalitet, menneskehandel og annen gjengrelatert kriminalitet. Dette temaet utforskes nærmere i rapportens temaartikkel om organisert kriminalitet. I tillegg til å ha innvirkning på enkeltpersoners skjebner, utgjør disse aktørene samlet sett et stort samfunnsproblem. Det er meget sannsynlig at slike grupperinger vil fortsette å misbruke DNBs låneprodukter gjennom 2022, og at de i forbindelse med dette vil fortsette å utnytte sårbare mennesker for å oppnå egen vinning. DNB registrerer også jevnlig tilfeller av forfalsket lønnsdokumentasjon eller fiktive eiendomsvurderinger ved misbruk av boliglån, men dette framstår oftest som opportunistisk kriminalitet som sjelden er grundig planlagt. Samtidig er det sannsynlig at enkelte aktører gjennomfører slike bedragerier i et mer organisert omfang, gjerne ved bruk av utro tjenere på innsiden av finansinstitusjonene. Dette er også nevnt i denne rapportens avsnitt om organisert kriminalitet. Slike innsidere kan bistå med manipulasjon av søknadsprosessene eller gi tilgang til informasjon som uvedkommende ikke skal ha tilgang til. Selv om omfanget er begrenset har slike saker et høyere skadepotensiale enn den opportunistiske kriminaliteten. DNB har ikke informasjon som tilsier at omfanget av slike bedragerier vil øke i 2022.

PHISHING

DNBs Financial Cyber Crime Center registrerte i 2021 nesten 8400 bedragerisaker, en økning på 66 prosent sammenlignet med året før. Den største økningen er tilknyttet phishingsaker. Her ble det registrert i overkant av 3100 ofre, som utgjør en økning på 568 prosent og indikerer en kraftig økning av phishing mot bankens kunder. I sin enkleste form gjennomføres phishing ved at kriminelle aktører sender ut store mengder falske e-poster eller SMS-meldinger og utgir seg for å være en legitim aktør. Her ber de offeret om å trykke på en lenke og oppgi sensitiv informasjon. Dette blir deretter misbrukt for den kriminelles egen vinning.

Den digitale utviklingen i samfunnet gjenspeiles i de digitale tjenestene som misbrukes, samtidig som enkeltmenneskers tillit til viktige samfunnsinstitusjoner utfordres. Mange av phishingforsøkene framstår svært profesjonelle med god norsk og mer troverdig innhold enn tidligere. På grunn av dette blir det stadig mer krevende for ofrene å fange opp at de faktisk har blitt utsatt for phishing. Dette gjør det også sannsynlig at vi vil se nye og kreative phishingangrep i 2022 der de kriminelle benytter dagsaktuell informasjon for å lure nye ofre.

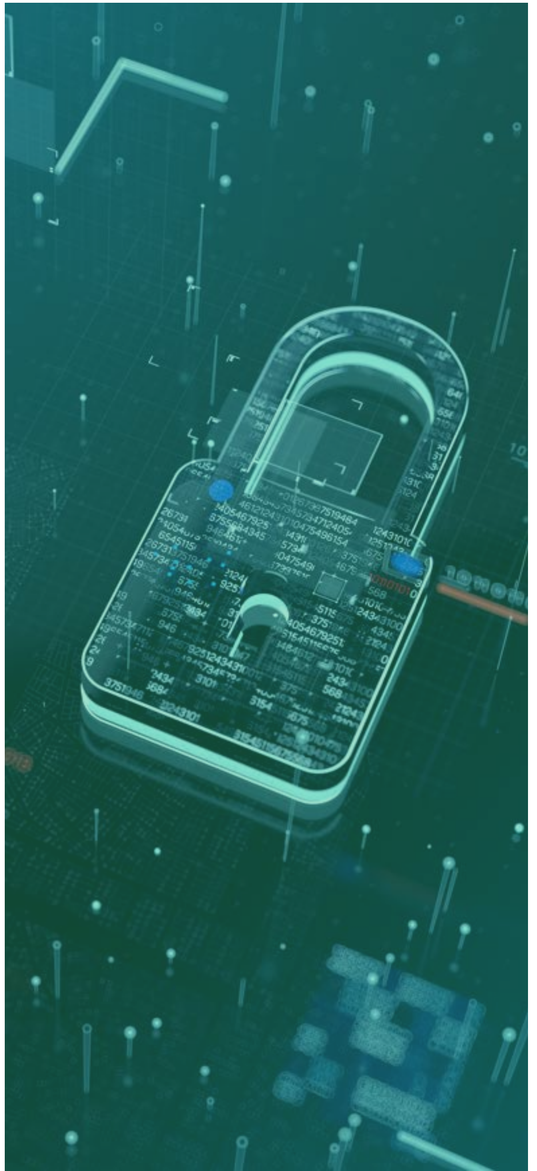
Vi ser at kriminelle aktører benytter krigen i Ukraina som tema i phishing i 2022

Utviklingen av phishing som fenomen er også belyst i fagartikkelen om phishing i denne rapporten.

Enkelte aktører benytter seg av skadevare i sine phishingangrep. Selv om det i 2021 var et begrenset omfang av vellykkede angrep, viser tall fra norske teleoperatører at det gjennom året ble stoppet svært mange SMS-meldinger med potensielt skadelig innhold. DNB er kjent med at det finnes skadevare for mobiltelefoner med et høyt skadepotensial mot norske finansinstitusjoner, men trusselen har over tid vært begrenset.

Enkelte aktører nærmer seg likevel, og det er sannsynlig at trusselen er økende. Det er derfor viktig å følge med på utviklingen av slik skadevare gjennom 2022.

Trusselen fra avanserte phishingaktører mot norske finansinstitusjoner og privatpersoner er høy. Det er sannsynlig at aktørene vil fortsette å utvikle seg gjennom 2022 og at de vil bruke stadig mer avanserte teknikker. Samtidig er det meget sannsynlig at de enkleste phishingangrepene med masseutsendelse av primitive meldinger også vil fortsette. Selv om de fleste forsøkene mislykkes, gjør det store omfanget av slike meldinger at denne type phishingangrep er svært lønnsom for aktørene.



FORSIKRINGSBEDRAGERIER

DNB Livsforsikrings (DNB Liv) portefølje har endret seg betydelig ved at personrisikoproduktene er solgt til Fremtind forsikring. Det totale svindelvolumet mot selskapet er derfor betydelig redusert ettersom en stor del av den avdekkede forsikringssvindelen tidligere var knyttet til disse produktene. Innen yrkesskadeforsikring økte imidlertid bedrageriene med 42 prosent sammenlignet med året før. Økningen skyldes sannsynligvis økt fokus i organisasjonen, men også økt salg av slike produkter.

Forsikringssvindel innen uføredekningene på bedriftsavtalene hadde et jevnt og stabilt volum i 2021. Forsikringssvindlerne benytter seg i all hovedsak av tradisjonelle metoder som å simulere sykdom, dikte opp skadehendelser, overdrive skadehendelser og lignende. Det er ikke avdekket sofistikerte angrep eller at organiserte kriminelle har utnyttet DNB Livs produkter til svindel.

SVINDEL INNEN UFØREFORSIKRINGER

Undersøkelser i Brønnøysundregisteret har en rekke ganger avslørt at kunder som hevder de er 100 prosent arbeid suføre, og krever uføreerstatning, i virkeligheten eier og/eller driver selskaper med en så stor aktivitet at det er uforenlig med uføregraden. Innhenting av selskapenes regnskaper og søk i åpne kilder har ofte gitt ytterligere beviser på dette. I en rekke tilfeller har kunden selv publisert informasjon på egne profiler i sosiale medier som indikerer en helt annen arbeidsevne enn oppgitt til helsevesenet og DNB Liv.

En metode avdekket i 2021 er at enkelte eiere og ansatte i mindre bedrifter med uføredekninger i bedriftsavtalene har oppgitt for høye lønninger ved tegning av avtalen. Det er sannsynlig at dette har blitt gjort for å kunne kreve en for høy uføreerstatning ved en fremtidig uførhet.

SVINDEL INNEN YRKESSKADE-FORSIKRINGER

DNB Liv har i 2021 avdekket flere svindel-forsøk innen yrkesskadeforsikring, og det er i hovedsak tre kjente metoder svindlerne har benyttet seg av:

- Kunden dikter opp et hendelsesforløp om en yrkesskade eller kunden dikter opp hvordan reelle helseplager har oppstått.
- Kunden overdriver en reell hendelse ved å gi en annen og betydelig mer alvorlig hendelsesbeskrivelse til DNB Liv enn hva som i virkeligheten har skjedd.
- Kunden endrer på hendelsesforløpet i sin forklaring til selskapet for å forsøke å unngå en avkortning i erstatningen for utvist grov uaktsomhet.

MISBRUK INNEN ARBEIDSLIVS-KRIMINALITET

DNB Liv registrerte i 2021 flere saker der norske selskaper tilsynelatende bevisst inngikk lovpålagte pensjons-avtaler uten å betale for disse.

Ved å unnlate å betale for slike avtaler kan selskapene få en økonomisk fordel overfor lovlydige selskaper i anbuds-prosesser.

Samtidig mister ansatte i disse selskapene sin rett til pensjonsopptjening og blir dermed bedratt av egen arbeidsgiver. Vi har i hovedsak registrert slike saker i tilknytning til mindre selskaper med dårlig økonomi innen bygg- og anleggsbransjen og i restaurantbransjen.

UTSIKTER MOT 2023

Bedrageritrusselen mot DNB Liv vil fortsatt være høy i 2022. Til tross for at forsikringsbransjen i Norge har avdekket noen færre forsøk på forsikrings-svindel i 2021 enn året før, er det ingen indikasjoner på en generell nedgang i den totale bedrageritrusselen mot DNB Liv.

Det vurderes som meget sannsynlig at «vanlige kunder» vil stå bak de fleste forsøkene på forsikringssvindel mot DNB Liv i 2022. Videre er det meget sannsynlig at DNB Liv vil utsettes for svindelforsøk ved at antatt useriøse og kriminelle selskaper forsøker å etablere lovpålagte pensjons- og yrkesskade-forsikringsavtaler uten innbetaling. Vi forventer at forsterket fokus på dette vil bidra til å avdekke flere slike saker i 2022. Det vurderes som lite sannsynlig at selskapet vil rammes av forsikringssvindel fra organiserte kriminelle miljøer.

Bedrageri – en økende trussel mot våre kunder

INVESTERINGSBEDRAGERI OG KJÆRLIGHETSBEDRAGERI

DNBs Financial Cyber Crime Center registrerte en økning i investeringsbedrageri og kjærlighetsbedrageri gjennom 2021, men med samme type handlingsmønster, modus og teknikker som tidligere. Fellesnevneren er sårbarhet, og som et utgangspunkt kan hvem som helst bli utsatt for slike bedragerier. Som følge av Covid-19 pandemien har mange mennesker havnet i sårbare situasjoner. Noen har følt på ensomhet, andre har opplevd kraftige innskrenkninger i privatøkonomien. Dette er faktorer som blir brukt for å lure ofre for både kjærlighetsbedrageri og investeringsbedrageri.

Så lenge pandemien pågår er det sannsynlig at de kriminelle vil fortsette å bruke den for å legitimere bedrageriene. Samtidig er det sannsynlig at aktørene vil omstille seg og utnytte den usikkerheten som oppstår når neste verdensomspennende hendelse oppstår. Den pågående Ukraina-konflikten med medfølgende geopolitisk ustabilitet og uro i finansmarkedene er eksempler på hendelser som kan gi uforutsigbarhet og ukritisk søken etter nye løsninger for mange mennesker. DNB har hittil i 2022 observert flere saker hvor Ukraina-konflikten har blitt misbrukt som ledd i sosial manipulering av ofre, og det er meget sannsynlig at det vil fortsette gjennom året.

Interessen for kryptovaluta samsvarer ofte med medieomtale og markedets svingninger. Et økende antall organisasjoner og myndigheter bidrar på globalt nivå til en aksept for kryptovaluta som betalingsmiddel og investeringsinstrument. Samtidig har mange begrenset kunnskap om kryptovaluta. Dette gjør det sannsynlig at investeringsbedrageri med kryptovaluta vil øke gjennom 2022. DNB har i økende grad observert saker med sammenblanding av kjærlighetsbedrageri og investeringsbedrageri. I tillegg til at ofre for kjærlighetsbedrageri blir brukt som muldyr i investeringsbedragerisaker, er det observert flere tilfeller av kjærlighetsbedrageri som har utviklet seg til investeringsbedrageri. Her kommer ofrene i kontakt med falske profiler gjennom datingtjenester og samtalene flyttes raskt over til alternative kommunikasjonsplattformer som WhatsApp. Etter at offeret har fått tillit til den falske profilen, blir samtalen styrt mot kryptovaluta og offeret blir gradvis lurt til å overføre penger til falske investeringsplattformer- og rådgivere. Selv om ofre for kjærlighetsbedrageri tradisjonelt har vært eldre, er det en tendens til at sistnevnte modus også retter seg mot yngre ofre.

Muldyr er personer som stiller sin konto til disposisjon for hvitvasking av midler fra straffbare forhold.

Sammenblandingen av bedrageriformer kommer til dels av at det er de samme aktørene som står bak flere av bedrageriformene, men også aktørenes sterke behov for å hvitvaske utbytte fra straffbare handlinger. Ofre som har blitt manipulert som følge av bedragerier kan enkelt brukes som muldyr i stedet for å rekruttere nye personer til hvitvasking alene. Samtidig bidrar slike sammenblandinger til en viss kamuflering av de grupperingene som står bak kriminaliteten, men med svak effekt fordi det finnes effektive metoder for å spore hvitvaskede midler.

Det er sannsynlig at det økende omfanget av både kjærlighetsbedrageri og investeringsbedrageri vil fortsette gjennom 2022. Det er også sannsynlig at flere yngre personer enn tidligere vil bli utsatt for bedrageritilfeller der kjærlighetsbedrageri og investeringsbedrageri sammenblandes.

LØSEPENGEVIRUS

Som nevnt tidligere i rapporten er det åpenbart at løsepengevirus har et stort skadepotensial for norske bedrifter. Ved slike angrep krever aktørene som oftest betaling gjennom kryptovaluta, men fordi aktøren har tilgang til bedriftens datasystem er det imidlertid også mulig at informasjon om bedriftens betalingsløsninger og bankforbindelser kan misbrukes. I noen tilfeller kan de kriminelle gå inn i kundens nettbank og tappe denne for penger, i mer sofistikerte tilfeller forsøker de å gå under radaren ved å endre små detaljer ved betalingsinformasjonen slik at bedriftene ikke selv oppdager at noe er galt ved tilsynelatende legitime betalinger.

Det er meget sannsynlig at norske bedrifter vil fortsette å bli utsatt for løsepengevirus gjennom 2022 og at trusselen er økende sammenlignet med tidligere år. Samtidig er det ikke automatikk i at disse angrepene vil misbruke bedriftenes bankforbindelser direkte. Det er likevel sannsynlig at de kriminelle vil benytte enhver mulighet til vinning, og dermed må banker være forberedt på at bedrifters kundeforhold kan bli misbrukt i forbindelse med løsepengevirus.

Spoofing av e-post innebærer at en kriminell aktør forfalsker avsenderadressen slik at det ser ut som om en reell person har sendt e-posten selv om det er den kriminelle som har gjort det.

LEVERANSEKJEDEANGREP MØTER BEDRAGERI

Ved tilgang til kompromitterte datasystemer finnes det også mulighet til å misbruke informasjon som ledd i Business Email Compromise (BEC) rettet mot andre bedrifter. Her utnyttes sårbarheter ved eksisterende leverandørkjeder mellom bedrifter på en slik måte at trusselaktørene enklere kan manipulere ofrene sine. Det er meget sannsynlig at bedrifter vil bli utsatt for BEC gjennom 2022, men også at omfanget kan øke. Dagens trusselsituasjon og digitale sårbarheter gjør at bedrifter i større grad bør sette søkelys på sårbarheter ved leveransekjedene i næringslivet slik at mistenkeligheter som følge av kriminelle aktørers illegitime tilgang til systemer blir fanget opp så raskt som mulig. Selv om trusselen med avanserte angrep er høy, er det fortsatt primitive og tradisjonelle bedragerier mot bedrifter som dominerer.

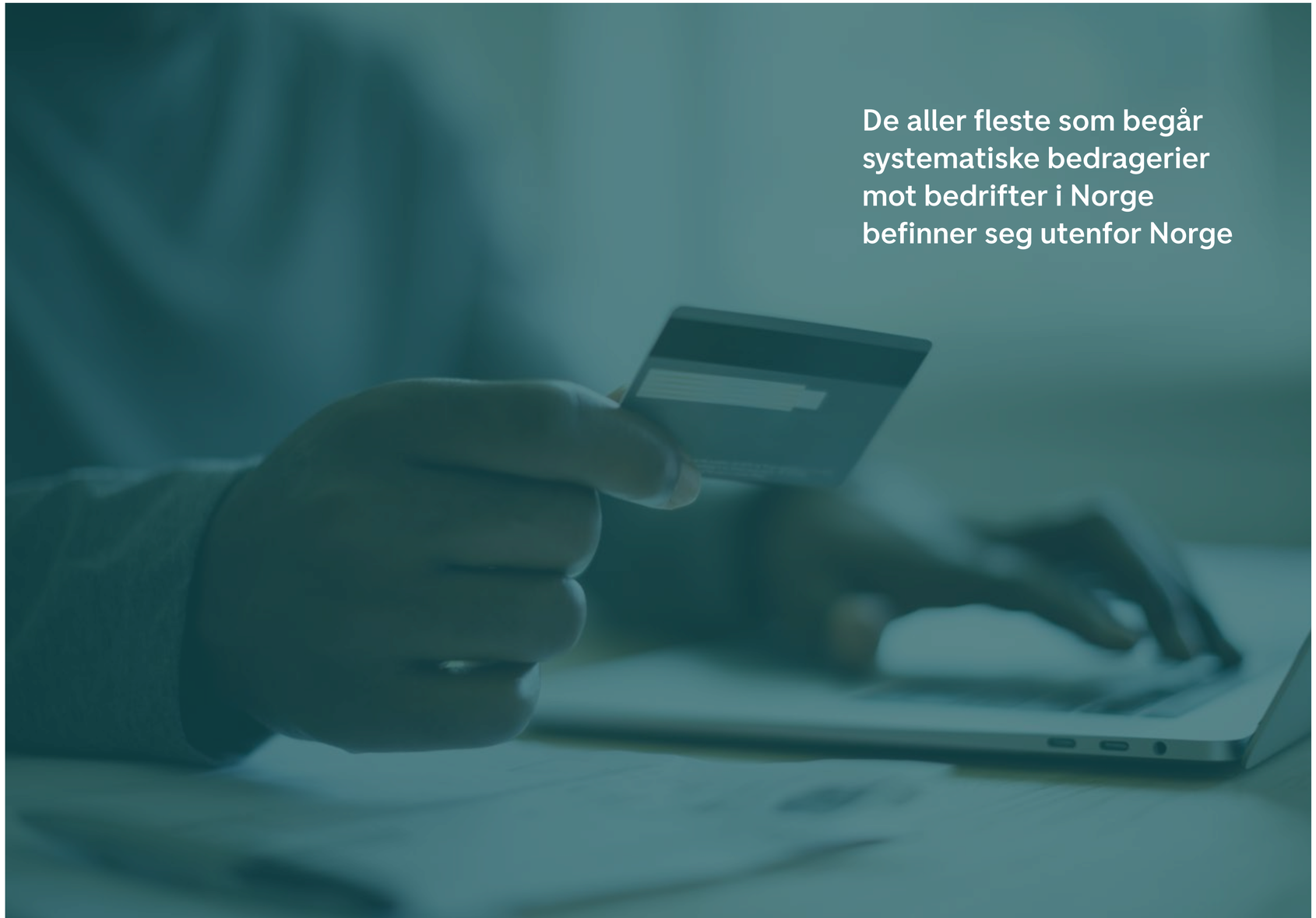
Gjennom 2021 registrerte DNB svært mange forsøk på fakturabedrageri og direktørsvindel uten kompromittering av datasystemer. I slike tilfeller spiller bedragerne på eksisterende tillitsforhold mellom bedrifter eller kolleger, og utgir seg for å være noen de ikke er. Et vanlig eksempel er at de spoofer (forfalsker) e-postadresser og sender falske fakturaer til offeret. Disse bedrageriene bærer ofte preg av enklere språk, moderate beløp og er gjerne masseprodusert. Det er meget sannsynlig at norske bedrifter vil bli utsatt for denne typen bedragerier gjennom 2022.

I direktørsvindel sender kriminelle aktører tilsynelatende ekte e-poster til ansatte i bedrifter. E-postene ser ut til å komme fra en leder i bedriften og inneholder gjerne en betalingsoppfordring som haster. I realiteten er dette falske e-poster der betalingsinformasjonen tilhører den kriminelle.

Business Email Compromise (BEC) innebærer at en kriminell aktør overtar e-postkorrespondansen mellom to bedrifter fordi én av dem har fått sine datasystemer kompromittert.
Her blir betalingsdetaljer i fakturaer endret slik at betalinger blir sendt til kriminelle i stedet for den rette mottakeren.

De aller fleste som begår systematiske bedragerier mot bedrifter i Norge befinner seg utenfor Norge. Likevel er det noen få aktører bak faktura-bedragerier som holder til innenfor våre landegrenser. For disse aktørene er det primært abonnementstjenester med uklare vilkår og villedende markeds-føring som ligger til grunn, og det er ikke alltid lett for offeret å forstå at de har blitt bedratt.

En vanlig framgangsmåte er å sende det som tilsynelatende er en faktura for programvare, rådgivningstjenester eller lovpålagte kontroller, men som i realiteten er et lite gunstig tilbud forkledd som en faktura. Selv om slike aktører med ujevne mellomrom blir fanget opp av myndighetene og virksomhetene blir avviklet, er det meget sannsynlig at slike bedragerier vil fortsette også i 2022.



Innsidetrussel mot DNB

Som Norges største bank forvalter DNB store verdier, både i form av finansielle midler, kompetanse og informasjon. I en undersøkelse gjennomført av Næringslivets sikkerhetsråd oppgir 8 prosent av respondentene at deres virksomhet har blitt utsatt for innsidehendelser de siste to årene. Studier viser at finansnæringen er blant de mest utsatte sektorene.

Innsidetrusselen kan treffe en virksomhet på mange ulike måter. På den ene siden står «ubevisste innsidere», som uten intensjon begår handlinger som skader virksomheten de arbeider for. På den andre står «bevisste innsidere» som med viten og vilje begår handlinger som forårsaker skade eller tap. Denne vurderingen tar for seg trusselen fra tilsiktede handlinger som kan ramme DNB – fra innsiden.

ANSATTE SOM TRUSSELAKTØRER

De fleste bevisste innsidere er selvmotiverte, og begår innsidehandlinger for egen økonomisk vinning. Innsidehandlinger kan også være motivert av ideologi, tvang, egoisme eller hevn. Faktorene som påvirker en ansatts motivasjon til å begå en innsidehandling er ikke nødvendigvis statiske, men kan oppstå på ulike tidspunkt og faser i et ansettelsesforhold.

I DNB deles tilsiktede innsidehendelser inn etter hvilke verdier disse rammer. Sikkerhetsbrudd som begås av ansatte favnes av konfidensialitetsbrudd, forsøk på å tilegne seg økonomiske midler, forsøk på å påvirke funksjonalitet i DNBs systemer, handlinger som påvirker ansattes liv og helse og handlinger som påfører tap eller skade på materiell eiendom.

Innsidehendelsene vi kjenner til i DNB har hatt begrensede konsekvenser for konsernet. Gode prosesser for å oppdage og håndtere disse sakene bidrar til å begrense skadeomfanget.

Vi må imidlertid ta høyde for at det kan finnes hendelser som ikke er oppdaget.

TRUSSELAKTØRER FRA UTSIDEN

Eksterne trusselaktører har både intensjon om og kapasitet til å rekruttere og påvirke ansatte i ulike virksomheter til å begå innsidehandlinger. Flere trusselaktører arbeider aktivt for å utnytte den individuelle sårbarheten til ansatte ved attraktive mål. Dette gjelder både statlige aktører, og organiserte kriminelle.
I et globalt perspektiv er det relativt sett få kjente innsidehendelser som involverer eksterne aktører. Vi vet imidlertid at innsidehendelser som involverer eksterne aktører kan få betydelige konsekvenser, både i form av finansielle tap og tap av omdømme.

INNSIDETRUSSEL

En innsider er en nåværende eller tidligere ansatt, konsulent eller tredjepart som har eller har hatt autorisert tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap.

ORGANISERT KRIMINALITET

I sin rapport «Profesjonelle aktører» fra 2021 skriver Økokrim at «tilgang eller evne til å påvirke profesjonelle aktører er ofte en forutsetning for at enkelte typer kriminalitet lykkes og ikke avdekkes av politi og kontrolletater.» Det er bred enighet om at det er lukrativt for kriminelle miljøer å ha tilgang på innsidere i finansnæringen, og politiet har i flere år advart mot at organiserte kriminelle jobber aktivt for å infiltrere norsk næringsliv.

Økokrim peker på at særlig tilrettelegging for innvilgelse av lån på uriktig grunnlag er et utbredt problem innen bank og finansnæringen. Flere bankansatte i Norge som er omtalt hos politiet med slike saker knyttes til kjente kriminelle aktører. I Sverige har politiet fremhevet bankansattes rolle som «sentrale muliggjørere» i hvitvasking. Gjennom informasjon fra den krypterte kommunikasjonsplattformen Encrochat avslørte svensk politi i 2021 at bankansatte har bistått kriminelle i organiserte former. Et annet eksempel fra Storbritannia omhandler en ansatt i anti-bedrageri-enheten til et stort finanskonsern som solgte kunders kortdetaljer til kriminelle for så å rapportere inn transaksjoner der de kriminelle benyttet informasjonen til å kjøpe luksusvarer i etterkant.

Det er grunn til å tro at kriminelle grupper kan forsøke å rekruttere innsidere i DNB. DNB vil ikke bare utgjøre en potensiell ressurs for kriminelle grupper med henblikk på hvitvasking og bedrageri. Tilgang til DNBs IT-infrastruktur er også et potensielt mål for flere cyberkriminelle aktører, både for å gjennomføre et angrep eller for å hente ut informasjon som kan understøtte kriminell virksomhet. I internasjonal kontekst finnes det eksempler på at cyberkriminelle har henvendt seg direkte til ansatte i store virksomheter via e-post for å rekruttere disse til å plante skadevare eller skaffe nettverkstilgang med henblikk på utføre angrep med krypteringsvirus. I et annet tilfelle fra USA benyttet organiserte kriminelle sosial manipulering og en langvarig kultiveringsprosess med fysiske møter for å overtale en ansatt til å installere skadevare hos sin arbeidsgiver Tesla.

SOSIAL MANIPULERING

En metode som benyttes for urettmessig å skaffe seg tilgang til verdier gjennom å påvirke mennesker med tilgang til verdiene. For å overbevise og oppnå tilgang til verdier kan en trusselaktør samle informasjon som blir brukt for å lage en skreddersydd situasjon hvor det spilles på tillit, frykt og fristelser.

STATLIGE AKTØRER

I sin åpne trusselvurdering for 2022 skriver PST at utenlandske etterretningstjenester også dette året forventes å legge betydelige ressurser i å rekruttere kilder i norske virksomheter. Særlig russiske etterretningstjenester prioriterer dette, og det er ikke bare personer med tilgang til sikkerhetsgradert informasjon som kan være av interesse.

Statlige etterretningstjenester kan ha en strategisk interesse av informasjon DNB besitter eller utgjør inngangsporten til. DNB ivaretar viktige samfunnsfunksjoner, og gjennom vår virksomhet forvalter DNB informasjon om sektorer som har høy prioritet for fremmede staters etterretningstjenester. Ved siden av interessefeltene utenriks-, forsvars- og sikkerhetspolitikk er også forsvarsindustri, helse, maritim teknologi og petroleumssektoren prioriterte områder.

DNB besitter også store mengder person-informasjon om personer med ulike rolle i norsk offentlighet og næringsliv.

TRUSSELAKTØRENES VERKTØYKASSE

Sosial manipulering er et sentralt verktøy for aktører som søker å rekruttere innsidere. Ansatte i DNB utsettes for ulike former for dette, særlig gjennom sosiale medier, via telefon (vishing) og på e-post (phishing). Både kriminelle grupperinger og statlige etterretnings-tjenester benytter slik metodikk, og har en betydelig kapasitet. Individuelle sårbarheter kartlegges og blir forsøkt utnyttet for å lykkes med å overtale eller presse noen til å agere som innsidere. Både frykt og fristelser tas i bruk for å skaffe seg «noen på innsiden».

Det er kjent at flere lands etterretnings-tjenester utøver press overfor borgere bosatt i andre land. Dette kan handle om at borgere av autoritære stater presses til samarbeid eller til å utlevere informa-sjon gjennom press mot slektninger og familie som fortsatt bor i opprinnelses-landet. De innrapporterte tilfellene av forsøk på sosial manipulering indikerer at DNB er et attraktivt mål for ulike trusselaktører.

Det er imidlertid grunn til å anta at det finnes mørketall. Det er ofte vanskelig å avdekke hvem som faktisk står bak, ettersom trusselaktørene oftest utgir seg for å representere legitime aktører.

UTSIKTER MOT 2023

DNB er Norges største finanskonsern og har flere tusen ansatte. Det er sannsynlig at det finnes enkeltansatte som vil kunne begå selvmotiverte innsidehandlinger. Videre er det sannsynlig at ansatte vil kunne utsettes for forsøk på rekruttering fra kriminelle grupperinger eller utenlandske etterretningstjenester. DNB vil kunne rammes av innsidehendelser av ulik alvorlighetsgrad.

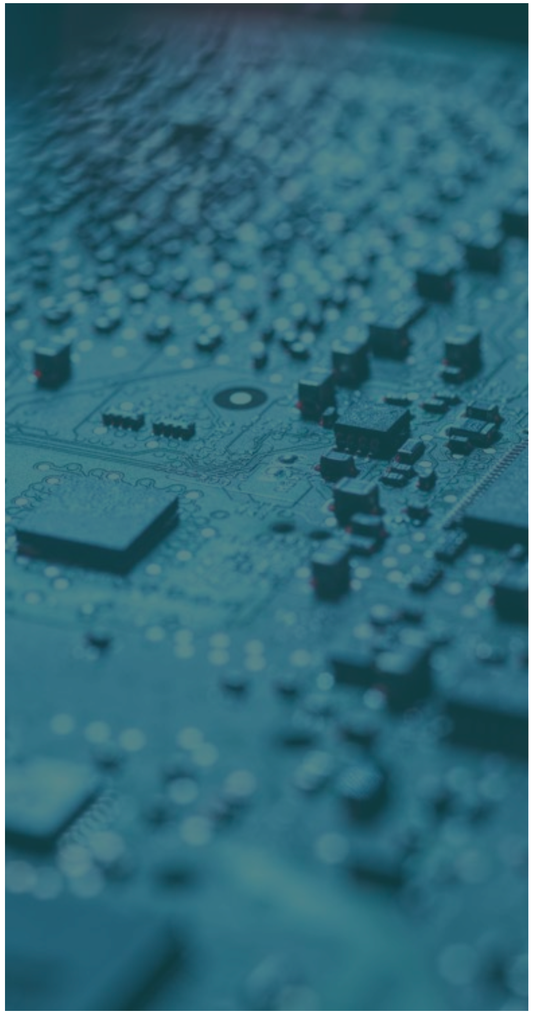
Tema

Storpolitikk i det digitale rom

I takt med den globale digitaliseringen har også internasjonal politikk beveget seg lengre inn i cyberdomenet. Cyberangrep blir stadig oftere benyttet som en form for moderne diplomati eller hybrid krigføring, og de siste årene har også private bedrifter blitt trukket inn og rammet av cyberangrep som en følge av dette.

I februar advarte amerikanske og britiske myndigheter privat sektor om mulig kommende cyberangrep som følge av den diplomatiske krisen mellom Russland og NATO over Ukraina, og disse advarslene har i noen tilfeller manifestert seg etter at Russland invaderte Ukraina 24. februar. Direkte cyberangrep som ledd i krigen har først og fremst rammet de direkte involverte partene (Russland, Ukraina og Hviterussland). Slike angrep kan ramme bedrifter direkte, eller som en utilsiktet konsekvens av cyberangrep som sprer seg utenfor angriperens kontroll. Dette har man eksempelvis sett i Latvia og Litauen som ledd i konflikten. Man kan anta at cyber-spionasjeoperasjoner forekommer i større grad, men slike angrep er også langt vanskeligere å oppdage. Når statsaktører opererer i det digitale rom kalles de «Advanced Persistent Threats» (APT), som refererer til en angriper som har en stor evne til å utføre avanserte cyberangrep, ofte med en politisk agenda. Slike grupper er ofte statlig organiserte militære- eller sivile etterretningsenheter med cyber-kapabiliteter, men det kan også være snakk om grupperinger av organiserte kriminelle som får operere uten statlig inngripen.

Det er for eksempel flere russiske cyberkriminelle grupperinger som ved å konsekvent unngå mål i Russland i stor grad kan operere ut fra landet uten innblanding fra russiske myndigheter. I 2022 har man sett en utvikling der også cyberkriminelle grupper tar side i statlige konflikter, eksempelvis ved at gruppene Conti og Anonymous har valgt hver sin side i konflikten i Ukraina, og utfører cyber-angrep for å forsøke å støtte sin foretrukne part.



RUSSLAND

Russland er et av flere land som er kjent for å ha avanserte cyberkapabiliteter, og som benytter det digitale rom for etterretningsoppdrag og hybrid krigføring. NotPetya startet som et cyberangrep mot Ukrainas skattesystem i 2017. Bakteppet var en konflikt om territorier, samt manglende betalinger for energileveranser. Skadevaren hadde flere likhetstrekk med krypteringsviruset «Petya», en skadevare som hadde truffet mange bedrifter året før.

Det ble fort klart at «NotPetya» var annerledes. Viruset spredte seg i lynfart, og påvirket raskt bedrifter utenfor Ukrainas landegrenser. En sort tekstboks med løsepengekrav dukket opp på dataskjermene, men det fantes i realiteten ingen krypteringsnøkkel som kunne låse opp filene igjen. Der krypteringsviruset Petya ble benyttet for økonomisk vinning, var NotPetya utelukkende destruktivt – det låste filene og kastet nøkkelen. I dag blir NotPetya (også kjent som NyetPetya) attribuert til russisk-statssponset aktivitet, og anses som et ledd i cyberkrigføring mot Ukraina. Globalisering har medført økt grad av kontakt og avhengigheter mellom virksomheter – også på maskinnivå.

Det amerikanske farmasiselskapet Merck tapte rundt 1.3 milliarder USD da NotPetya-angrepet spredte seg dit.

Estimater på totale globale kostnder som følge av angrepet er 10 milliarder USD. Merck forsøkte å kreve deler av tapet tilbake på forsikring. Forsikringsselskapet pekte imidlertid på unntaksklausuler for krigshandlinger, og argumenterte derfor med at cyberangrepet var en krigshandling utført av Russland mot Ukraina. Angrepet medførte også konsekvenser for russiske mål. Den ukontrollerte spredningen av skadevaren traff blant annet et russisk oljeselskap.

USA

USA er et annet land som er kjent for sine cyberoperasjoner. En av de mest sofistikerte statlige cybergruppene er «Equation Group», som sannsynligvis opererer fra USAs National Security Agency (NSA). Trolig var det Equation Group og israelsk etterretning som stod bak Stuxnet, en svært destruktiv skadevare som i 2010 ble benyttet for å sabotere det topphemmelige iranske atomprogrammet. Angrepet fikk bred internasjonal oppmerksomhet da det ble kjent, og selve skadevaren spredte seg etter hvert verden over.

Under sitt presidentskap har Joe Biden ved flere anledninger omtalt cyberkrigføring i sine uttalelser. I juli 2021 ba han Vladimir Putin ta ansvar for avviklingen av cyber-kriminelle grupper som opererer ut av Russland, og i februar og mars 2022 gikk han ut og advarte mot statlige russiske cyberoperasjoner både i Ukraina, og mot vestlige land som gjengjeldelse for støtte av Ukraina.

IRAN

I etterkant av Stuxnet-angrepet mot Irans atomprogram, har Iran satset på å videreutvikle egne cyberkapabiliteter, både offensivt og defensivt. I etterkant av lanseringen av en islamskfiendtlig video fra en amerikansk pastor i 2012 utførte iranske hackere flere tjenestenektangrep mot flere amerikanske finansinstitusjoner, inkludert New York-børsen og Nasdaq, med den hensikt å skade finansindustrien. Angrepet var ideologisk motivert og rettet seg mot institusjoner og bedrifter som ble opplevd som representanter for USA, slik som Bank of America, AT&T og JPMorgan Chase.

I 2016 ble ni iranere med knytning til det iranske militæret anklaget for angrepet. I 2018 ble en annen gruppe iranere anklaget for å stjele data fra 144 amerikanske universiteter. Iran har videre blitt anklaget for å forsøke å forgifte Israels vannforsyning ved å hacke seg inn i infrastrukturen i 2020. Israel skal ha tatt igjen med et cyberangrep mot en større iransk havn, samt flere mål i Irans atomprogram.

NORD-KOREA

«Wannacry» var et svært omfattende og skadelig cyberangrep som påvirket hundretusenvis av maskiner verden over i 2017, og som berørte selskap i 150 land på tvers av industrier; fra sykehus, til banker til industriproduksjon. Angrepet var unikt i at det tilsynelatende traff alle, og i etterkant har man kommet frem til at det sannsynligvis ble utført av Nord-Korea som et rent destruktivt og demonstrativt angrep, muligens i et forsøk på å presse frem fremdrift i forhandlingene om atom- og missilprogrammene med USA.

I 2014 angrep det man mener er en nordkoreansk etterretningsoffiser Sony Pictures. Store mengder av selskapets data ble offentlig lekket, og angriperen(e) krevde at Sony skulle trekke tilbake filmen «The Interview», som er en komedie om et planlagt attentat mot Nord-Koreas leder Kim Jong-Un. I et angrep i 2016 stjal nordkoreanske hackere 81 millioner USD ved å kompromittere Bangladesh Banks systemer.

Ved et annet tilfelle i 2019 stjal en nordkoreansk etterretningsenhet 10 millioner USD fra Bank of Chiles minibanknettverk. Nordkoreanske hackere knyttes ofte til cyber-krigføring mot mål i Sør-Korea, samt angrep for økonomisk vinning til fordel for staten.

SKYLDFORDELING OG ØYE FOR ØYE?

Det kan være svært vanskelig å stadfeste hvem som står bak et cyberangrep. Angripere benytter flere avanserte teknikker for å skjule sine spor, og noen ganger planter de misvisende informasjon for å så tvil om attribusjon.

Det hender også at stater benytter kriminelle cybergrupper, enten direkte eller indirekte, til å utføre arbeid på deres vegne. Dette gir statlige aktører en viss grad av troverdig benektelse for angrep.

Det er derfor vanlig at man «med sannsynlighet» attribuerer et angrep til en stat, uten at vi kan fastslå dette. Dette vet også statlige aktører, som utnytter denne usikkerheten til å utføre etterretningsoppdrag med få konsekvenser. Utfordringer knyttet til dette medførte at 28 land (inkludert Norge) i 2019 signerte en «Joint Statement on Advancing Responsible State Behavior in Cyberspace». Landene sier med dette at de skal bygge tillit mellom land for å forhindre at cyberhendelser bidrar til konflikt, og at «dårlig oppførsel i det digitale rom» må få konsekvenser.

Krigen i Ukraina har illustrert hvordan vi er inne i en periode som er preget av rivalisering mellom stormakter.

Enkelte større land er villige til å gå langt i maktbruk overfor mindre stater, også innenfor cyber-domenet. Skillelinjen mellom miltære- og sivile, offentlige- og private mål hviskes ut når cyber angrep blir benyttet som ledd i hybrid krig føring. Stater må bli stadig mer sofistikerte i sine cyberkapabiliteter for både å mot-virke – og utføre – cyberangrep. Dette påvirker også privat sektor.

Selv om konflikt andre steder i verden kan føles langt unna når man sitter i Norge, har tidligere cyberangrep vist at vi kan rammes indirekte via samarbeids-partnere eller leverandørforhold. DNB er sentralt plassert i norsk finansiell infrastruktur, og må opprettholde en høy grad av beskyttelse, årvåkenhet og prioritet på cyberområdet for å unngå å bli fanget i kryssilden av storpolitikk.

Organisert kriminalitet i Sverige og Norge: Utfordringer for finansnæringen

I DNBs årlige trusselvurdering 2021 satte vi søkelyset på bruken av vold og trusler i bedragerisaker, som var en relativt ny trend i Norge. Flere av miljøene som bruker vold og trusler har sterke koblinger til miljøer i Sverige som er kjent for å utnytte sitt voldspotensiale. Her finnes koblinger både til organiserte kriminelle miljøer med mafialignende oppbygning og kriminelle MC-miljøer. I årets trusselvurdering ønsker vi å belyse likheter og forskjeller mellom Sverige og Norge, og hvilke implikasjoner dette har for trusselbildet mot finansnæringen.

Myndigheter i Norge og Sverige er samstemte i at kriminalitetsbildet preges av økende globalisering, digitalisering og teknologisk utvikling. Europol melder at organisert kriminalitet omsetter for minst 125 milliarder euro årlig innenfor EU. Om lag 85 prosent av de svarte pengene sluses gjennom bankene. Økt grensekryssende kriminalitet som involverer nettverk i flere land påvirker trusselbildet også i Norden.

Ved siden av stadig flere internasjonale kontaktflater viser svenske myndigheter til at organiserte kriminelle grupper i økende grad benytter legale strukturer for å skjule illegal virksomhet. Kriminelle tjenester utvikles og selges til andre kriminelle aktører, og kan i sin struktur minne om vanlige kommersielle forretningsmodeller.

BEDRAGERI

Innen bedrageriområdet finnes det åpenbare paralleller mellom kriminaliteten som begås i Norge og den som begås i Sverige. Flere sakskomplekser hvor man ser bruk av både digitale bedragerier og sosial manipulasjon kobles til miljøer som enten har en tilstedeværelse i, eller et tett samarbeid med, aktører i Sverige. Det er tydelig at disse koblingene brukes for å hvitvaske penger da vinningen fra bedragerier ofte brukes til kjøp av varer i Sverige. Vi ser også at modus som er utprøvd over tid i Sverige dukker opp med lokale aktører og det som trolig er bakmenn i utlandet. Utviklingen på phishing-området illustrerer godt hvordan nye metoder og trender ofte dukker opp i Sverige før de kommer til Norge. Her har vi grunn til å tro at vi står overfor både transnasjonale miljøer og miljøer som deler informasjon med andre på tvers av landegrenser. Bedragerier som retter seg mot bilfinansiering og usikrede kreditter er også et område hvor denne koblingen er spesielt tydelig. Flere store transnasjonale kriminelle miljøer er involvert i slike saker. Disse multikriminelle grupperingene gjennomfører ikke bare bedragerier, men er ofte involvert i mer klassisk organisert kriminalitet som narkotika- eller menneskesmugling. Flere av disse kompleksene kobles tilbake til Sverige på bakgrunn av at biler og penger blir fraktet over grensen, og ved at aktørene er kjent for å ha en sterk tilstedeværelse i Sverige.

Bedragerier vi ser i Norge er ofte påfallende like de som rapporteres fra Sverige, med bruk av falsk dokumentasjon, oppkjøp av legitime selskaper og bruk av stråmenn. Bruk av e-legitimering gir et mulighetsrom for å distansere seg fra kriminell aktivitet ved bruk av stråmenn og andres identiteter. Et stort antall konti og identiteter minsker også behovet for å benytte kontanter for å skjule transaksjoner. Samtidig øker det antall personer som kan være innblandet i kriminell aktivitet, og antallet transaksjoner de kriminelle kan utføre uten at dette innebærer en økt oppdagelsesrisiko.

VOLDSBRUK I ORGANISERTE KRIMINELLE MILJØER

Det er klare forskjeller mellom Sverige og Norge når det kommer til voldsbruken i de kriminelle miljøene. Sverige ligger helt i topp på listen over flest drap med bruk av skytevåpen i Europa. Dette er gjenstand for betydelig medieoppmerksomhet i Sverige, og representerer en åpenbar utfordring på samfunnsnivå. Bruken av skytevåpen synes imidlertid å være nært knyttet til gjengproblematikk og er i stor grad avgrenset til noen geografiske områder. I en slik sammenheng er det grunn til å anta at voldsbruk relatert til gjengkonflikter i liten grad påvirker den direkte trusselen mot finansnæringen. Like fullt er det en betydelig kapasitet og vilje til å benytte vold også blant de mer avanserte og etablerte organiserte kriminelle grupperingene i Sverige som i økende grad flytter sin virksomhet over i legale strukturer.

Svensk politi påpeker i rapporten «De organiserade bedragerierna» fra 2021 at økningen i den grove voldsbruken sammenfaller med en økning i bedragerisaker.

Det vurderes her som sannsynlig at den lukrative bedragerivirksomheten er en av flere faktorer som har påvirket voldsutviklingen. En mulig forklaring som trekkes frem er at nye aktører utenfor de tradisjonelle kriminelle miljøene er kommet til og har opparbeidet seg en høy status på kort tid. I Sverige utgjør utbyttet av bedragerivirksomhet om lag 2 milliarder svenske kroner i året, som tilsvarer det totale utbyttet av narkotikaomsetningen på gateplan.

Svært mange faktorer skal sammenfalle over lang tid for at en slik eskalering i voldsnivå skal finne sted. Det er ikke grunnlag for å si at Norge vil se en tilsvarende utvikling. Likevel ser vi en rekke indikatorer i det norske kriminalitetsbildet som ikke bør overses: Økt bruk av vold og trusler, også mot «sivile», flere nye aktører innen økonomisk kriminalitet som raskt tjener mye penger, store kjente organiserte miljøer som deltar på samme arena, og varsler fra Europol som tilsier at kriminelle miljøer øker sin tilstedeværelse og er mer villige til å bruke vold, blant annet for å utøve kontroll over egen virksomhet.

TRUSLER MOT ANSATTE

Som vurderingen Trusler og vold mot ansatte viser, utsettes flere av DNBs ansatte for trusler hvert år. DNB kjenner ikke til at personer med kobling til organiserte kriminelle grupper har stått bak trusler mot våre ansatte i Norge. Det har imidlertid vært eksempler på at samarbeidspartnere som forvalter DNBs produkter har blitt utsatt for press eller trusler.

Kriminelle grupper med «høy signatur», slik som kriminelle MC-klubber, kan gjennom sin skremselskapital påvirke uten å fremsette trusler. Subtile antydninger kan være tilstrekkelig for å påvirke beslutninger dersom en ansatt opplever å være i en utsatt posisjon.

De seneste årene har myndighetene i Sverige og Norge pålagt bankene et stadig større ansvar for å avdekke og motvirke økonomisk kriminalitet. Dette har i Sverige medført en endring i trusselbildet mot bankansatte. Tidligere var det ansatte i kundefront som ble utsatt for trusler, men nå utsettes også ansatte som jobber med klagesaker, hvitvasking og bedrageri i bankene for trusler. Også DNB-ansatte som arbeider med anti-hvitvasking og bedrageri har blitt utsatt for trusler. Vi har imidlertid ikke sett konkrete eksempler på at organiserte kriminelle har forsøkt å påvirke enkeltsaker.

INNSIDERE I FINANSNÆRINGEN – EN LUKRATIV RESSURS FOR ORGANISERTE KRIMINELLE

Finansnæringen er blant sektorene som er mest eksponerte for korrupsjon, infiltrasjon og utilbørlig påvirkning. Svenske og norske myndigheter har over lengre tid vært samstemte i sine advarsler om at organiserte kriminelle miljøer søker tilgang til innsidere i finansnæringen. For noen bedrageri- og hvitvaskingsmetoder er dette en forutsetning for å lykkes. Dette kan dreie seg om å kjøpe informasjon om bankenes produkter, tjenester og rutiner, eller at en medhjelper unnlater å innrapportere mistenkelige transaksjoner. Bankansatte som tilrettelegger for bedrageri og hvitvasking gjennom å gi lån på falskt grunnlag representerer en særlig utfordring.

Organiserte kriminelle miljøers evne og vilje til å utnytte finansnæringen for å begå økonomisk kriminalitet må tas på alvor. Stødig fokus på innsidetrusselen og robust samarbeid med politi og myndigheter er en forutsetning for å håndtere et stadig mer krevende trusselbilde.

Forsikringssvindel

Forsikringssvindel kan litt forenklet defineres som et straffbart bedrageri hvor en kunde gir bevisst uriktige opplysninger i den hensikt å få utbetalt en uberettiget erstatning fra et forsikringsselskap. Tradisjonelle eksempler på dette er kunden som senker sin egen ødelagte bil i sjøen for å få full erstatning, kunden som plusser på et ekstra kamera når kofferten ble stjålet for å tjene noen tusen kroner eller kunden som later som om han er syk når han i realiteten er frisk for å få utbetalt en stor uføreerstatning.

OMFANGET AV FORSIKRINGSSVINDEL

Hvert år svindles trolig norske forsikringsselskap for flere milliarder kroner til sammen. Det totale omfanget av forsikringssvindel er vanskelig å anslå da det antas å være store mørketall i tillegg til den svindelen som hvert år blir avdekket av selskapene. Det finnes ingen skikkelig forskning i Norge eller Norden for øvrig på omfanget av forsikringssvindel. Amerikansk forskning fra 2020 og overslag fra FBI viser at rundt 10 % av alle skadeerstatningskrav i USA er forsikringssvindel. I USA anslås den totale kostnaden til over 40 milliarder USD per år. Selv om forholdene i USA ikke direkte kan sammenlignes med Norge, gir tallene likevel en indikasjon. Dersom den samme svindelprosenten legges til grunn i Norge, tilsvarer dette et beløp på 4,3 milliarder kroner for det samlede omfanget av forsikringssvindel. Kostnaden ved feilaktige utbetalinger som følge av forsikringssvindel fører til at norske husholdninger og bedrifter hvert år betaler en høyere pris for sine forsikringsavtaler. Dette er et stort problem som forsikringsbransjen i Norge forsøker å motvirke blant annet gjennom aktiv svindelbekjempelse i selskapene, samarbeid selskapene imellom og med politiet.

BEKJEMPELSE AV FORSIKRINGSSVINDEL I NORGE

Ifølge Finans Norge avdekket og stanset norske forsikringsselskap forsikringssvindel for 392 millioner kroner i 2021, hvor 79 % av tilfellene ble avdekket innen privat skadeforsikring, 6 % innen skadeforsikring næring og 15 % for syke- og uføreprodukter. Ettersom syke- og uføreproduktene har høyere gjennomsnittlig verdi per sak, utgjorde disse sakene hele 218 millioner kroner i avdekket forsikringssvindel.

Hvert år svindles trolig norske forsikringsselskap for flere milliarder kroner til sammen

De fleste forsikringsselskapene i Norge har ansatt egne utredere som etterforsker saker hvor det mistenkes forsikringssvindel. Disse utrederne er i all hovedsak rekruttert fra politiet og har god kompetanse innen etterforskning av straffbare forhold.

De største forsikringsselskapene i Norge, har flere titalls utredere, jurister og analytikere ansatt for å bekjempe svindel.

I Finans Norges bransjenorm om utredning av forsikringssvindel har forsikringsbransjen nedfelt at avdekket forsikringssvindel som hovedregel skal politianmeldes. Forsikringsselskapene har et samfunnsansvar for å avdekke økonomisk kriminalitet mot bransjen for å forsøke å begrense kundenes økte kostnader som en konsekvens av svindel. Forsikringssvindel er omhandlet i Straffelovens § 375 og § 376 og straffes med bøter eller fengsel i inntil 6 år og ubetinget fengselsstraff er en vanlig straffeutmåling selv ved forholdsvis beskjedne svindelbeløp.

HVEM ER FORSIKRINGSSVINDLEREN?

Økokrim skriver i sin temarapport om bedrageri i 2021 at det i Norge er større sosial aksept blant unge for forsikringsbedrageri enn for annen type kriminalitet og at den yngre delen av befolkningen er mer tilbøyelig til å gjennomføre forsikringsbedrageri enn de som er eldre. Likevel viser resultatene fra Gjensidiges årlige svindelundersøkelse at de unge ikke drar med seg disse holdningene etter hvert som de blir eldre, og selskapene har derfor liten grunn til å frykte en fremtidig økning som følge av en holdningsendring.

Både politiet og forsikringsselskapene erfarer at kriminaliteten de siste årene har blitt mer komplisert og organisert. Også forsikringsnæringen rammes av kriminelle gjenger og andre tilsynelatende organiserte miljøer, men den gjennomsnittlige svindleren som blir avslørt i Norge er likevel «vanlige folk» som ikke er kjente kriminelle eller del av noe organisert miljø. Det kan se ut til at den typiske forsikringssvindleren i Norge er en kunde som griper en tilgjengelig mulighet til å tjene litt ekstra penger, gjerne med «unnskyldningen» om at vedkommende har betalt forsikringspremie i årevis.

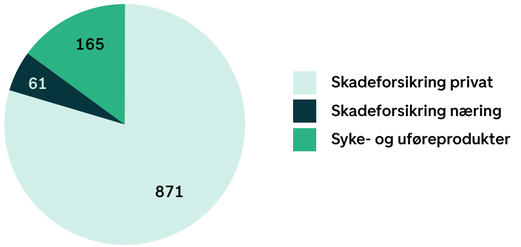
En kunde i DNB Liv ble i 2021 dømt i Hordaland tingrett til 1 år og 3 måneders ubetinget fengsel for å ha svindlet DNB Liv og NAV etter at han over flere år lot som om han var syk og 100 prosent arbeidsufør, samtidig som han jobbet fullt for en bedrift i Bergen. Utredere i DNB Liv samarbeidet med utredere i NAV og etterforskere i politiet for å avdekke og stanse svindelen.

DNBS FORSIKRINGSSELSKAPER

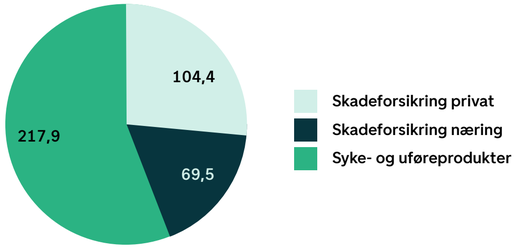
DNB er heleier av DNB Livsforsikring som i hovedsak behandler pensjonsavtaler, uføreforsikringer og personalforsikringer, herunder yrkesskadeforsikring. Selskapet er Norges nest største leverandør av personalforsikringer til norske bedrifter og blir jevnlig utsatt for forsøk på forsikringssvindel innen både yrkesskade og uførepensjon.

DNB Livsforsikring har ansatt flere utredere i tillegg til en jurist som har ansvaret for etterforskningen av forsikringssvindel. DNB Liv har i 2021 bidratt til å videreutvikle et dataprogram som ved hjelp av kunstig intelligens skal hjelpe til med å identifisere potensielle svindelsaker innen yrkesskadedekningene. Resultatene etter testingen er lovende og det antas at programmet vil bidra til å identifisere en rekke svindelsaker i 2022. DNB eier også 35 prosent av Fremtind forsikring som i tillegg til helseforsikringer tilbyr tradisjonelle tingskadeforsikringer som bil-, reise- og bygningsforsikringer. Fremtind har en større utrederavdeling med både utredere og jurister som avslører forsikringssvindel for rundt 75 millioner kroner hvert år.

Antall svindelsaker avdekket i Norge i 2021



Avdekket svindelbeløp i Norge i 2021 - i mill.kr



Phishing – preget av volum, målrettethet og nytenking

Phishing er blitt en så vanlig del av hverdagen at vi knapt reagerer når vi oppdager e-poster, telefoner og meldinger som forsøker å få oss til å dele informasjon vi ikke vil dele. Når det sendes flere milliarder falske e-poster hver dag, er det kanskje ikke så rart at vi blir litt blasert. Phishing er imidlertid ikke lenger hva det det var, og utviklingen innebærer at vi må revurdere både hvordan vi beskytter oss og hvilken trussel aktørene bak utgjør.

Historisk sett har phishing knyttet til økonomisk kriminalitet primært dreid seg om volum. Begrensningen har ligget i hvor mange phishingforsøk de kriminelle klarer å sende ut og deres kapasitet til å håndtere informasjonen de stjeler.

Dersom aktørene bruker for lang tid på å nyttiggjøre seg informasjonen blir bedrageriet oppdaget og informasjonen verdiløs. Likevel har dette ført til phishingkampanjer med et bredt nedslagsfelt i håp om å treffe ofre i et uoppmerksomt øyeblikk. Gjennom å velge tema for phishingkampanjer basert på de vanligste søkene i de store søkemotorene sikrer trusselaktørene seg at kampanjen treffer tema som er av interesse for mange. Teleoperatørene gjør en viktig forebyggende jobb ved å sile ut meldinger og oppringninger som med sannsynlighet kan være phishing eller en annen form for bedrageri. I 2021 stoppet Telenor 282 millioner svindelanrop globalt og på det meste ble det stoppet 1,3 millioner meldinger i døgnet.

Vi har blitt vant til å gjenkjenne og håndtere slike enkle kampanjer som baserer seg på stort volum og som treffer bredt. Ved å følge enkle råd, slik som å ikke trykke på lenker og være bevisste på at banken og politiet aldri vil etterspørre våre passord, har vi unngått å bli lurt. Men phishing er i endring.

VOLUM, ANGREPSSUM OG MÅLRETTETHET

Ved Covid-19 pandemiens start så vi et betydelig oppsving i phishingaktiviteten. Den pågående bølgen av økt aktivitet ble imidlertid først tydelig i løpet av sommeren 2021. DNBs Financial Cyber Crime Center opplevde en 568 prosent økning i antall personer som ble utsatt for phishing fra 2020 til 2021.

Det er flere grunner til dette. Ikke bare har antallet aktører økt med opptil 400 prosent sammenlignet med før pandemien, men de har også blitt mer avanserte. Ved å automatisere de innledende fasene av phishingkampanjer, for eksempel gjennom å automatisere enkle svar på meldinger, kan de kriminelle angripe flere ofre samtidig. Dette gjør det også mulig å identifisere hvilke mål den sosiale manipulasjonen bør rettes mot for å oppnå størst effekt.

En vesentlig endring kan knyttes til angrepssum. Der det tidligere var snakk om utbytte på noen tusenlapper er det nå snakk om flere hundre tusen eller millioner av kroner. Dette endrer konsekvensene av phishing drastisk. I et samfunnsperspektiv er det alvorlig at en kriminell handling som får så omfattende konsekvenser er så lett tilgjengelig, medfører lav risiko og ender med minimale konsekvenser for dem som blir tatt.

Den største endringen på dette området er imidlertid knyttet til målrettethet. Utover et fåtall enkeltsaker er målrettede phishingkampanjer eller spearphishing mindre vanlig innen økonomisk kriminalitet. Slike angrep rettes mot en enkeltperson eller en gruppe, men uavhengig av mål er de vanskeligere å unngå. Trusselaktørene gjennomfører nå flere slike målrettede angrep ettersom dette gir større sjanse for å lykkes enn brede kampanjer mot et stort antall mottakere. På gruppenivå kan disse angrepene rette seg mot en spesiell bransje eller en gruppe med felles språk. På individnivå handler det om å skreddersy meldingen til mottaker ved å bruke informasjon om interesser og aktiviteter som hentes fra åpne kilder.

Slik skreddersøm kan gjøre det potensielle offeret mindre kritisk, og øker sjansen for at angrepet lykkes. Noen trusselaktører overvåker offentlig tilgjengelig informasjon for å forberede spearphishing i målrettede angrep mot enkeltpersoner og grupper. Her er omfanget mindre, men skadepotensialet høyere.

DNB erfarte i 2021 at kriminelle aktører fulgte med på offentlig informasjon fra Brønnøysundregistrene som forberedelse til spearphishing. I slike saker fanget de opp offentlige bedriftsendringer, skaffet til veie kontaktinformasjonen til de involverte personene via åpne kilder og sendte målrettede SMS-meldinger til dem. Meldingene bar preg av å komme fra Brønnøysundregistrene og krevde signering med BankID, men var i realiteten del av et phishingangrep hvor kriminelle hadde som mål å tappe offerets bankkonto.

NYE KANALER GIR NYE MULIGHETER

I tillegg til kjente phishingkanaler, som masseutsendelse av SMS eller e-post, benytter flere aktører seg av kommunikasjonstjenester som Messenger og WhatsApp. Ved å bruke nye kanaler har aktørene i større grad lykkes med å bygge tillit hos ofrene.

Ved hjelp av søkemotoroptimalisering som er innebygd i de mest brukte søkemotorene, klarer kriminelle aktører å plassere falske nettsider øverst i søketreffene. Dette kalles SEO poisoning (Search engine optimalization poisoning). Selv om de falske nettsidene benytter seg av klassiske metoder for å hente sensitiv informasjon fra sine ofre, er det nytt at SEO poisoning benyttes i så stor grad for å gjennomføre målrettede angrep mot finansinstitusjoner og deres kunder i Norge.

Phishing via telefon, eller vishing, er også et betydelig samfunnsproblem som rammer mange. Ifølge Telenors rapport Digital Sikkerhet 2021 blokkerte selskapet nesten 20 millioner anrop fra utlandet første halvdel av 2021. De fleste aktørene befinner seg utenfor Norge, men disse knytter til seg lokale samarbeidspartnere som fyller rollen som kjentmann eller muldyr.

Det er meget sannsynlig at flere aktører benytter seg av personer med inngående kunnskap om norsk språk og kultur. Dette er spesielt synlig i vishing-saker der ofre blir oppringt og møtt av en person som snakker perfekt norsk.

Det er ikke lenger de forventede e-postene som preger phishingkampanjer. Trusselaktørene tar i økende grad i bruk kanaler hvor vi er mindre bevisste på muligheten for å bli bedratt. Økt automatisering, nytenking og manipulasjon fra trusselaktørene krever at vi endrer våre holdninger og øker bevisstheten rundt phishing.

Nulldagssårbarheter og reduksjon i «tid til utnyttelse»

Sårbarhetshåndtering er et komplisert og utfordrende fagfelt av flere grunner. En moderne bedrift har gjerne tusenvis av individuelle systemer, mange datamaskiner, og kompliserte nettverk. Det er derfor krevende å arbeide med identifisering og håndtering av sårbarheter. Ekstra utfordrende blir det når tiden det tar fra en sårbarhet oppdages til den blir brukt i cyberangrep blir stadig kortere.

En teknisk sårbarhet refererer vanligvis til en svakhet i IT-systemer som kan gi en angriper tilgang til et system eller et nettverk.

Når en sårbarhet oppdages, arbeider utviklere vanligvis raskt for å lansere en sikkerhetsoppdatering. Ideelt sett rekker alle brukere å installere denne sikkerhetsoppdateringen før angripere har anledning til å utnytte sårbarheten.

I realiteten går oppdatering ofte langsommere enn ønsket. Dette kan ha flere årsaker og vil variere mellom virksomheter. Dette kan skyldes avhengigheter til andre systemer som må løses før en sikkerhetsoppdatering kan gjennomføres, det kan være hensynet til operasjonell tilgjengelighet da patching noen ganger krever nedetid, det kan være risiko eller forringet funksjonalitet forbundet med oppdatering, utfordringer knyttet til mangelfull oversikt over IT-porteføljen, eller rett og slett underbemanning på personell som har kompetanse til å identifisere berørte systemer og utføre oppdateringene. Noen ganger velger en bedrift å ikke umiddelbart patche utsatte systemer dersom det finnes det andre sikkerhetsmekanismer som samlet sett reduserer risiko forbundet med sårbarheten.

Ekstra utfordrende blir det når sårbarheten vi skal håndtere er såkalte «nulldagssårbarheter». Med nulldagssårbarhet menes vanligvis en sårbarhet som ikke er kjent for leverandøren av det berørte produktet før det utnyttes i cyberangrep. «Null dag» refererer dermed til at det er null dager fra sårbarheten oppdages til den blir utnyttet av cyberkriminelle, og at tiden er svært knapp til å beskytte det utsatte systemet. Konseptet "nulldagssårbarhet» ble kjent etter «Stuxnet-angrepet» mot det iranske atomprogrammet i 2010. Stuxnet er en Windows-spesifikk dataorm som benyttes for å destabilisere industrielle systemer. Angrepet satte Irans atomprogram sterkt tilbake, og medførte nedsmelting av mange sentrifuger og fysisk ødeleggelse av om lag tusen maskiner.

Siden Stuxnet har antall sårbarheter som er såkalte «nulldagssårbarheter» vært økende, og i 2021 ble nulldagssårbarheter benyttet i rundt to tredeler av all skadevare. De siste årene har vi observert en kontinuerlig nedgang i målingen av «tid til utnyttelse», som vil si at tiden fra en sårbarhet blir kjent til den blir utnyttet av hackere går ned.

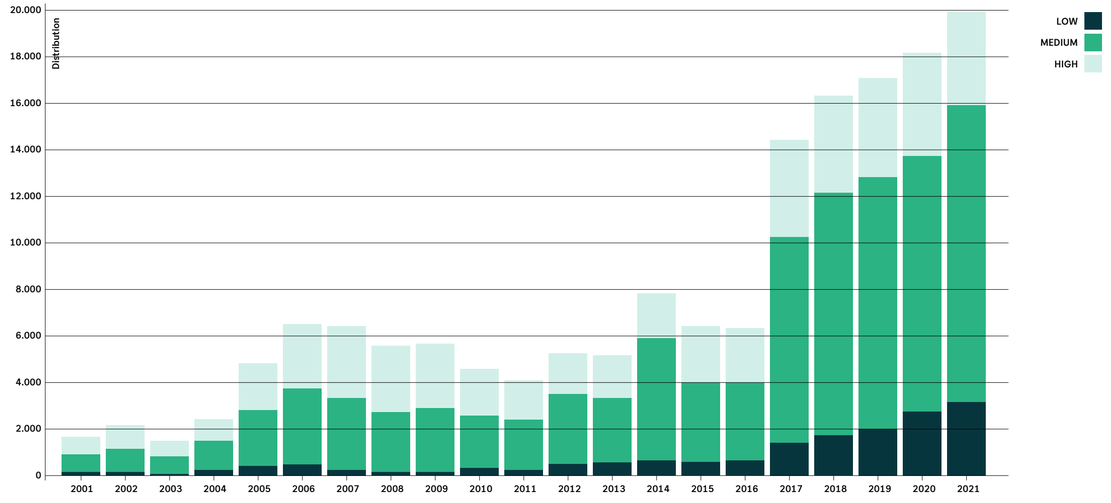
Da Microsoft publiserte en kritisk sårbarhet i programvare for e-post servere i mars 2021, tok det hackergruppen Hafnium fem minutter å begynne å skanne internett for sårbare maskiner.

I desember 2021 var det en liknende situasjon da en kritisk nulldagssårbarhet i javarammeverket (Log4J) ble offentliggjort av Apache. I en slik situasjon er det avgjørende at de riktige ressursene omdisponeres slik at sårbarhetshåndteringen kan utføres så raskt det lar seg gjøre.

En annen utfordring i sårbarhetshånd tering er at ikke alle sårbarheter kan utbedres gjennom en systemoppdatering. Noen ganger er sårbarheten så integrert med funksjonaliteten til systemet at dette ikke er mulig. I juli 2021informerte Windows om en sårbarhet i print-funksjonaliteten i alle Windows Printere som kunne medføre komplett kompromittering av bedrifter – gjennom printeren. Det ble raskt klart at det ikke fantes noen systemoppdatering som kunne rette sårbarheten, og at det heller ikke ville komme en slik oppdatering på kort sikt. I enkelte tilfeller må man simpelthen vurdere om hele tjenesten må tas ned for å redusere risiko, og flere selskaper valgte på dette tidspunktet å deaktivere printing helt.

I en bedrift som DNB er det essensielt at ansatte med ansvar for IT-systemer er klar over endringene vi har sett i risikobildet de siste årene. Antallet identifiserte sårbarheter i IT-systemer øker år for år. Tiden fra en sårbarhet blir kjent til den blir aktivt utnyttet, er stadig kortere. Der det tidligere var akseptabelt å installere sikkerhetsoppdateringer basert på sykliske rutiner (for eksempel en gang i måneden), er ikke dette alltid lenger godt nok. Grafen illustrerer antallet sårbarheter som har blitt kjent år for år siden 2001, og trenden er tydelig – volumet øker.

Når vi samtidig vet at angrepskode i 80 prosent av tilfellene blir utviklet før sårbarheten blir offentlig kjent, er det viktig at alle sårbarheter vurderes og (dersom mulig) mitigeres så fort som mulig. Dette krever stadig mer av bedrifter, da risikoen med å vente er økende år for år med kortere intervaller mellom offentliggjøring av en sårbarhet og utbredt utnyttelse av den.



Mobiltelefonsystemer

PÅ SPRANGET INN I 5G, MEN FORTSATT MED NOEN SVAKHETER I SIKKERHET

Mobiltelefontrafikk har lenge vært viktig for DNBs kommunikasjon, både internt og med våre kunder. Med fjerde generasjons mobiltelefoner (4G) som plattform har vi etter hvert fått et bredt tilbud av tjenester som tilbys på mobil og nettbrett. Mobiltelefonbrukere er i dag meget godt vant med applikasjoner som kan lastes ned. Det er imidlertid en del svakheter knyttet til sikkerheten ved bruk av mobiltelefon som trolig ikke er kjent for brukere flest. Femte generasjons GSM mobiltelefoni, bedre kjent som 5G, vil gi mye høyere datahastigheter og utrullingen er godt i gang. Mange venter at båndbredden vil medføre en eksplosiv økning i bruk. Mye av arkitekturen i 5G-mobiler er ganske lik 4G og mange av svakhetene vil fortsatt være til stede. For DNB-ansattes telefoner er det gjort sikkerhetstiltak mot flere av angrepsformene beskrevet nedenfor, men det er en stadig utvikling og trusselaktører ventes å komme med nye angrepsmåter.

SPOOFING – MANIPULERING AV AVSENDERNUMMERET

Internasjonalt avtalte protokoller definerer hvordan landsnummer, nummerserier og ruting av telefontrafikk skal være. Eksempelvis er nummerserien i Norge landsnummer 47 og åtte siffer. Antall siffer i landsnummer og telefonnummer varierer fra land til land. Når du mottar et anrop eller en sms omformes IMSI-nummeret som følger og du får opp hvem som ringer/sender sms i displayet. Svakheter i protokollene gjør det mulig å manipulere nummeret som vises for mottakeren. Bedragere og andre med tvilsomme hensikter kan få det til å se ut som om de ringer fra et legitimt norsk telefonnummer, når de i virkeligheten sitter i et kriminelt call center i Vest-Afrika eller Sør-Asia. Ofte kan man se at nummerserien ikke stemmer i lengde og sammensetning eller at det ringes fra et nummer som ikke skal være i bruk. Teleselskapene jobber for å motvirke dette, blant annet ved svartelisting av IMSI-nummer, men de kriminelle skifter også nummer og teknikk hyppig.

MANIPULERING GJENNOM LENKER ELLER VEDLEGG I SMS ELLER E-POST.

Lenker kan komme i sms, kalender oppdateringer, meldinger på sosiale medier, eller e-post og leder ofte mot en falsk nettside. På nettsiden kan det være enten nedlasting av skadevare eller en manipulert, tilsynelatende legitim nettside der bruker oppfordres til å legge inn påloggingsinformasjon eller andre sensitive data. Vedlegg i e-poster kan inneholde skadevare. Dette er imidlertid relativt sjeldent fordi vedleggene ville måtte tilpasses mobilens operativsystem ettersom skadevare for PC eller server ikke ville virke på selve mobilen.

INSTALLERING AV EKSTRA APP OG ANGREP MOT OPERATIVSYSTEM

Brukeren kan lures til å laste ned en forfalsket applikasjon, manipuleres til å laste ned en app eller gjøre endringer i operativsystemet. En manipulert telefon kan settes opp til å logge og eksportere tastetrykk (keylogging) eller screenshots, eksportere data fra minnet, eksportere app-data, eksportere posisjonsdata, samt eksportere kamera- eller lydopptak.

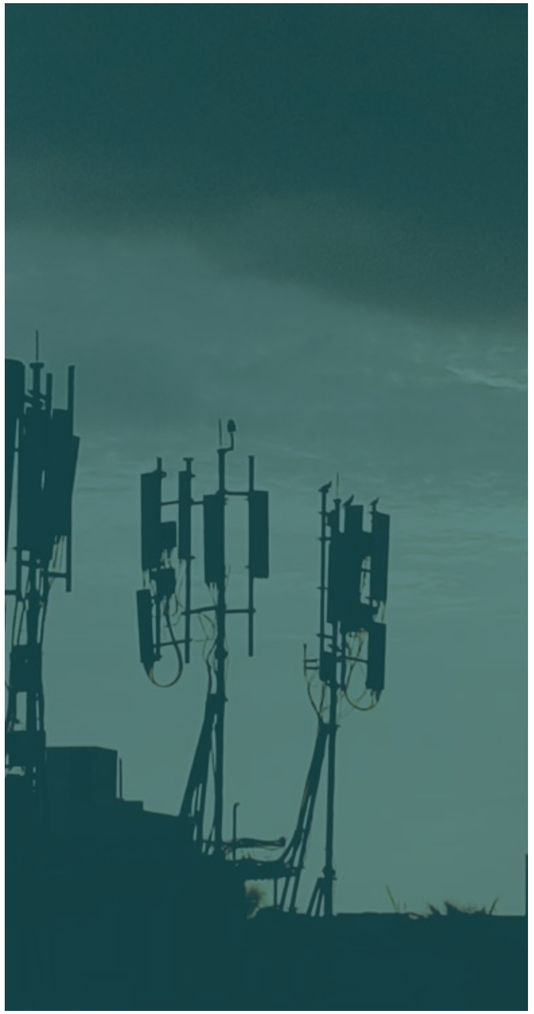
Brukeren kan lures til å laste ned en app ved en phishing mail (se mer om phishing side 37), eller en trussel aktør kan få plassert en falsk app i et miljø for app-nedlasting. Appen som lastes ned kan senere skjules fra appregistret på telefonen. I Google Play og App Store er det gjort betydelige tiltak for å forhindre dette, men brukere kan lures inn på andre tilsynelatende ekte, men i realiteten falske nettsider hvor det tilbys nedlasting av applikasjoner. En enda mer avansert, men heldigvis sjeldent forekommende metode er å gjøre endringer i mobilens operativsystem.

Operativsystemet manipuleres i form av en forfalsket oppdatering. Som regel må brukeren aktivt være med og godkjenne oppdatering, men det israelske firmaet NSO Group som selger avlyttingssystemer til mange lands myndigheter, lykkes i 2019 med å finne en måte å manipulere operativsystem på uten medvirkning fra bruker eller varsel om oppdatering. DNBs telefoner er denne spesifikke metoden sperret, men avanserte trusselaktører kan fremover utvikle nye metoder for å nå inn til operativsystemet uten brukerens medvirkning

En annen avansert metode som vi heldigvis ikke har sett så mye til enda, er leveransekjedeangrep mot app-leverandører. Trusselaktøren bryter seg inn i IT-systemet til en app-leverandør og legger inn trusselaktørens «oppdateringer» i app-oppdateringer som skal sendes ut. For PC- og serverbaserte nettverk har denne metoden vært brukt en del år og vi kan se for oss en tilsvarende utvikling for mobiltelefoner. Apple og Google arbeider aktivt for å hindre dette fra leverandører som bruker App Store og Google Play.

FALSK BASESTASJON (IMSI-CATCHING) – MANIPULERING AV RADIOSEGMENTET

Den metoden for å bryte inn i mobiltrafikk som kanskje har vært mest omtalt i media er bruk av falske basestasjoner. Dette er teknisk krevende og vil sannsynlig kun være aktuelt mot noen prioriterte telefoner. Trusselaktøren benytter en falsk basestasjon, signalene til/fra mobilen går igjennom denne basestasjonen før det videresendes til en ekte basestasjon. En falsk basestasjon kan styres mot ett eller noen spesifikke telefoner. Den falske basestasjonen må plasseres innenfor noen hundre meter fra målet for å virke med sterkere signal i målområdet enn ekte basestasjoner. Størrelsen på en slik falsk basestasjon kan være så liten som en koffert eller liten ryggsekk. Metoden vil være beste egnet for å følge telefon- og datatrafikken til nøkkelpersoner som trusselaktøren er spesielt interessert i. Metoden kan også brukes for å finne ut om telefonen til spesifikke personer har vært på et bestemt sted, eksempelvis til stede under viktige forhandlinger.



TRUSLER I DATASEGMENTET

TYVERI OG UTNYTTELSE AV AGGREGERT TRAFIKKDATA

I styring av mobiltelefontrafikk, og spesielt roaming, genereres spesifikke data om samtalers varighet, over hvilken basestasjon og mellom hvilke abonnementer (IMSI - nummer) en samtale eller datatrafikk går. Denne typen trafikkdata kan sees på som metadata for samtalen eller datautvekslingen. For å gjøre opp mellom teleleverandørene utveksles slike data i fem-seks større internasjonale clearing-houses. I 2021 viste det seg at ett av disse, USA- og India-baserte Syniverse hadde vært utsatt for datatyveri, angivelig av en statsaktør, over en periode på cirka fem år. Vi kan se for oss at kriminelle i fremtiden vil kunne prøve å komme til denne typen data. Filtrert og behandlet riktig vil det kunne gi mye informasjon om en banks relasjon til kunder, noe som vil være et godt utgangspunkt for systematiske bedragerier i stor skala.

OVERVÅKNING AV GRENSEKRYSSENDE DATATRAFIKK

Mobiltelefontrafikk som går mellom telekomleverandører ute i verden går som vanlig trafikk i datalinjer. En rekke land har innført overvåkning av datalinjer som krysser landenes grenser. Mobiltelefontrafikk kan filtreres og overvåkes som annen datatrafikk.

4G: (UMTS) Fjerde generasjon GSM mobiltelefonsystemer. Innført fra ca. 2007. Softwaredrevne telefoner med applikasjoner (apper) og høyere båndbredde enn tidligere generasjoner.

5G: Femte generasjon GSM mobiltelefonsystemer. I Norge har utrulling av teknisk infrastruktur startet. Utrullingen kommer til å vare noen år og vi vil se parallell drift av 4G og 5G. Mobiltelfonen vil fra start være relativt lik, men med mye høyere dataoverføringshastighet. Det vil bli mulig for store brukere å kjøpe egne avdelte «nett i nettet».

Radiosegmentet: Delen av mobilsystemet som sender radiosignaler mellom mobilen og sender/mottaker i basestasjonen.

Datasegmentet: Fra basestasjonen gjennom lokale og regionale datalinjer, teleleverandørens datasenter og ut igjen til en annen basestasjon. Datasignalene kan krysse over til en annen teleleverandør og annet land avhengig av hvem det ringes fra/til.

IMSI-nummer: Et unikt nummer for hvert SIM-kort. Abonnementet er knyttet til dette nummeret.

Trafikkdata: Oversikt over telefon- og datatrafikk, hvem har ringt/ overført data til hvem, over hvilke basestasjoner til hvilken tid. IMSI-nummeret og telefonens IMEI-nummer inngår i trafikkdata.