Trusselvurdering 2023

DNB

Om årlig trusselrapport

Årlig trusselvurdering 2023 er utarbeidet på tvers av fagmiljøene i DNB. Trusselvurderingen består av vurderinger innenfor syv ulike trusselkategorier som viser til sannsynligheten for en hendelse mot DNB, samt fem artikler som omhandler generelle temaer knyttet til trusselbildet. Rapporten tar sikte på å gi en bredest mulig vurdering av relevante sikkerhetstrusler mot DNBs virksomhet i en tidsramme på ett til to år frem i tid. Group Security i DNB koordinerer arbeidet og ansvarlig for utgivelsen er Anders Hardangen, Sikkerhetsdirektør i DNB.

Sannsynlighetsord

Sannsynlighetsordene som vi benytter under trusselkategoriene beskriver vurdering av sannsynligheten for en hendelse mot DNB. Begrepene og beskrivelsen av sannsynlighetsordene er de samme som benyttes av blant annet politiet, PST og Forsvaret i deres vurderinger.

Meget sannsynlig	Det er meget god grunn til å forvente	>90 % sannsynlighet
Sannsynlig	Det er grunn til å forvente	60-90 % sannsynlighet
Mulig	Det er like sannsynlig som usannsynlig	40-60 % sannsynlighet
Lite sannsynlig	Det er liten grunn til å forvente	10-40 % sannsynlighet
Svært lite sannsynlig	Det er svært liten grunn til å forvente	<10 % sannsynlighet

Nøkkelfakta

Her beskriver vi med korte nøkkelfakta noen av de viktigste hovedmomentene innenfor de trusselkategoriene og tema som vi tar for oss i rapporten.

Frustrasjon har ført til flere trusler mot ansatte

Digitale trussel-aktører prøver å trenge inn i DNBs systemer hver dag

Ukjente aktører ønsker tilgang til informasjon om DNB-ansatte

Programvarekomponenter kan være en åpen dør til dine hemmeligheter

Målrettede aksjoner fra klimaaktivister kan treffe DNB

Antall forsikringssvindler kan øke på grunn av økonomiske nedgangstider

Kriminelle grupper misbruker tillits-baserte systemer til uberettiget vinning

Lange forsyningslinjer kan være sårbare for sabotasje

Hybride bedra-gerier tar over for tradisjonelle bedrageriformer

Innsidere motiveres oftest av økonomisk fortjeneste

Interessekonflikter fører til høyere korrupsjonsrisiko

Økende bruk av inter-nasjonale sanksjoner skaper uforutsigbarhet for næringslivet

Trusselaktører kan ha mange motivasjonsfaktorer i sine angrep mot finansnæringen.

Da vi utarbeidet årlig trusselvurdering for 2022 var verden på vei til å endres mer enn det vi kunne ane. Russland hadde akkurat startet sin aggresjon mot Ukraina og det var vanskelig å si hvordan konflikten ville arte seg. Nå, ett år senere, er Europa fortsatt i krig og en av de verste konfliktene siden andre verdenskrig er et faktum på vårt kontinent.

Anders Hardangen.

Anders Hardangen,
Sikkerhetsdirektør i DNB

Dette er med på å endre trusselbildet for hele den vestlige verden, for Norge og for DNB som en del av den norske finansnæringen.

«Mens trusselbildet for inntil få år siden var nesten utelukkende preget av finansielt motiverte trusselaktører, må vi i dag forberede oss på å bygge motstandskraft mot statlige og politiske krefter som kan ha en annen motivasjon.»

Trusselaktører kan ha mange motivasjonsfaktorer i sine angrep mot finansnæringen. De kan ønske å påvirke opinionen, øke usikkerhet eller å sabotere. I ytterste konsekvens kan målet være en form for hybrid krigføring.

Trender som vil fortsette å utvikle seg

Hendelsene DNB opplever daglig og jobber aktivt med å avverge er fortsatt primært tilknyttet finansielt motiverte aktører, men trusselvurderingen er et hjelpemiddel for å kunne forutse nye trusselaktører og fremtidige handlinger. I 2022 så vi en stor økning i antall hendelser innenfor bedragerifeltet, mens det var færre alvorlige cyberangrep enn tidligere år. Dette er trender som vil fortsette å utvikle seg, og trusselaktørene vil bruke et vidt spekter av måter de oppnår det de vil på. Trusselvurderingen til DNB skal hjelpe med å identifisere utviklingen i trusler og trender som berører finansinstitusjonene. Slike hjelpemidler er helt nødvendige for å jobbe risikobasert og kunne foreta de riktige tiltakene på det rette tidspunktet.

DNBs formål med offentliggjøring av denne trusselvurderingen er å gi et bilde fra et norsk perspektiv slik at vi kan øke bevisstheten rundt truslene vi står overfor og hva vi opplever av angrep mot DNB og våre kunder. Tidligere år har mitt budskap vært at vi står sammen mot de som truer vår sikkerhet og våre verdier, i år står dette budskapet seg enda sterkere.

Trusselvurderinger utgjør en viktig del av prosessen ved å identifisere og bevisstgjøre om mulige trusler som det bør rettes tiltak mot.

Ikke siden andre verdenskrig har Norge blitt berørt av en krig slik vi har blitt etter Russlands invasjon av Ukraina. Vi har i Norge lenge hatt en beredskap som har vært bygget for dyp fred. Nå har vi på kort tid måttet håndtere situasjoner som mulig sabotasje mot kritisk infrastruktur, digitale angrep og spionasje.

Sofie Nystrøm,
Direktør i Nasjonal sikkerhetsmyndighet

De eskalerende geopolitiske spenningene gjør at vi må tenke nytt om egen sikkerhet og hvordan vi best mulig kan sikre sentrale nasjonale interesser i et stadig endret trussel- og risikobilde. Arbeidet med sikkerhet handler om å beskytte noe som er verdifullt. Tap av dette kan gi negative konsekvenser, ikke bare for virksomheter selv, men samfunnet for øvrig.

Innen cyberoperasjoner har antallet alvorlige og svært alvorlige hendelser i 2022 holdt seg på et tilsvarende nivå som i 2021. Selv om antall faktiske kompromitteringer var lavere enn i 2021. Det det ble benyttet et bredt spekter av angrepsmetoder og ofte i form av politiske hevnaksjoner. Kriminelle pro-russiske hackergrupper har gått mot spesifikke mål i Norge og gjennomført tjenestenektangrep for å skape uro og usikkerhet i befolkningen.

«Sabotasje og andre handlinger mot kritisk infrastruktur har det siste året vært et høyaktuelt tema, og utgjør en trussel i krigstider så vel som i fredstider.»

Avhengigheten mellom samfunnsfunksjoner har gjort oss sårbare. Angriperne søker etter å hoppe over gjerdet der det er lavest og gå mot leverandører og underleverandør som ikke klarer å ivareta sikkerheten like godt.

Mange land vil bruke store ressurser og avanserte metoder for å skaffe informasjon eller fortrinn som er viktig for å ivareta sine nasjonale interesser. Blant disse metodene finner vi cyberoperasjoner, fysisk og digital kartlegging, påvirkningsoperasjoner, rekruttering av personer og strategiske investeringer.

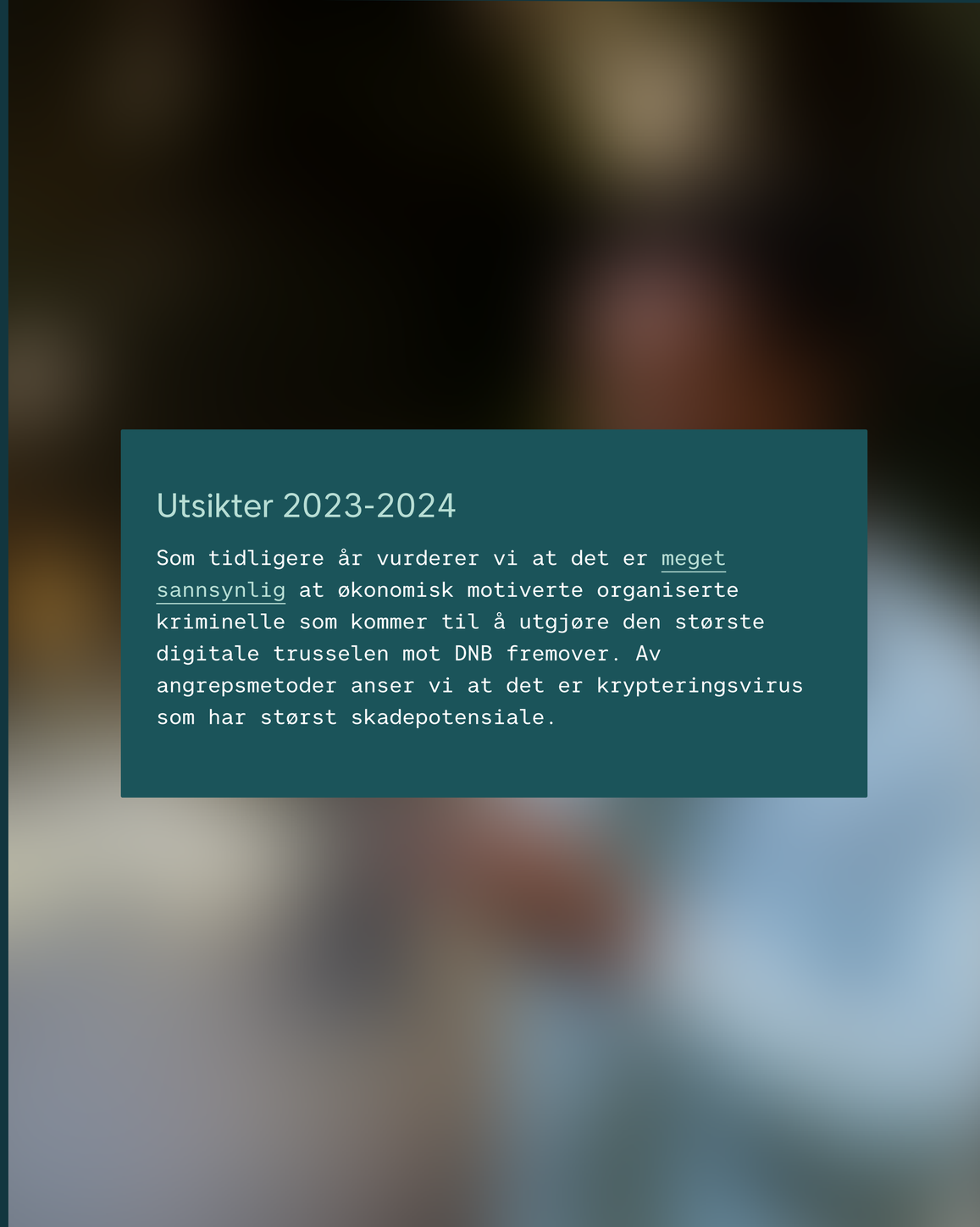
Beredskap bygges før krisen inntreffer. Norske virksomheter må i dag prioritere sikkerhet i enda større grad for å kunne ha tilstrekkelig motstandskraft i fremtiden. Virksomheter må identifisere hvilke verdier de råder over, analysere risikoen for at verdiene kan gå tapt, og iverksette og opprettholde nødvendige tiltak slik at verdiene er tilstrekkelig beskyttet.

Trusselvurderinger utgjør en viktig del av denne prosessen ved å identifisere og bevisstgjøre om mulige trusler som det bør rettes tiltak mot. Ved å offentliggjøre sin trusselvurdering bidrar DNB til økt trussel- og sikkerhetsforståelse for andre virksomheter og samfunnet for øvrig.

Trusselvurdering

Digitale trusler – aktører

Hver dag forsøker trusselaktører å trenge inn i DNBs digitale infrastruktur i den hensikt å få tak i informasjon, sabotere eller oppnå økonomisk vinning. De fleste angrep er økonomisk motiverte, men vi har det siste året sett at også finans-institusjoner kan bli angrepet som følge av samfunnsfunksjon, for å skape usikkerhet og ustabilitet. Pro-russiske hacker-grupper har det siste året utført omfattende og organiserte tjenestenektangrep mot mål i NATO-land. Stadig oftere ser vi at finansinstitusjoner innlemmes i dette som ledd i forsøk på å ramme vestlig økonomi.



Utsikter 2023-2024

Som tidligere år vurderer vi at det er meget sannsynlig at økonomisk motiverte organiserte kriminelle som kommer til å utgjøre den største digitale trusselen mot DNB fremover. Av angrepsmetoder anser vi at det er krypteringsvirus som har størst skadepotensiale.

Sikkerhetssituasjonen i Europa har endret det digitale trusselbildet

Etter den russiske invasjonen av Ukraina 24 februar, har det geopolitiske klimaet vært preget av eskalerende spenninger mellom Russland og NATO. Dette har skapt en ny sikkerhetspolitisk situasjon som også får konsekvenser for Norge. Ifølge PST er faren for en reell sabotasjeaksjon større nå enn før krigen i Ukraina, men skal ikke være sannsynlig i dag. En slik aksjon anses heller som et verste-fall-scenario i et trusselbilde i rask utvikling. Dersom det skulle komme en sabotasjeaksjon mot Norge, kan den være enten fysisk eller digital. Selv om det ikke er rapportert om sofistikerte cyberangrep mot vestlige finansinstitusjoner, blir sektoren stadig utsatt for tjenestenektangrep (DDoS). Stort sett har angrepene svært begrenset konsekvens, men det kan virke skremmende for forbrukere som kanskje får inntrykk av at tilgangen på finansielle tjenester står i fare. Trusselbildet utvikles dynamisk og som følge av krigen hurtigere enn tidligere, og god informasjonsutveksling er viktigere enn tidligere for å oppnå trussel- og situasjonsforståelse.

Utfordrende å attribuere cyberangrep

Det kan være svært krevende 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 det.

Organiserte kriminelle er den mest aktuelle trusselaktøren for finanssektoren

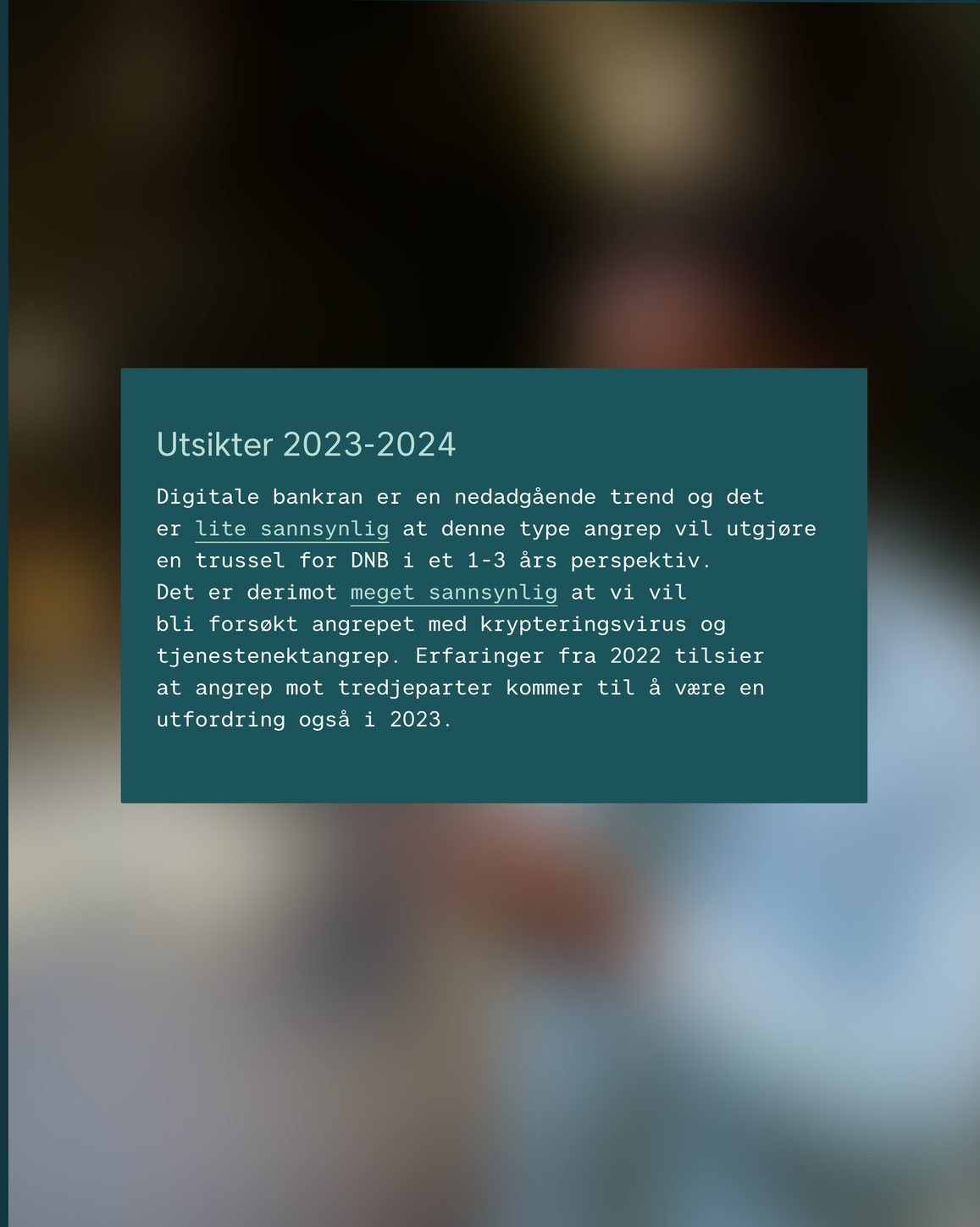
Den største digitale trusselen mot DNB kommer fra økonomisk motiverte kriminelle grupper. De er profesjonelle og svært kompetente, og har tradisjonelt ofte hatt tilholdssted i Øst-Europa og noen land i Asia. Noen ganger er det vanskelig å skille mellom disse gruppene og statlige aktører, fordi en del av betingelsene for å få lov til å operere kan være at gruppene av og til tar oppdrag fra statlige etterretningstjenester. I tillegg har man i 2022 sett en utvikling der også cyberkriminelle grupper tar side i statlige konflikter og utfører cyber-angrep for å fremme en politisk agenda. Slike grupperinger kalles da for «Hacktivister».

Statlig-støttede aktører utgjør en svært krevende trussel

Når statsaktører opererer i det digitale rom kalles de «Advanced Persistent Threats» (APT). De har stor evne til å utføre avanserte cyberangrep, som regel for spionasjeformål, eller til støtte for en politisk agenda. Slike grupper er ofte statlig organiserte militære- eller sivile etterretningsenheter med cyberkapabiliteter, men det kan også være snakk om grupperinger av organiserte kriminelle som får operere uten statlig inngripen. I 2022 var det lavere aktivitet på cyber-fronten fra APT-aktører enn det vi hadde forventet. En av grunnene til dette kan være at for eksempel Russland har fokusert sin cyberkapabilitet hovedsakelig på Ukraina i forbindelse med krigen. Dette er i så fall en trend vi forventer vil fortsette så lenge krigen pågår.

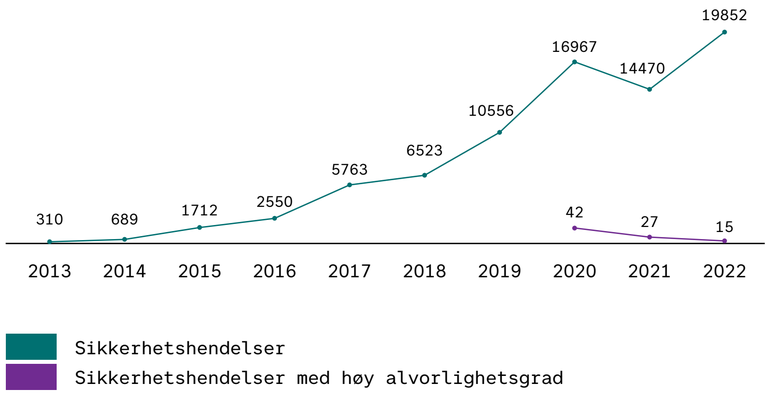
Digitale trusler – angrepsformer

Selv om antallet angrepsforsøk er stadig økende, har vi sett en trend med nedgang i de mer alvorlige hendelsene. I 2022 håndterte DNB 15 cyberangrep som hadde et alvorlig skadepotensial for konsernet. Dette representerer en nedgang fra de siste to årene. Samtidig ser vi at de cyberangrepene som rapporteres i samfunnet kan få et større omfang enn tidligere fordi disse ofte er leveransekjedeangrep og har større nedslagsfelt.



Utsikter 2023-2024

Digitale bankran er en nedadgående trend og det er lite sannsynlig at denne type angrep vil utgjøre en trussel for DNB i et 1-3 års perspektiv. Det er derimot meget sannsynlig at vi vil bli forsøkt angrepet med krypteringsvirus og tjenestenektangrep. Erfaringer fra 2022 tilsier at angrep mot tredjeparter kommer til å være en utfordring også i 2023.



DNB anser fortsatt den digitale trusselen som høy i de fleste kategorier. Videre er trusselbildet stadig i endring og har i økende grad blitt et samfunnsproblem. Cyberangrep kan medføre stor skade med konsekvenser for renommé og evnen til å ivareta forpliktelser overfor kunder og tilgjengelighet til finansielle tjenester. Sikkerhet er derfor et samfunnsansvar som DNB tar på alvor og et tema som angår alle ansatte på alle nivåer i organisasjonen.

Hacktivisme er på fremmarsj

Hacktivisme er et begrep som kombinerer «hacking» og «aktivisme», og går ut på at cyberangrep utføres basert på politisk eller ideologisk agenda. Etter Russlands invasjon av Ukraina i februar 2022 har mange cyberkriminelle aktører valgt side i konflikten, og utført angrep til støtte for sin valgte part. Det benyttes både destruktive cyberangrep, digitale desinformasjonskampanjer, og tjenestenektangrep som ledd i dette. Gjennom 2022 har NATO-land blitt utsatt for tjenestenektangrep fra grupper som NoName057(16) og Killnet. Dette er svært aktive grupper som på daglig basis velger seg mål i NATO-land basert på en forståelse av at digitale angrep mot viktige bedrifter sender sterke signaler. I januar og februar i 2023 har slike angrep også rettet seg mot finansinstitusjoner i Norge, Sverige og Danmark.

Hacktivisme forbeholder seg ikke kun politisk agenda i forbindelse med krigen i Ukraina, men har det siste året også blitt benyttet til støtte for et bredt spekter av andre politiske temaer. Eksempelvis har hackergruppen Anonymous utført cyberangrep mot mål i Iran til støtte for opprop for kvinners rettigheter i landet, og tyrkiske Türk Hack Team har truet mål i Sverige i forbindelse med Koran-brennning. I løpet av 2022 har Hacktivisme etablert seg som en stabil trend og vi kan forvente å se mer av dette i årene som kommer.

Krypteringsvirus har størst skadepotensiale

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 de siste årene og er tilpasset offerets betalingsevne. Som regel er dette målrettede angrep, men det er også eksempler på at skadevare kan spre seg utenfor en angripers kontroll og dermed nå utilsiktede mål. Dette skjer først og fremst når skadevare kjent som en «orm» benyttes i et angrep. En «orm» er en type selv-spredende virus som kopierer seg selv fra en maskin til en annen innad på samme nettverk. Slike angrep har blitt observert i enkelte tilfeller i 2022 der angrep myntet på Ukraina tilsynelatende utilsiktet har nådd mål i for eksempel Latvia og Litauen.
I tillegg til rent destruktive angrep kan man anta at cyber-spionasjeoperasjoner forekommer i større grad, men slike angrep er også langt vanskeligere å oppdage.

Økning i tjenestenektangrep

Vi opplever fortsatt at tjenestenektangrep utføres mot DNB med jevne mellomrom, og vi blokkerer denne trafikken i samarbeid med tjenesteleverandører. 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 bankens nettsider, betyr det at de kan bli utilgjengelige for kundene våre.

Tjenestenektangrep har blitt flittig brukt i forbindelse med krigen i Ukraina, der pro-russiske hackergrupper angriper bedrifter i land som støtter Ukraina. I disse angrepene er det ikke kun nettsider tilhørende statlige selskaper som blir tatt ned, men også selskaper som oppfattes å understøtte viktige samfunnsfunksjoner på andre måter. Finansinstitusjoner har blitt ansett som gode mål for å ramme sivilsamfunnet, noe vi blant annet har sett i angrep mot danske og svenske banker i januar og februar i 2023. DNB er generelt sett godt rustet mot slike angrep, og vi forventer at tjenestenektangrep fortsetter på samme nivå fremover.

Digitale bankran utføres av profesjonelle vinningskriminelle

Digitale bankran kan forekomme ved at trusselaktører forsøker å få illegitim tilgang til bankens datasystemer og forsøker å overføre penger ut av banken. Å gjennomføre digitale bankran er teknisk krevende, og har blitt enda vanskeligere de siste årene. For noen år siden var det enkelte tilfeller av slike «digitale bankran» i andre land, men det er flere år siden dette har vært en aktuell problemstilling. Vi ser at det sannsynligvis er en sammenheng mellom nedgangen i digitale bankran mot tradisjonelle banker, og at aktørene har tatt i bruk andre metoder for å oppnå økonomisk vinning. Dette er først og fremst fordi trusselaktørene i økende grad utfører digitale bankran mot kryptobørser, samt at de heller benytter løsepengevirus og digital svindel.

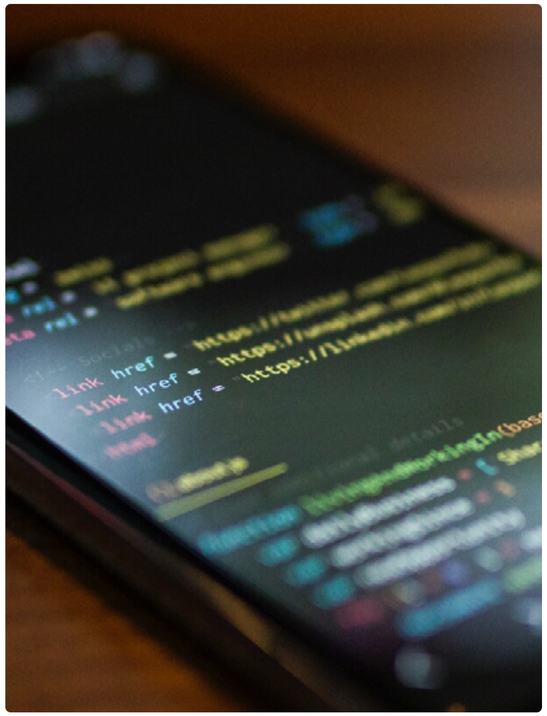
Tredjepartsangrep er svært effektive, og øker i antall og omfang

Mange virksomheter er avhengige av å kjøpe tjenester og programvare fra underleverandører. Dette gjelder også DNB. Vi vurderer tredjepartsangrep å være en økende trend som trolig blir mer utbredt i kommende år. I lys av dette blir håndtering av tredjepartsrisiko viktigere enn før og sikkerhetsmessige vurderinger ved integrasjon av tredjeparter må i større grad gjøres som et forebyggende tiltak. I 2022 håndterte DNBs Cyber Defense Center 5 hendelser hos tredjeparter som hadde alvorlig skadepotensiale for DNB. Vi må forvente angrep via tredjeparter og derfor være i stand til å forsvare oss mot det når det skjer.

Stadig flere cyberangrep har et tredjepartsaspekt. I leveransekjedeangrep infiltrerer trusselaktøren et datasystem eller nettverk via en partner eller leverandør som har rettmessig tilgang. Da kompromitteres tredjeparten først, og så utnyttes den allerede etablerte tilliten mellom tredjeparten og sluttmålet i videre angrep.

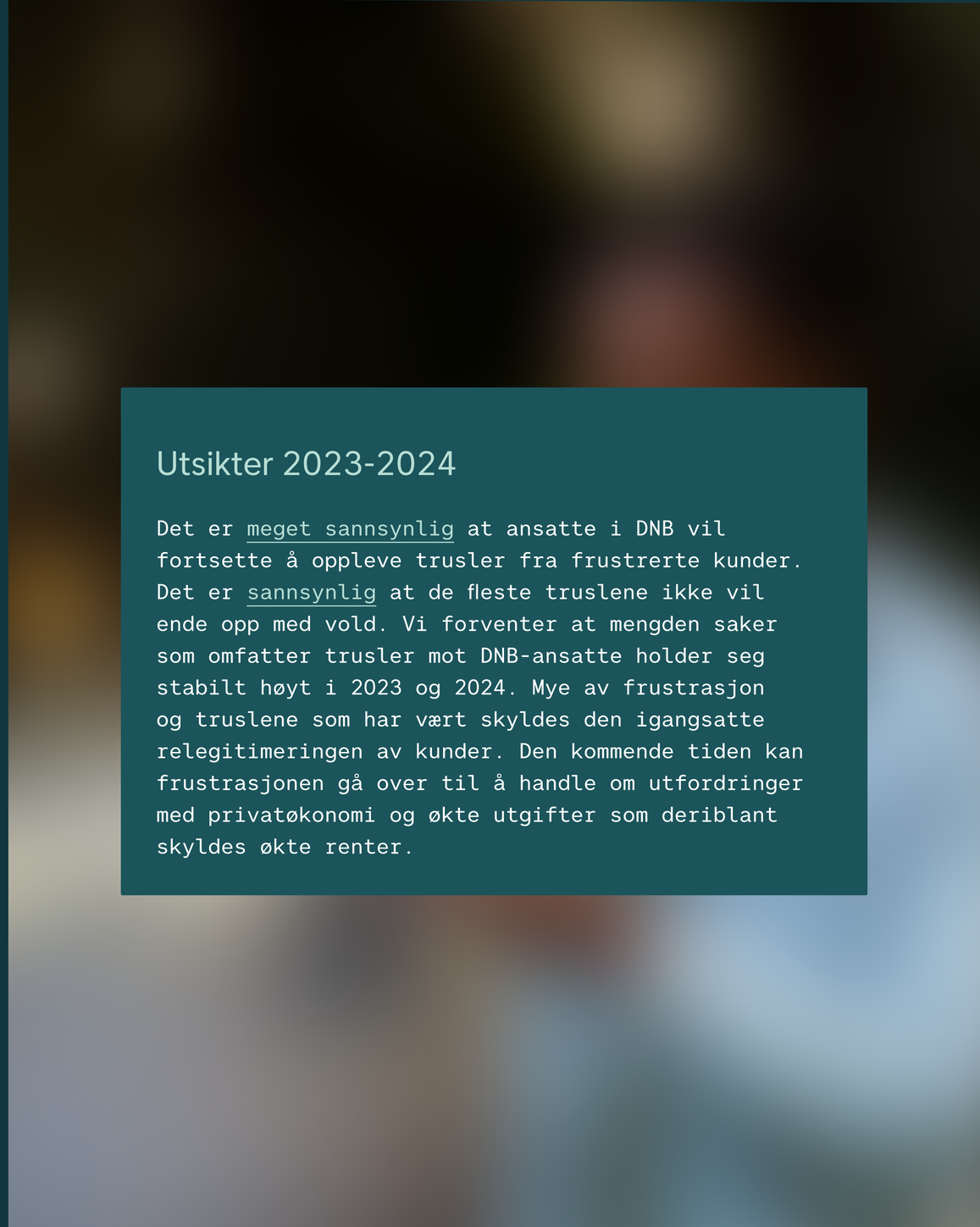
Det kan være flere grunner til at cyberkriminelle grupper velger tredjepartsangrep. Én årsak kan være at tredjeparts-leverandøren har dårligere sikkerhet enn sluttmålet. En annen kan være for å nå flere mål som følge av tilganger og integrasjoner som forvaltes av tredjeparten. På den måten får trusselaktøren tilgang til disse virksomhetene gjennom tredjepartsleverandøren. Da kan de fokusere på å kompromittere én virksomhet, og gjennom den få tilgang til mange flere.

Når en bedrift opplever et cyberangrep, er det viktig at koblinger mot tredjeparter kartlegges og sikres raskt. Tredjepartsangrep kan forekomme som rene cyber-angrep via tilgangene en tredjepart legitimt innehar eller det kan forekomme ved å utnytte relasjonen til sosialmanipulasjon. Det kan for eksempel skje i såkalte «Business Email Compromise» (BEC)-angrep, der en kompromittert epost-konto blir utnyttet til å sende ut skadelig epost til tidligere kontakter. DNB observerte flere slike kampanjer i fjor. De er ofte svært effektive, da eposten og sosial manipulering kommer fra noen mottaker tidligere har snakket med og kanskje stoler på.



Trusler mot DNB-ansatte

DNB-ansatte opplever i enda større grad å bli utsatt for trusler fra privatkunder, både på telefon og fysisk i DNBs lokaler. I et fåtall tilfeller har truslene kulminert til vold. I 2022 så vi en merkbar økning i antall tilfeller av trusler og vold mot ansatte sammenlignet med 2021. Mange av truslene ble fremsatt av privatkunder etter at deres kontoer ble sperret som en konsekvens av det myndighetspålagte kravet om relegitimering. Noen av de som fremmer truslene har tidligere vært kjent av banken for lignende forhold.



Utsikter 2023-2024

Det er meget sannsynlig at ansatte i DNB vil fortsette å oppleve trusler fra frustrerte kunder. Det er sannsynlig at de fleste truslene ikke vil ende opp med vold. Vi forventer at mengden saker som omfatter trusler mot DNB-ansatte holder seg stabilt høyt i 2023 og 2024. Mye av frustrasjon og truslene som har vært skyldes den igangsatte relegitimeringen av kunder. Den kommende tiden kan frustrasjonen gå over til å handle om utfordringer med privatøkonomi og økte utgifter som deriblant skyldes økte renter.

DNB-ansatte blir utsatt for alvorlige trusler

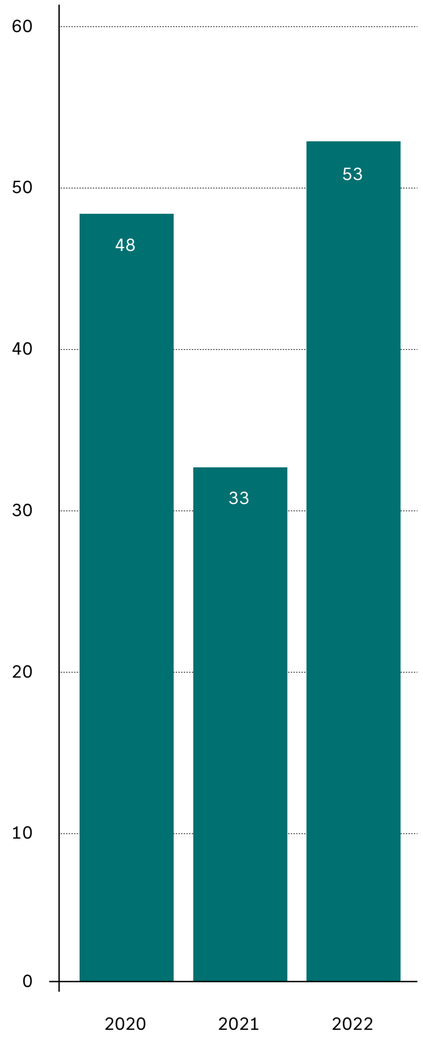
De fleste DNB-kunder har gått gjennom prosessen med å verifisere identiteten i løpet av 2022. Noen av våre kunder har av ulike grunner hatt problemer med å fullføre prosessen og har vendt sin frustrasjon mot DNB-ansatte. Det har vært flere tilfeller der enkeltkunder har fremsatt trusler mot DNB-ansatte etter å ha fått kontoene sine sperret på grunn av manglende legitimasjon. I andre tilfeller har truslene kommet fordi kunden ønsket hjelp til tjenester som kundebehandlere ikke har mulighet eller fullmakt til å gi. Truslene som fremsettes er ofte meget grove.

Flere av truslene går på person og ansatte blir truet med at kunden vil oppsøke den ansatte hjemme. Vi har ikke kjennskap til at dette faktisk har skjedd i løpet av 2022, men en ansatt har opplevd å få tilsendt et brev med trusler hjem. Det er fra tidligere år eksempler på ansatte som har blitt oppsøkt hjemme av kunder.

Ved to tilfeller mottok DNB-ansatte bombetrusler fra frustrerte kunder. I begge tilfeller ble det vurdert av DNB og politiet at vedkommende ikke ville gjøre alvor av truslene, samtidig som begge sakene i ettertid ble anmeldt. I flere andre saker, som ble vurdert som ikke reelle, har ansatte blitt truet med at innringer skulle komme til et av DNBs lokaler med skytevåpen. Til sammen har DNB i 2022 anmeldt 21 uønskede hendelser til politiet, sammenlignet med kun 9 i fjor. Det har i veldig få saker vært forsøkt eller faktisk blitt utøvd vold mot ansatte. I de få tilfeller hvor dette har funnet sted har det vært rettet mot vektere i et av DNBs lokaler. Det er iverksatt en rekke rutiner og tiltak i DNB i forbindelse med ovennevnte saker, både når det gjelder trusselutøver og oppfølging av ansatte. DNB har en erfaren sikkerhetsavdeling som bistår ansatte og ledere under og etter hendelsene.

Økte renter og krevende økonomiske tider kan resultere i flere trusler

Det finnes lite tilgjengelig historisk informasjon om fremsatte trusler mot ansatte i finanssektoren i Norge, og det er derfor lite grunnlag for å vurdere hvordan økonomiske nedgangstider påvirker trusler mot bankansatte. Samtidig viser DNBs egne hendelser at fortvilelse og frustrasjon kan gi utfordrende adferd og gjøre personer mer tilbøyelige til å fremsette trusler. Som Norges største utlånsbank er DNB særlig utsatt når det gjelder misnøye og frustrasjon over rentehevinger, som kommer på toppen av økte strøm-, matvare- og drivstoffpriser. Utenom kundebehandlere som sitter i førstelinjen og møter kunder, er også DNB-ansatte i media mer utsatt for trusler, som bunner i frustrasjon over de økte renteutgiftene som attribueres banken.



Trusler og vold mot ansatte

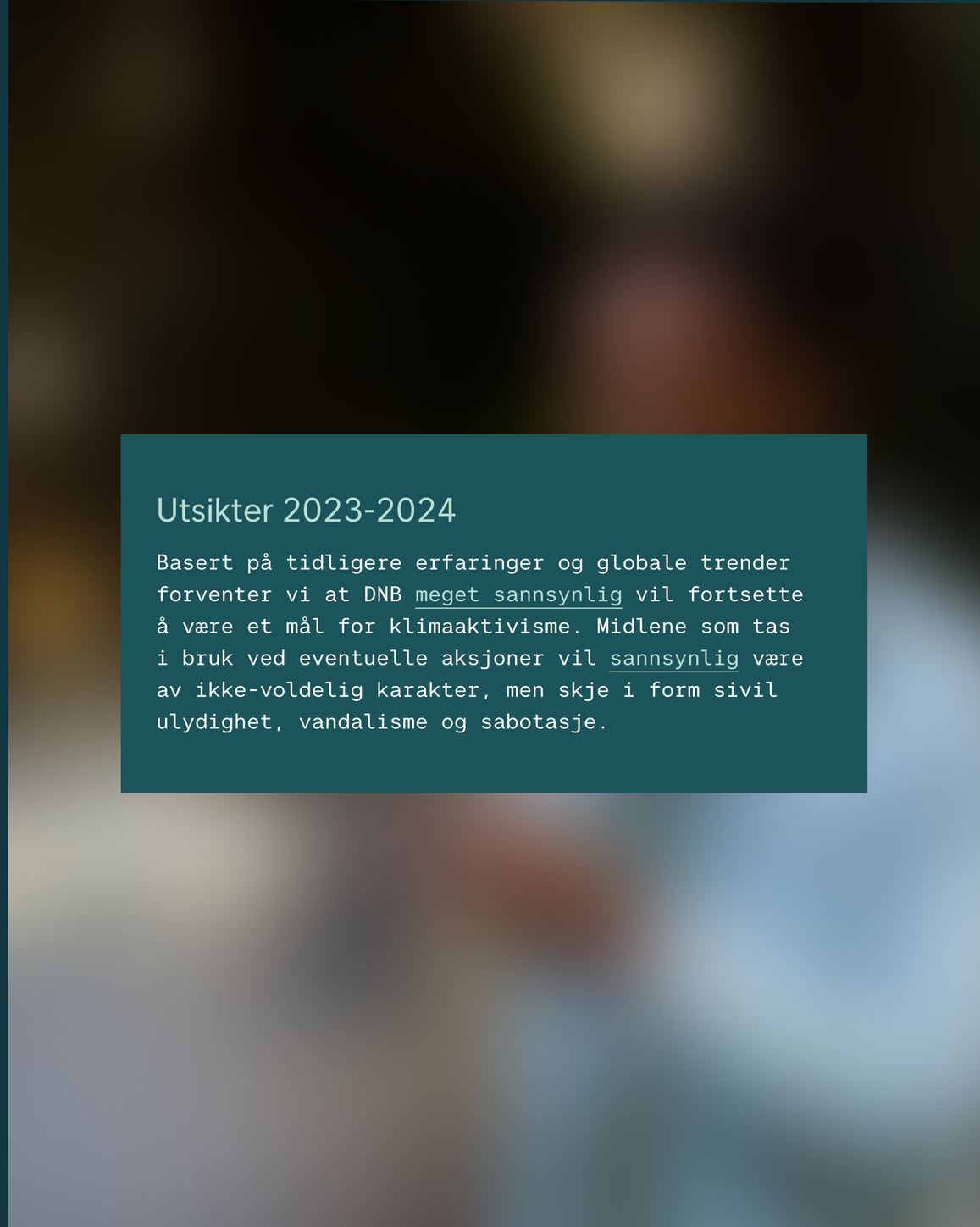
DNB har hatt dobling i antall innringere som truer med selvskading og selvmord

DNB-ansatte opplever også å bli oppringt av personer som i samtalen med kundebehandlere gir uttrykk for at de har selvmordstanker. I 2022 så vi 40 slike hendelser, som er mer enn en dobling i antall saker sammenlignet med i fjor. Bakgrunnen for selvmordstankene har oftest vært frustrasjon over relegitimeringen, avvikling av kundeforhold, men også i stor grad utfordrende privatøkonomi, gjeldsproblemer og samlivsbrudd.

DNB-ansatte tar samtalene med den største alvorlighet og prøver alltid å henvise kundene til «Hjelpetelefonen». I de mer alvorlige sakene kontakter den ansatte helsevesenet og politiet som følger opp personen på adressen. Dette er en psykisk påkjenning både for kunden og for den ansatte. Ledere i DNB og HMS-personell følger opp medarbeidere som kan føle slike samtaler som en påkjenning.

Aktivisme mot DNB

Det har gjennomgående i 2022 vært målrettede aksjoner fra klimaaktivister mot selskaper i bank- og finanssektoren i Europa og USA. Bakgrunnen for aksjonene har vært finansinstitusjonenes investeringer og finansiering av olje- og gassindustrien. Også DNB erfarte i 2022 å være et mål for miljøaktivistgrupper. Til tross for at DNB er en pådriver for bærekraftig omstilling er det sannsynlig at vi vil være et mål for aktivistene også i den kommende tiden. Vi forventer at aktivisme mot DNB vil være av ikke-voldelig karakter. Samtidig viser utviklingen i retorikk og bruk av virkemidler at det i større grad begås ordensforstyrrelser og skadeverk under slike aksjoner.



Utsikter 2023-2024

Basert på tidligere erfaringer og globale trender forventer vi at DNB meget sannsynlig vil fortsette å være et mål for klimaaktivisme. Midlene som tas i bruk ved eventuelle aksjoner vil sannsynlig være av ikke-voldelig karakter, men skje i form sivil ulydighet, vandalisme og sabotasje.

Klimaaktivister går målrettet etter bank- og finansinstitusjoner

I løpet av 2022 har klimaaktivister hatt et høyt aktivitetsnivå hvor det ble tydelig at det nå tas i bruk nye og sterkere virkemidler for å nå frem med sitt budskap. Blant annet ved at klimaaktivister går til angrep på berømte kunstverk og sabotasje gjennom obstruksjon. PST har tidligere antydet at det er et potensial for radikalisering i bevegelsen, men at det fremdeles ikke er noen høy risiko for voldelig ekstremisme fra disse miljøene. Imidlertid kan klimasaken for enkelte individer oppleves som en eksistensiell trussel, noe som drar dem mot randsonen hvor aksjonsrepertoaret radikaliseres.

I 2022 så vi at det i Europa og USA var en rekke protester og aksjoner mot selskaper i bank- og finansnæringen hvor det ble tatt i bruk virkemidler som ruteknusing og tilgrising av fasader. I noen tilfeller har aktivistene utført ulovlige handlinger mot konsernledelsens private eiendommer. DNB erfarte 26. april i fjor at miljøaktivistgruppen Extinction Rebellion (XR) utførte en direkte aksjon mot DNBs hovedkontor i Bjørvika. Åtte aktivister skrev slagord på deler av kontorfasaden og tildekket den med kunstig olje. Aktivistene var fredelige og forlot lokalene etter at politiet ble tilkalt. Aktivistene hadde også forsøkt å rengjøre kontorfasaden i ettertid. XR aksjonerte igjen 5. mai samme år mot DNBs kontorer i Trondheim. Fire demonstranter fra XR kom seg inn i DNBs kontorer hvor de ble værende frem til lokalene stengte og politiet ankom.

DNBs overordnede mål er å nå netto nullutslipp fra vår finansierings- og investeringsvirksomhet innen 2050. For å klare dette har vi satt delmål om å redusere utslippene vi finansierer fram mot 2030, samt finansieringsmål for bærekraftige aktiviteter. DNB er en internasjonal pådriver for bærekraftig omstilling og har vært tydelig på behovet for å bruke målene i Paris-avtalen som standard i dette arbeidet. Selv om DNBs ambisjoner er høye, samsvarer de ikke nødvendigvis med forventingene til klimabevegelsen. Grupperinger har både åpent gjennom sosiale medier og direkte til DNB formidlet at de vil fortsette sine direkte aksjoner mot konsernet til deres krav om endringer i DNBs bærekraftspolitikk er oppfylt.

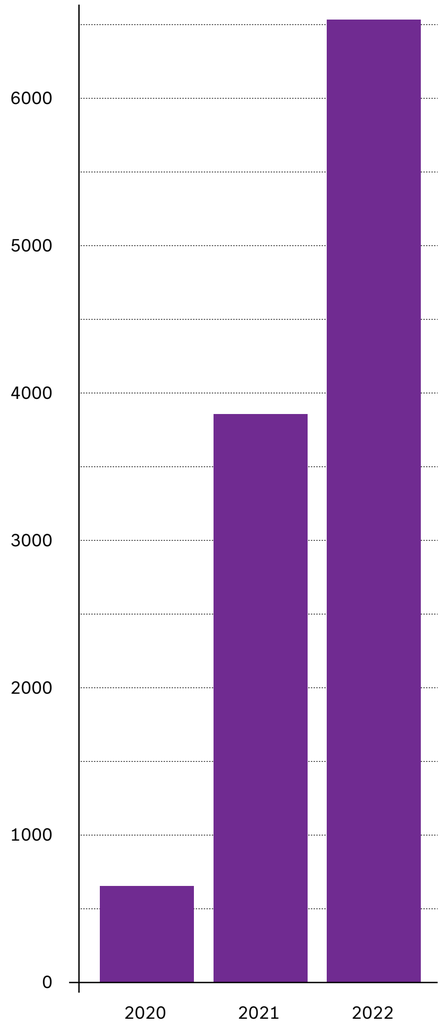
Bedrageri mot DNB

DNBs Financial Cyber Crime Center (FC3) opplyser i sin årsrapport for 2022 at det var totalt 6550 phishingtilfeller i løpet av året, noe som utgjør en økning på 69 % sammenlignet med året før. Fordi phishingangrep kan gjennomføres i massiv skala og i stor grad automatiseres, har flere og flere trussel-aktører gått over til å gjennomføre slike bedragerier. DNB anser phishingforsøk som en trussel mot DNB fordi vår merkevare ofte misbrukes til dette formålet, men også fordi mange av våre kunder utsettes for dette. Det er svært sannsynlig at trusselaktører vil fortsette å gjennomføre phishingangrep gjennom 2023, og det er ikke usannsynlig at 2023 kommer til å bli nok et rekordår.

Utsikter 2023-2024

Vi forventer at antall bedragerier mot DNB vil fortsette å øke gjennom 2023. Det er imidlertid utfordrende å si akkurat hvordan utviklingen vil være gjennom året. I lang tid har kriminelle aktører prioritert å gjennomføre phishingangrep på grunn av effektivitetsmulighetene som eksisterer, mens andre har misbrukt kredittprodukter for å finansiere annen kriminell virksomhet. Det er likevel meget sannsynlig at de kriminelle vil tilpasse seg samfunnet og finansinstitusjonene, og at nye bedrageriformer kan oppstå på kort varsel. Det er også sannsynlig at organiserte kriminelle vil fortsette å gjennomføre lånebedragerier mot banken for å finansiere annen alvorlig kriminalitet.

Phishing



Fortsatt høy andel av systematiske phishingangrep i digitale kanaler

Phishingforsøk spenner fra enkle SMS-meldinger som tilsynelatende kommer fra en legitim aktør med beskjed om å trykke på en lenke, til mer avanserte former for spearphishing hvor enkeltpersoner ringes opp med hensikt å manipulere dem til å gjøre noe i løpet av telefonsamtalen. Felles for all phishing er at de misbruker legitimiteten som en eksisterende organisasjon har bygget. Hvilken organisasjon som får merkevaren misbrukt varierer, men ofte har DNB og andre banker blitt misbrukt. Trusselaktørene velger som oftest organisasjoner med stor tillit i håp om at offeret lettere skal la seg lure. Framgangsmåtene er imidlertid like uavhengig av hvilken merkevare som misbrukes.

Organiserte kriminelle grupperinger med tilknytning til en rekke land i og utenfor Europa har i økende grad sett til phishing som verktøy for å gjennomføre bedragerier. Aktører som tidligere har fokusert på andre typer bedragerier gjennomfører heller phishing mot et stort antall ofre fordi det lønner seg i det store bildet. I stedet for å investere tid og krefter i å gjennomføre enkeltbedragerier mot spesifikke personer i kjærlighetsbedragerier eller lignende, er det mer effektivt å sende tusenvis av phishingmeldinger til et stort antall ofre i håp om at noen lar seg lure.

Til tross for at teleoperatørene gjør sitt for å stanse phishingmeldinger og vishinganrop, finner trusselaktørene stadig vekk nye måter å omgå kontrollmekanismene på. Dessuten tilpasser de kriminelle seg raskt og endrer gjerne metodene sine slik at de skal passe samfunnsutviklingen for øvrig. Det er også vanlig å rekruttere norskspråklige kriminelle for å gjøre språket i meldingene og anropene mer troverdig. Slike forhold gjør det utfordrende for mange å forstå at phishingmeldinger bare er forsøk på å lure dem. Med tanke på hvor lukrativt det er å gjennomføre phishingangrep kan trusselen med god sikkerhet klassifiseres som høy.

Organiserte kriminelle vil fortsette å gjennomføre lånebedragerier mot DNB og det er ingen grunn til å anta at de vil redusere aktiviteten sin i 2023. Organiserte kriminelle er kjent for å bruke lånebedragerier som en av flere metoder for å sikre inntekt som kan finansiere andre lovbrudd. Dette gjøres ofte ved misbruk av sårbare menneskers identitet, forfalskede lønnslipper eller annen manipulasjon av søknader.

Lånebedragerier gjennomføres av organiserte kriminelle for å finansiere annen kriminalitet

Både i Norge og Sverige har politiet pekt på knytninger mellom voldelig kriminalitet og bedragerier, og det ser ut til at voldelige kriminelle i større grad går vekk fra tradisjonelle tyverier og ran, til å heller begå lignende handlinger i det digitale rom. En slik utviklingen er likevel ikke oppsiktsvekkende med tanke på den digitaliseringen samfunnet har stått overfor i lang tid. Det er naturlig at kriminalitet beveger seg over på digitale flater i takt med at fysiske penger forsvinner. Enkelte kriminelle miljøer er kjent for å bruke grov vold for å oppnå sine mål. Slike metoder brukes også når disse miljøene begår bedragerier. For eksempel har det vært tilfeller der enkeltpersoner blir truet med vold om de ikke gir fra seg BankID-brikken sin til voldsutøver. Disse brikkene blir deretter brukt til å ta opp lån som senere blir misligholdt og fører til tap for banken. Samtidig blir pengene brukt til å finansiere grupperingenes øvrige aktiviteter, for eksempel i tilknytning til narkotikahandel. I tillegg til de store samfunnsmessige konsekvensene slik aktivitet har, bidrar det til å gjøre enkelt-personer til gjeldsslaver med de utfordringene det medfører.

Til tross for at organiserte kriminelle gjennomfører lånebedragerier er det også slik at opportunistiske enkeltindivider gjennomfører lånebedragerier. Under Covid-19 så vi at enkelte gjennomførte bedragerier tilknyttet de statlige støtteordningene som ble lansert for å hjelpe norsk næringsliv. Disse støtteordningene var tillitsbaserte og ble tilbudt av enkelte norske banker på vegne av norske myndigheter. For bankene er konsekvensene av slike bedragerier av begrenset art, men for samfunnet er det et stort tillitsbrudd. Nå som vi er inne i nye perioder med økonomisk ustabilitet og uvanlig høye strømpriser, har norske myndigheter igjen lansert en støtteordning som skal hjelpe det norske næringslivet med økte strømutgifter. Det er sannsynlig at enkelte vil forsøke å gjennomføre bedragerier også med denne støtteordningen selv om omfanget sannsynligvis vil være begrenset. Samtidig vil det alltid være slik at enkelte ønsker å tjene ekstra penger ved å misbruke slike tillitsbasert ordninger, slik at problemet vil eksistere også neste gang en tilsvarende støtteordning lanseres.

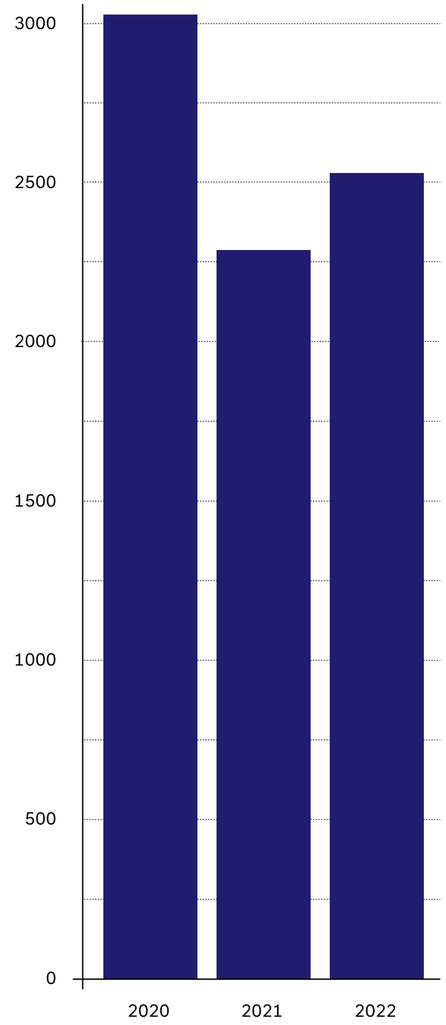
Bedrageri mot DNBs kunder

DNBs Financial Cyber Crime Center (FC3) registrerte i 2022 stabile nivåer av bedragerier med emosjonell manipulasjon. Emosjonell manipulasjon er et samlebegrep for bedragerier hvor de kriminelle misbruker personlige forhold og spiller på offerets emosjonelle reaksjon på kontakt. Eksempler inkluderer kjærlighetssvindel, investeringssvindel og saker som ofte omtales som Nigeriasvindel. Til tross for at alle bedragerier misbruker sårbarheter hos offeret, har disse bedrageriene til felles at de ofte trenger dypere inn i sinnet til den som blir bedratt. Det er svært sannsynlig at kriminelle vil fortsette å gjennomføre slike bedrageri også i 2023.

Utsikter 2023-2024

I likhet med bedragerier mot DNB forventer vi at antallet bedragerier mot DNBs kunder vil fortsette å øke gjennom 2023. Til tross for at det er utfordrende å predikere hvordan utviklingen vil være, er det meget sannsynlig at kriminelle vil fortsette å misbruke menneskers følelsesliv på samme kyniske måter som de har gjort til nå. Det er også meget sannsynlig at kriminelle aktører vil nyttiggjøre seg den teknologiske utviklingen vi står overfor og at de vil tilpasse seg samfunnsutviklingen etter hvert som endringer skjer. Det er sannsynlig at vi i løpet av 2023 i større grad vil se bedragerier som tar i bruk kunstig intelligens, maskinlæring og andre teknologiske nyvinninger enn det som har vært vanlig til nå. Eksempelvis kan vi forvente økt bruk av både språkmodellering og deepfakes for å automatisere kommunikasjon med ofre i investerings- og kjærlighetsbedragerier, eller til å manipulere ansatte i bedrifter til å gjennomføre illegitime betalinger.

Emosjonell manipulasjon



Hybride bedragerier tar over for mer tradisjonelle bedrageriformer

I lang tid har emosjonell manipulasjon vært en foretrukket bedrageriform, men i dag gjennomfører kriminelle i økende grad masseproduserte phishingangrep nettopp fordi dette ofte oppleves som mer effektivt. Til tross for en liten nedgang de siste årene er det ingen grunn til å anta at antall bedragerier med emosjonell manipulasjon vil synke, nettopp fordi de kriminelles avkastning kan bli stor dersom de klarer å manipulere offeret i tilstrekkelig grad og over lang nok tid. Samtidig er det sannsynlig at enkelte aktører vil gjennomføre phishingangrep som et tillegg til de øvrige bedrageriene de utfører. Som belyst under "Bedragerier mot DNB" skyldes dette sannsynligvis at phishingangrep anses som relativt enkle å gjennomføre. Det kan derfor resultere i at antallet phishingsaker fortsetter å øke, mens øvrige bedragerityper forblir på stabile nivåer.

Når det gjelder investeringsbedragerier er det fortsatt slik at falske investeringsplattformer for kryptovaluta dominerer bedragerisakene, men det forekommer også aktiviteter relatert til falsk mining av kryptovaluta og bruk av komplekse investeringsinstrumenter. Investeringsbedragerier er imidlertid en bedrageriform som blir særlig lett påvirket av samfunnsutviklingen for øvrig. Hver gang det skjer store hendelser i verdensøkonomien blir også det legitime kryptovalutamarkedet påvirket. Dette fører til at kriminelle bruker ekte informasjon til å manipulere ofrene sine i falske historier. Nå som vi er i en periode med økonomiske nedgangstider er det sannsynlig at kriminelle vil endre sin taktikk og framgangsmåte, men det vil uansett finnes ofre som er mottakelige for falske investeringsråd eller lovnader om rask profitt. Til tross for varierende antall saker de siste årene er det usannsynlig at vi vil se en nedgang i antall investeringsbedragerier. Den variasjonen som er synlig fra år til år kommer av naturlige sesongvariasjoner og skyldes at de kriminelle til enhver tid fokuserer innsatsen sin på de mest lønnsomme bedrageriformene.

Emosjonell manipulasjon inkluderer blant annet kjærlighets- og investeringsbedragerier. Her trenger bedrageren dypere inn i følelseslivet til offeret og framgangsmåten oppleves derfor mer invaderende.

En interessant utvikling er likevel at bedrageriformene i større grad kombineres i det som kan kalles hybridbedragerier. Eksempelvis ved å kombinere kjærlighets- og investeringsbedragerier. Som oftest innynder bedragerne seg hos offeret og overøser dem med kjærlighet. Når tillit er opprettet er

det mindre sannsynlig at offeret reagerer på bedragerens utsagn. Da kan bedrageren slå til og presentere fantastiske investeringsmuligheter, det er jo tross alt enklere å ta imot investeringsråd fra noen man stoler på. Den investeringen som presenteres er imidlertid ikke reell og er som oftest tilknyttet en falsk investeringsplattform som bedrageren styrer i bakgrunnen.

Selv om akkurat denne formen for bedrageri er relativt ny, er det ikke uvanlig for trusselaktørene å være kreative i utførelsen av bedragerier. Det er god grunn til å anta at neste års rapport vil inneholde en helt ny bedrageriform som ikke enda er kjent.

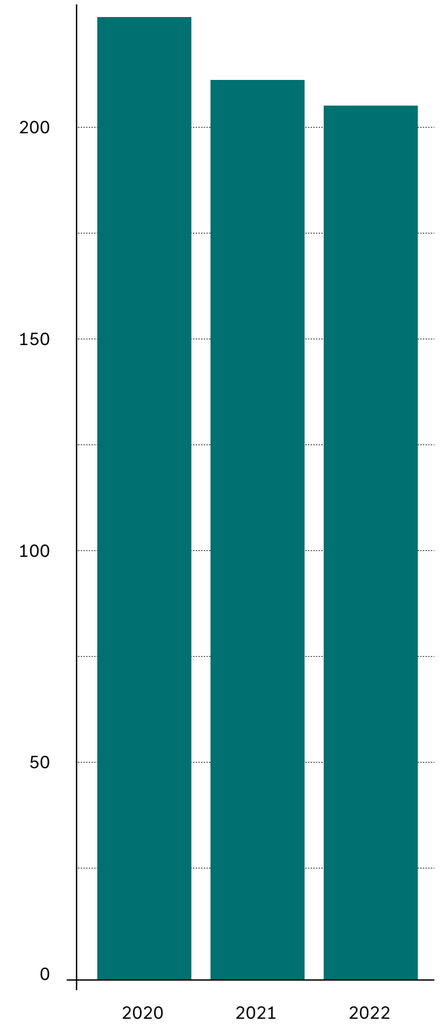
CEO- og BEC-bedragerier utgjør fortsatt en høy trussel mot bedrifter

De siste årene har DNBs Financial Cyber Crime Center (FC3) sett en minimal reduksjon i antall saker med bedragerier mot bedrifter. Denne nedgangen er mest sannsynlig tilfeldig eller beror på interne forhold. Andre steder i verden er det fortsatt svært høye nivåer av slike bedragerier, og det er ingen grunn til å tro at kriminelle vil redusere innsatsen mot nordiske bedrifter nevneverdig. Det er derfor svært sannsynlig at bedrifter kommer til å bli utsatt for både enkle og avanserte bedragerier i nær framtid.

DNB erfarer at mange av de trusselaktørene som begår bedragerier mot bedrifter er forskjellige fra de som begår bedragerier mot privatpersoner. Det er imidlertid ikke uvanlig at enkelte aktører gjennomfører bedragerier mot begge typer av ofre, og at disse i perioder kan prioritere å gjennomføre angrep mot enten den ene eller den andre gruppen slik at det fører til en opplevd økning i antall saker hos én gruppe og en opplevd nedgang i den andre. For disse aktørene er det naturlig å til enhver tid rette angrepene sine mot den gruppen som framstår mest lukrativ, noe som innebærer at de kan veksle mellom ulike typer av ofre og ulike bedragerimetoder.

De enkleste formene for bedriftsbedragerier er såkalte direktørsvindler (CEO fraud). Disse kan i utgangspunktet sammenlignes med Nigeriabrev rettet mot bedrifter. Her sendes masseproduserte eposter til utallige mottakere i håp om at noen lar seg lure. Mer avanserte former for bedriftsbedragerier har grensedragninger

Bedrageri mot bedriftskunder

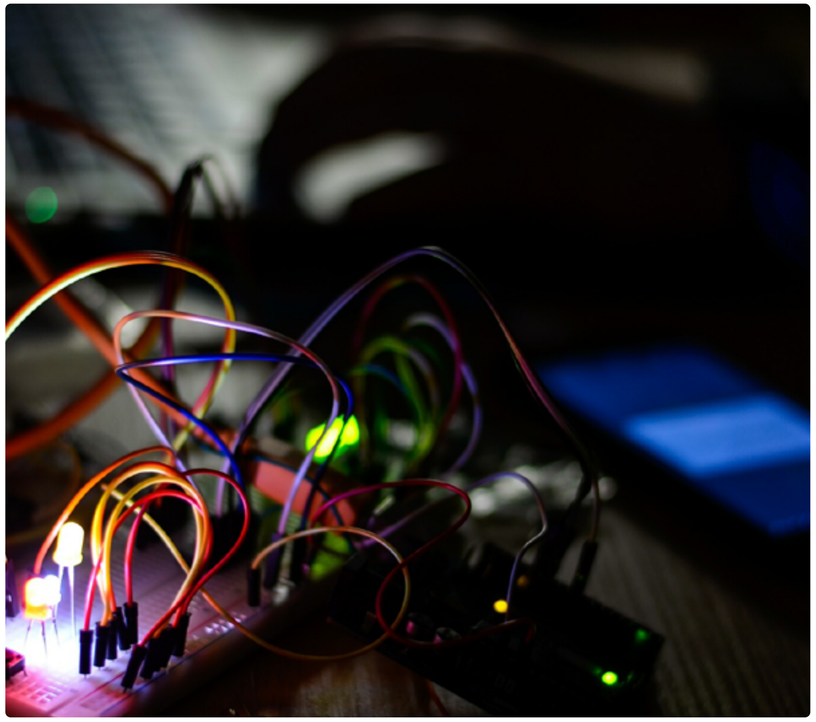


mot andre typer cyberkriminalitet og omtales som Business Email Compromise (BEC). I BEC-bedragerier må trusselaktøren først få tilgang til epostsystemene til en reell organisasjon. Når dette er oppnådd, får aktøren frie muligheter til å overvåke epostkommunikasjon, kartlegge samarbeidspartnere og sende eposter med falskt innhold, ofte uten å bli oppdaget. BEC forutsetter en viss grad av teknologisk kompetanse og er gjerne forbundet med mer avanserte trusselaktører. Fordi bedrageriformen er ressurskrevende kan det være at enkelte trusselaktører i perioder går over til enklere bedrageriformer for å oppnå sine mål.

Kriminelle kan utnytte nye digitale innovasjoner til å begå bedragerier

Den siste tiden har avanserte verktøy som bruker kunstig intelligens blitt tilgjengeliggjort for alle som bruker internett. Tjenester som OpenAIs ChatGPT, Microsofts Bing og GooglesBard gjør at alle kan få tilgang til sofistikerte språkmodeller som er i stand til å formulere meningsfulle ytringer på egenhånd. Til tross for at bruk av chatboter i kriminell virksomhet krever visse teknologiske ferdigheter og på ingen automatisk måte kan brukes til bedragerier, er det slik at enkelte kriminelle har begynt å eksperimentere med dette allerede.

I tidligere vurderinger har trusselen fra deepfake-teknologi blitt belyst. Trusselen eksisterer fortsatt og har sannsynligvis økt. Flere og flere trusselaktører får øynene opp for mulighetene teknologi gir, og gjør stadig mer for å bruke dette til å effektivisere bedragerier. For ofrene blir det i praksis svært utfordrende å forstå at de blir lurt når de både ser og hører videosamtaler av det som framstår som en ekte person. Oppå dette diskuterer «personen» levende og besvarer alle tenkelige spørsmål. Selv om bruken av slike verktøy har vært begrenset i bedrageriverden til nå, vil hver eneste teknologiske utvikling gjøre at teknologien blir mer og mer tilgjengelig for kriminell virksomhet.



Bedrageri mot DNB Livsforsikring

Det har vært et normalt tilfang av svindelsaker i 2022 sammenlignet med tidligere år. Den største andelen av avdekkede svindelsaker lå innen yrkesskadeforsikringer, men mot slutten av året så selskapet en økning i svindel-forsøk også innen uføreforsikringer i bedriftsmarkedet. Denne trenden har fortsatt inn i 2023. Det er ikke avdekket sofistikerte angrep eller tilfeller der organiserte kriminelle har utnyttet DNB Livs produkter til svindel.

Utsikter 2023-2024

Bedrageritrusselen mot DNB Liv vil fortsatt være høy i 2023 og det vurderes som sannsynlig at selskapet vil oppleve en økning av svindelforsøk som følge av økonomiske nedgangstider. DNB Livs produkter er antakelig ikke like enkle å utnytte til svindel som tingskadeforsikringer, men vi anser det som sannsynlig at enkelte ansatte i hardt rammede bedrifter vil forsøke å utnytte ulykkes- eller uføreforsikringer da disse kan gi høyere utbetalinger enn arbeidsledighetstrygd. Det vurderes som meget sannsynlig at det er «vanlige kunder» som vil stå bak de aller fleste forsøkene på forsikringssvindel mot DNB Liv i 2023. Det vurderes som lite sannsynlig at DNB Liv vil bli rammet av sofistikerte forsikringssvindel fra kriminelle miljøer.

Antall svindelsaker innen yrkesskadeforsikringer er trolig høyere enn hva som avdekkes

De avdekkede metodene for svindelforsøk innen yrkesskadeforsikringer er tilsynelatende de samme som tidligere år:

- Kunden dikter opp hendelsesforløpet for en ulykkeshendelse som ikke har funnet sted. Hensikten er å få en urettmessig erstatningsutbetaling for helseplager som skyldes andre forhold enn en yrkesskade og som reelt ikke ville ha gitt noen utbetaling.
- Kunden overdriver bevisst helseplagene etter en reell yrkesskade i den hensikt å få utbetalt en større erstatning.
- Kunden endrer på sin forklaring om et hendelsesforløp i den hensikt å unngå en avkortning i erstatningen.

Ca. 0,3 % av yrkesskadesakene som meldes til DNB Liv hvert år blir avslørt som svindel. Det er ikke foretatt noen analyse av hva den reelle andelen av svindel innen dette forsikringsproduktet er, men det er en antakelse i bransjen at ca. 10 % av alle erstatningskrav innenfor yrkesskader er forsikringssvindel. Finans Norge vil i 2024 igangsette en mørketallsundersøkelse for å få mer kunnskap om det reelle omfanget i Norge.

Personer svindler fastlegen, NAV og forsikringsselskapet for å få utbetaling fra uføreforsikring

De fleste svindeltilfellene som blir avdekket innen uføreforsikringene på bedriftsmarkedet er saker hvor kunden tilsynelatende har lurt både fastlegen sin og NAV for å få innvilget utbetalinger for arbeidsuførhet. DNB Livs saksbehandlere har en rekke ganger avdekket at kunder likevel arbeider for fullt, ofte i egne eller nær families bedrifter. Dette avdekkes vanligvis ved kontroll opp mot foretaksregisteret og andre åpne kilder på internett.

Økonomiske nedgangstider kan gi økt svindel

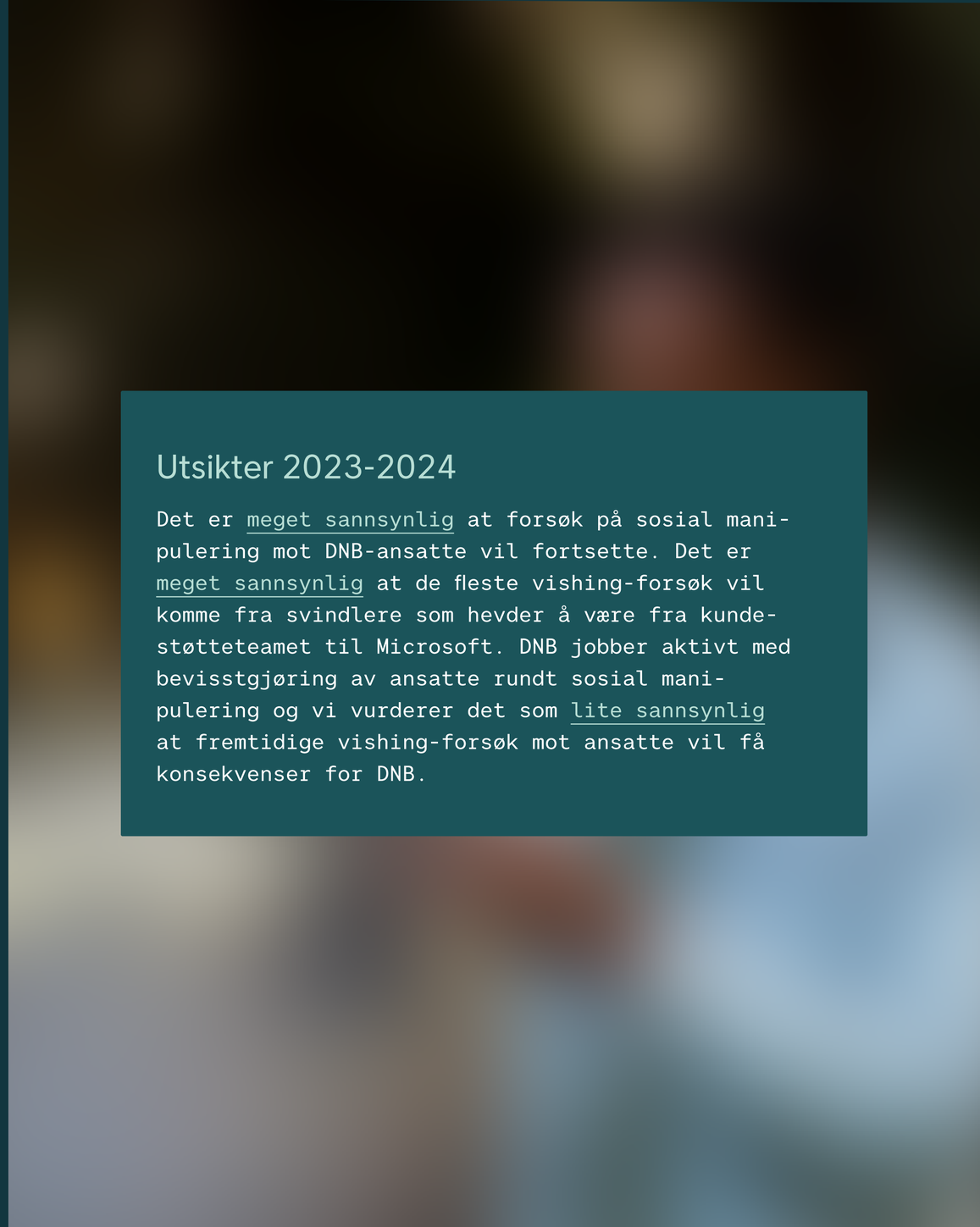
Norge og verden ellers har gått fra krise til krise de siste årene med blant annet pandemi, krig i Ukraina, økte energikostnader og inflasjon. Dette har for mange privatpersoner og bedrifter medført store økte kostnader. Flere europeiske forsikringsselskap meldte mot slutten av 2022 om store økninger i avdekket svindel som følge av økonomiske nedgangstider. Et av de største advokatfirmaene i England omtalte i januar 2023 denne situasjonen som «a pandemic of fraud».

Norge er ikke like hardt rammet av nedgang i økonomien som andre vestlige land, men forsikringsselskapet Fremtind, som delvis eies av DNB, har ved flere anledninger i 2022 meldt om en økning i antall svindelsaker som følge av at kundene får en mer presset økonomi. De forventer en videre økning innen forsikringssvindel også i 2023.

Vishing og kartlegging

DNB-ansatte opplever stadig å bli utsatt for forsøk på sosial manipulering. Selv om phising-saker er mest omfangsrike i denne kategorien, skjer det også særlig i form av vishing. Det har vært en økning i vishing-saker sammenlignet med 2021 og det er primært «Microsoft-svindlere» som kontakter de ansatte. Samtidig er det flere eksempler der ukjente aktører ringer til DNB ansatte med det formålet om å tilegne seg opplysninger om andre ansatte i DNB.

«Vishing» eller «voice phishing» er når svindlere prøver å få tak i sensitiv informasjon ved å starte kontakt via telefonsamtaler



Utsikter 2023-2024

Det er meget sannsynlig at forsøk på sosial manipulering mot DNB-ansatte vil fortsette. Det er meget sannsynlig at de fleste vishing-forsøk vil komme fra svindlere som hevder å være fra kundestøtteteamet til Microsoft. DNB jobber aktivt med bevisstgjøring av ansatte rundt sosial manipulering og vi vurderer det som lite sannsynlig at fremtidige vishing-forsøk mot ansatte vil få konsekvenser for DNB.

Ansatte blir utsatt for vishing-forsøk, uten at det fører til konsekvenser

I de fleste vishing-saker er det personer som utgir seg for å ringe fra en teknisk avdeling i Microsoft og opplyser om «kritiske feil». Microsoft-svindlere har holdt på i flere år og er nå et velkjent bedragerifenomen som DNB-ansatte har god kjennskap til og som ikke har resultert i noen form for kompromitteringer av personell eller systemer. I andre saker blir DNB-ansatte oppringt av ukjente aktører som ønsker å få opplysninger om andre ansatte. Informasjonen som det ofte blir bedt om er stilling, e-postkonto, telefonnummer mm.

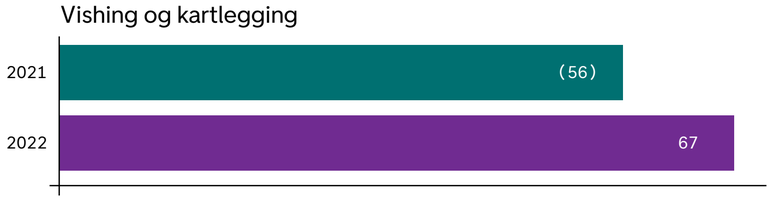
Ved flere anledninger i 2022 har aktører gjennom voice-phising forsøkt på å få opplysninger om en konkret divisjonsdirektør i DNB. Ved et tilfelle ringte en person med britisk telefonnummer til en DNB-ansatt og utga seg for å være en representant fra «Den europeiske sentralbanken». Vedkommende ønsket informasjon om ni ansatte som jobbet innen risikomiljøet til DNB i Norge, Storbritannia og Finland. Vedkommende ønsket først kontaktinfo og etter å ha blitt avvist ønsket vedkommende bekreftelse på at personene var ansatt i spesifikke stillinger. Flere av vishing-forsøkene har vært rettet mot ansatte som jobber innen risikomiljøet.
Det er trolig at denne type sosial manipulering og innhenting av informasjon om ansatte gjøres som en forberedelse til et fremtidig spearphishing-angrep enten mot DNB eller en tredjepart. Å hacke et system med kun teknisk tilnærming kan ta lang tid. Med sosial manipulering kan dette være mulig på minutter. Kriminelle aktører kan også ha som hensikt å kartlegge ansatte for å finne de i DNB som har tilgang til systemer og verdier som kan være med på å tilrettelegge for aktørenes kriminelle aktiviteter.

Et lite sannsynlig, men fortsatt reelt scenario er at statlige aktører prøver å kartlegge DNB. Utenlandske etterretningstjenester legger betydelige ressurser i å rekruttere kilder. Gjennom kartleggingen vil man forsøke å finne en person eller personer som har, eller som kan få tilgang på eller har kjennskap til verdiene aktøren søker. Dette er opplysninger som aktøren kan bruke til å finne potensielle mål for en rekrutteringsoperasjon. Etterretning av indirekte nytte som kontaktopplysninger og roller til ansatte, informasjon om prosjekter, samarbeidsnettverk, underleverandørkjeder og IT-systemer, kan også benyttes videre med den hensikt å få tilgang til konfidensiell informasjon.

DNB kan være et mål for utenlandsk etterretning

Norske sikkerhets- og etterretningstjenester har gjentatte ganger fremhevet trusselen om industrispionasje mot norske bedrifter. Å vurdere hvor sannsynlig etterretningstrusselen mot DNB er vil bære preg av stor usikkerhet og være basert på antakelser. Samtidig vurderer vi at DNB kan være et reelt mål for utenlandsk etterretning. Flere statlige aktører kan ha ulike formål og interesse av å innhente informasjon, kartlegge og sondere sårbarheter i DNB.

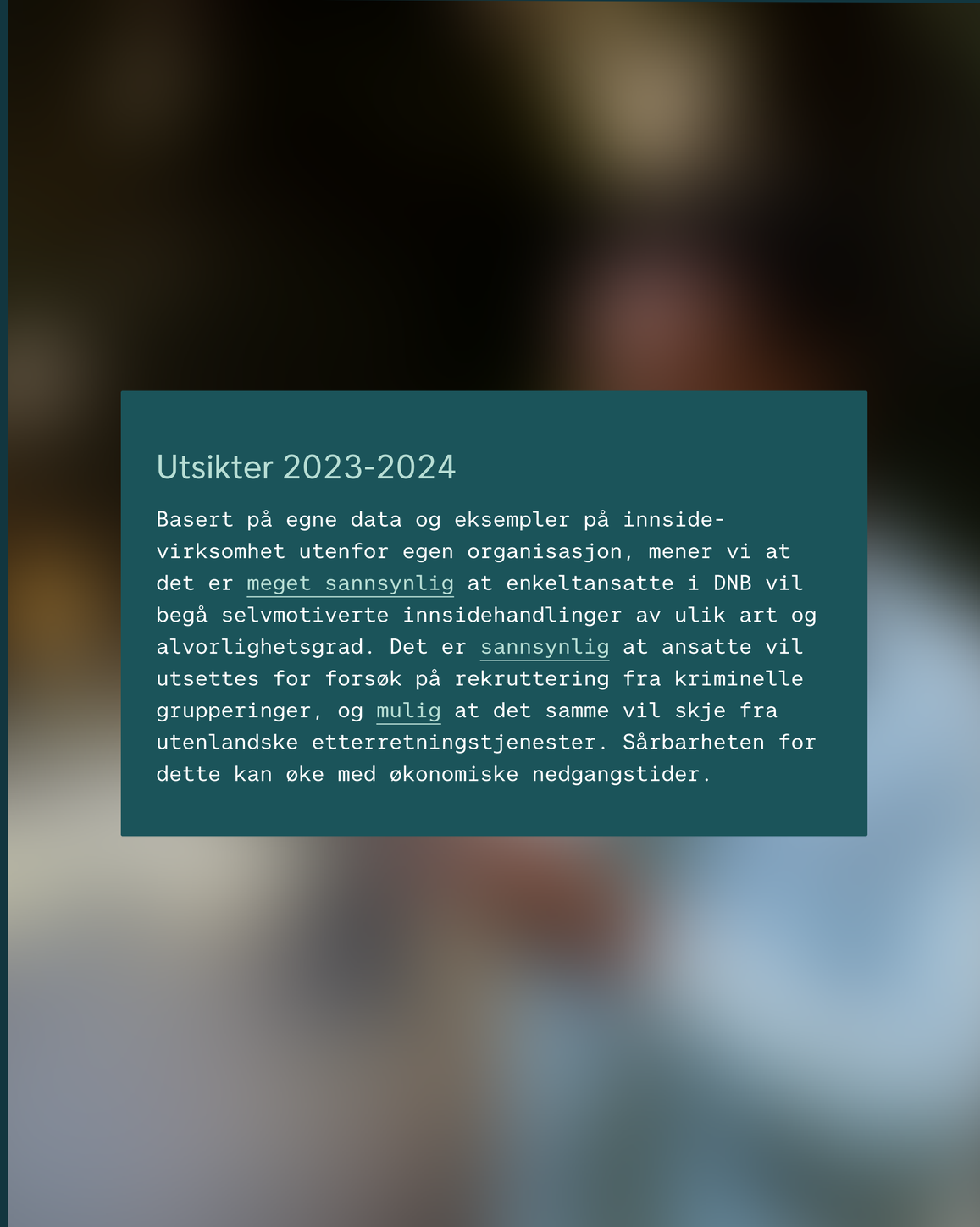
Som Norges største bank og oppgjørsbank forvalter DNB store verdier på vegne av samfunnet og vi utgjør en viktig del av samfunnets funksjonalitet. Forstyrrelser i DNBs finansielle tjenester kan føre til økt uro og problemer i hverdagen til befolkningen, samt skade viktige samfunnsinteresser. Detaljer om infrastruktur og sikkerhetsordninger kan være av interesse for stater som søker å påvirke driften av DNB eller til og med å lamme den under en krise eller en «synkronisert angrepspakke»[1]. I tillegg besitter DNB sensitiv informasjon om selskaper og personer som noen fremmede makter kan se verdien av. Slik informasjon kan for eksempel benyttes i forbindelse med forbigåelse av sanksjoner eller for å gi fortrinn til og bistå eget næringsliv.



[1]Cullen. P & Reichborn-Kjennerud, E. (2017). Understanding Hybrid Warfare. The Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare Project (Norsk utenrikspolitisk institutt, NUPI).

Innsidevirksomhet

Innsidetrusselen er mangfoldig og kan manifestere seg på ulike måter. Den kan utspille seg ved at den ansatte selv har en motivasjon eller ved at eksterne trusselaktører forsøker å benytte seg av ansatte for å nå sine mål. DNB besitter som Norges største bank ettertraktede verdier i form av blant annet informasjon, systemer, finansielle midler og fullmakter. For eksterne trusselaktører kan det være verdifullt å ha en tilrettelegger «på innsiden» av banken. DNBs verdier kan også være attraktive for selvmotiverte innsidere som er villige til å begå kriminelle handlinger for egen økonomisk vinning, ideologisk overbevisning eller som hevn.



Utsikter 2023-2024

Basert på egne data og eksempler på innside-virksomhet utenfor egen organisasjon, mener vi at det er meget sannsynlig at enkeltansatte i DNB vil begå selvmotiverte innsidehandlinger av ulik art og alvorlighetsgrad. Det er sannsynlig at ansatte vil utsettes for forsøk på rekruttering fra kriminelle grupperinger, og mulig at det samme vil skje fra utenlandske etterretningstjenester. Sårbarheten for dette kan øke med økonomiske nedgangstider.

Selvmotiverte innsidere motiveres oftest av økonomisk fortjeneste

Finansbransjen er en utsatt bransje for innsidehandlinger. Størsteparten av innsidehandlingene er selvmotiverte og gjort for å oppnå økonomisk vinning. Faktorene er ikke statiske og kan påvirkes av både interne forhold ved personen selv og av eksterne forhold. Bakenforliggende årsaker kan være ideologi, hevn, ego og penger.

Det siste året har prisene på mat, strøm, drivstoff og renter økt. Ansatte i DNB påvirkes av de samme økningene i levekostnader som andre, spesielt ansatte som allerede har en anstrengt økonomisk situasjon. Det er ikke gitt at økonomiske vansker i alle tilfeller vil medføre at ansatte i DNB begår innsidehandlinger, men for enkelte kan det gi ytterligere insentiver for å begå innsidehandlinger for økonomisk vinning. For stillinger med resultatbasert lønn og bonusordninger, vil dette også kunne gi et insentiv for å øke egen produktivitet, for eksempel ved å bidra til lånebedragerier.

En annen side ved økonomiske nedgangstider er at de kan resultere i besparelser hos arbeidsgiver i form av lønn, bonuser, reiser og andre goder. Omstendigheter på en arbeidsplass som oppfattes som negative for den ansatte kan være en motivasjonsfaktor som fører til innsideaktivitet. Særlig hvis dette kommer i tillegg til personlige problemer og andre stressorer.

De vanligste innsidehandlingene medfører ikke store konsekvenser for DNB

Ansatte har i kraft av sine roller og oppgaver i DNB flere tilganger som kan misbrukes til egen vinning. Sannsynligste scenario er ansatte som tar med seg informasjon videre til ny arbeidsgiver for å skaffe seg en fordel i ny stilling. DNB har hatt flere slike saker til utredning for siste året og det er sannsynlig at det vil oppstå nye saker det kommende året. Dette er saker som hver for seg ikke utgjør store operasjonelle konsekvenser for DNB.

Ved flere anledninger i 2022 har DNB utredet saker hvor det har vært rutinebrudd vedrørende e-takster på eiendommer. Det er ulike grunner til dette, men en stor andel av saker viser at det har vært tette bånd mellom kunden og eiendomsmegleren. Den direkte økonomiske profitten ved slike handlinger vil være hos kunden som får e-taksten. Eiendomsmegleren vil imidlertid oppnå en utilbørlig fordel gjennom å tilrettelegge for en person vedkommende har en relasjon til.

Ansatte kan også være motivert av misnøye og et ønske om å hevne seg på arbeidsgiver. Av saker fra andre virksomheter vet vi at ansatte med slike intensjoner kan utgjøre et svært stort skadepotensial. I løpet av det siste året har DNB hatt en hendelse hvor en misfornøyd ansatt utførte handlinger for å skade funksjonaliteten i våre datasystemer. Hendelsen fikk begrensede skadefølger som følge av gode deteksjons- og håndteringsrutiner. DNB har mekanismer for å motvirke slik atferd, som tilgangsstyring og rutiner for offboarding av ansatte.

Organiserte kriminelle vil ønske å påvirke og rekruttere ansatte

For innsidevirksomhet som involverer eksterne kriminelle aktører, anser DNB det som sannsynligste scenario at ansatte tilrettelegger for lån på falskt grunnlag eller for hvitvasking. Ofte vil det være en personlig relasjon mellom aktørene. Økokrim har tidligere trukket frem at det har vært tette bånd mellom kriminelle og personer «på innsiden» i saker der profesjonelle aktører har tilrettelagt for kriminell virksomhet. Aktørene har ofte hatt et langvarig bekjentskap og samarbeid over flere år.

Flere store norske banker har opplevd straffesaker mot ansatte for korrupsjon og bedrageri siste året, herunder også DNB, hvor tilrettelegging for kriminell aktivitet har vært likhetstrekk. Det er likevel ikke kun med henblikk på hvitvasking og bedragerier kriminelle grupper kan motiveres til å rekruttere innsidere i DNB. Tilgang til DNBs IT-infrastruktur er også et potensielt mål for flere cyberkriminelle aktører. 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 å utføre angrep med krypteringsvirus.

Enkelte ansatte har forhøyet risiko for innsidevirksomhet

I DNB finnes ansatte med eleverte tilganger og finansielle fullmakter. Disse ansatte vil i kraft av sine tilganger kunne påføre DNB større skade ved enkelthendelser, uavhengig om motivasjonen til disse er økonomisk vinning, hevn eller annet. Eksempler på slike roller kan være administratorer på datasystemer, eller ansatte innen finans med vide fullmakter.

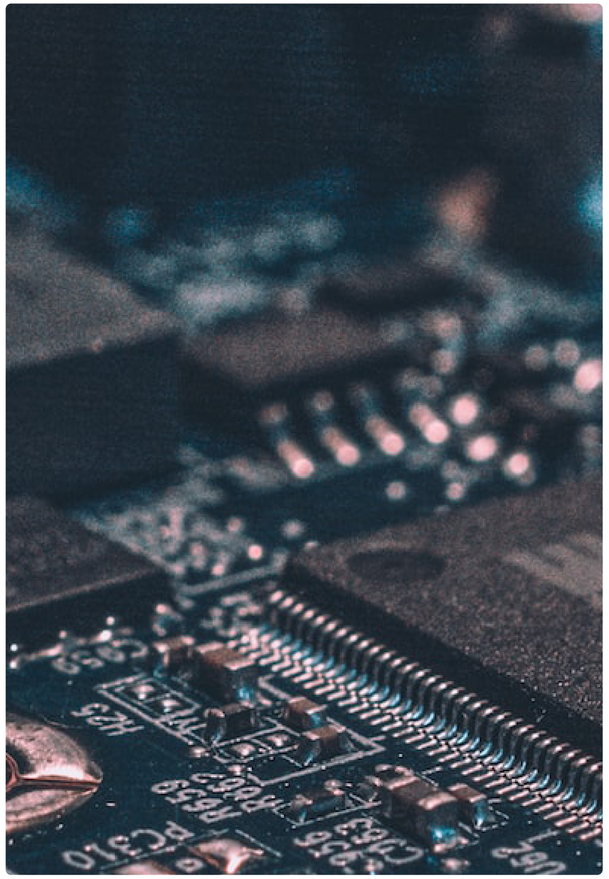
Videre er DNB et konsern med et stort mangfold blant sine ansatte og med kontorer i flere land. Dette er en viktig del av DNBs virke, samtidig som at det er kjent at flere lands etterretningstjenester utøver press overfor egne borgere bosatt i andre land. Dette kan handle om at borgere av autoritære stater blir presset til samarbeid eller til å utlevere informasjon gjennom press mot slektninger og familie. De innrapporterte tilfellene av forsøk på sosial manipulering indikerer at DNB er et attraktivt mål for ulike trusselaktører. Det er også 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. PST trekker i sin årlige trusselvurdering frem at land som Russland, Kina, Iran og Nord-Korea vil utgjøre en etterretningsmessig trussel mot norske virksomheter det kommende året, og at en ikke trenger å ha tilgang til gradert informasjon for å være attraktiv.

DNB har enkeltansatte som er fra andre land, som kan være mer sårbar for slik tilnærming. DNB har innført risikoreduserende tiltak for å redusere risikoen knyttet til disse. For DNB handler ikke dette om mistenkeliggjøring av ansatte, men at man som arbeidsgiver har et ansvar for å håndtere den risikoen som ansatte utsettes for gjennom sitt arbeid.

Tema

Internasjonale sanksjoner

Antallet og omfanget av internasjonale sanksjoner er raskt økende – spesielt som en følge av Russlands krig i Ukraina. Forholdet mellom økonomiske stormakter preges også av at politiske interesser i økende grad veier tyngre enn økonomiske hensyn, noe som senker terskelen for å innføre sanksjoner og andre handelsrestriksjoner. Dette innebærer at utfordringene og usikkerheten blir større for både DNB og våre kunder.



Banken som et viktig apparat i håndhevingen av sanksjonsregimet

DNB legger betydelig innsats i transaksjonsovervåkning for å forhindre at banken utfører betalinger i strid med internasjonale sanksjoner. Trusselen om eksplisitte sanksjoner mot DNB er lav, men samtidig er utviklingen preget av uforutsigbarhet og endringer i høyt tempo.

Sanksjoner benyttes for å straffe handlinger som bryter med etablerte normer og regler, eller for å hindre utvikling som kan true internasjonal fred og sikkerhet. Det er derfor en viktig del av bankenes samfunnsansvar å påse at sanksjonerte regimer, personer og selskaper ikke får tilgang til midler de ikke skal ha. Når pengestrømmer stanses og midler fryses, blir kostnaden ved å utføre uakseptable handlinger høy.

Finansinstitusjoner har også en lovpålagt plikt til å etterleve sanksjoner. Mens alle land og dermed alle finansinstitusjoner er folkerettslig forpliktet til å følge FN-sanksjoner, blir også det meste av EUs sanksjoner innlemmet i norsk lov. Banker kan bli strafferettslig ansvarlige dersom forpliktelsene ikke overholdes. I tillegg har enkelte av de amerikanske sanksjonsregimene ekstraterritoriell rekkevidde, det vil si at de også gjelder for ikke-amerikanske aktørers handlinger. Det innebærer at amerikanske, unilaterale sanksjoner også legger føringer for hvordan DNB håndterer internasjonale betalinger.

Sanksjoner benyttes som politisk verktøy

Når sanksjoner innføres som straffereaksjon, som over Russlands krig i Ukraina, henger sanksjonsbruken sammen med sikkerhetspolitiske hensyn. Det skal straffe seg å bryte allment aksepterte regler for hvordan stater forholder seg til hverandre. I andre sammenhenger, som når EU innfører sanksjoner som følge av brudd på menneskerettigheter, er virkemiddelbruken knyttet til et utenrikspolitisk verdigrunnlag.

Det er samtidig flere eksempler på at årsaken bak sanksjonsbruk er knyttet til strategiske og politiske interesser, og at sanksjoner dermed benyttes som et verktøy for geopolitisk posisjonering. Stater innfører restriksjoner mot andre stater for å hindre utviklingen av bestemte militære kapasiteter og for å beholde teknologiske fortrinn, eller som reaksjon på det sanksjonerte landets politikkutøvelse.

Et eksempel på det første er et økende antall amerikanske restriksjoner mot kinesiske teknologiselskap. Et eksempel på det siste er Kinas boikott av Litauen, og press mot andre europeiske selskap hvor litauiske produkter inngår i verdikjeden. Bakgrunnen var en tiltakende politisk konflikt mellom Kina og Litauen, blant annet som følge av at Taiwan i 2021 åpnet et representasjonskontor i Vilnius.

Økende kompleksitet skaper utfordringer for finansinstitusjonene

Utviklingen innebærer en rekke utfordringer for DNB og andre finansinstitusjoner. For det første er det en nær eksplosiv økning i bruken av dette virkemiddelet. Nye sanksjoner innføres på kort varsel. Som eksempel er det etter invasjonen av Ukraina i 2022 innført en lang rekke sanksjonspakker fra ulike hold mot Russland, og ytterligere sanksjoner forberedes fortløpende. Sanksjonsregimene er preget av økende kompleksitet. Dette er blant annet knyttet til at EU-landene, som forhandler om sanksjonspakkene, søker å begrense effekten av sanksjoner på egne økonomier.

For det andre er bruken av sanksjoner knyttet til en pågående reorientering av globale handelsmønstre, hvor sikkerhets- og geopolitiske hensyn vektes mot, og i mange tilfeller veier tyngre enn, økonomiske interesser. Posisjonen til institusjoner som setter premissene for samhandling mellom stater reduseres. Eksempelvis har betydningen av Verdens Handelsorganisasjon (WTO) lenge vært svekket som følge av lammelse av organisasjonens appellorgan, mens de mest truende konfliktene i dag involverer medlemmer med vetomakt i FNs sikkerhetsråd. Når betydningen av slike institusjoner reduseres, tar stater unilaterale verktøy i bruk for å forfølge sine interesser. Nettopp sanksjoner, eksportkontroll og andre former for restriksjoner er slike unilaterale virkemidler. Dette medfører økende uforutsigbarhet både for finansaktører som DNB og for våre kunder.

For det tredje er ekstraterritorielle sanksjoner en særegen utfordring. I tillegg til at USA benytter dette virkemiddelet, viser også Kina økende vilje til å rette sanksjoner mot tredjeparter. Den kinesiske sanksjonslovgivningen er svært vidtrekkende, og bruken er uforutsigbar. Etter at kinesiske myndigheter i 2021 reviderte sanksjonslovverket og innførte bestemmelser om såkalte «blocking statutes» overfor andre lands sanksjoner mot Kina, kan næringslivsaktører som opererer i landet bli tvunget til å ta et valg mellom fortsatt aktivitet i Kina, eller å fortsette aktivitet knyttet til det sanksjonerende landet.

Tredjeparter risikerer dermed å bli trukket inn i de tiltakende spenningene mellom økonomiske stormakter.

Bankens kunder påvirkes indirekte av sanksjonene

Sanksjoner påvirker i høyeste grad også DNBs kunder. Som eksempel er det i henhold til EUs sanksjoner og norsk lov forbudt å eksportere luksusvarer over visse verditerskler til Russland. Slike sanksjoner likner i stor grad eksportkontrollregler, som i sin tur er et svært omfattende og detaljert regelverk. Her påligger det i første rekke våre kunder et ansvar for å påse at eksporten kan gjennomføres i henhold til regelverket.

I takt med at tonen mellom USA og Kina forverres, og amerikanske myndigheter innfører strengere eksport-kontroller mot Kina, vil denne typen utfordringer mot DNBs kunder – i særlig grad næringslivskunder – øke i omfang. Som eksempel kan selskap forhindres fra å eksportere produkter hvor amerikansk teknologi eller utstyr inngår i verdikjeden, noe som potensielt kan ha store finansielle konsekvenser for kunden – og i neste instans for banker som bidrar til å finansiere aktiviteten. DNB blir i slike tilfeller indirekte eksponert mot sanksjoner. Det er en del av trusselbildet vi må forholde oss til, og håndtere.

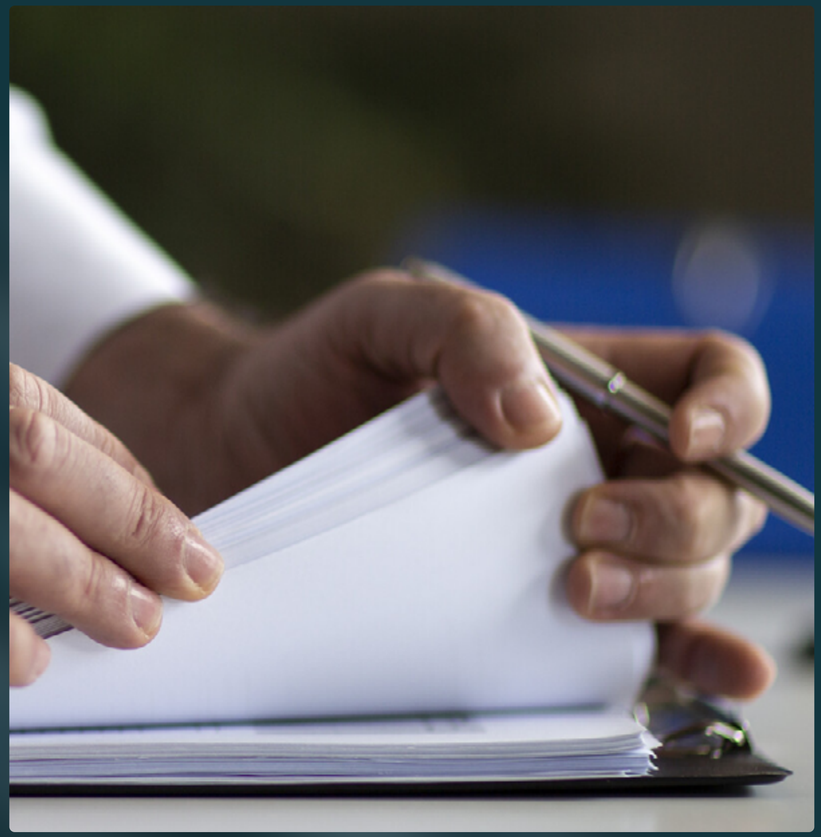
Fortsatt geopolitisk uro vil føre til økt sanksjonsbruk

Fortsatt russisk militær aktivitet i Ukraina vil føre til at stadig nye russiske aktører, selskaper og banker sanksjoneres. Dette vil medføre ytterligere forsøk på sanksjonsomgåelser, eksempelvis gjennom økt bruk av tredjeland og stråpersoner. EU har siden desember 2020 et økt handlingsrom for å sanksjonere brudd på menneskerettigheter, noe som sammenfaller med at demokratiets vilkår globalt gradvis forverres. Dette tilsier at også europeisk sanksjonsbruk vil kunne øke i tiden framover.

En fortsatt gradvis forverring i forholdet mellom USA og Kina vil videre kunne føre til restriksjoner på dollarbetalinger til en rekke kinesiske mottakere. Dersom Kina innleder en militær kampanje for å ta kontrollen over Taiwan er det sannsynlig at strenge sanksjoner vil bli innført mot Kina, og spesielt dersom USA trekkes inn i en militær konflikt. Med svært tette handelsforbindelser mellom Kina og Norge, og norske selskapers avhengighet av kinesiske leverandører, vil dette kunne ha en stor innvirkning både for DNB og for våre kunder.

Korrupsjon i bank- og finanssektoren

Bank- og finanssektoren har en sentral samfunnsfunksjon og utgjør en viktig del av den kritiske infrastrukturen både nasjonalt og internasjonalt. En av sektorens hovedutfordringer er å hindre at det finansielle systemet misbrukes til kriminelle formål som blant annet korrupsjon. Korrupsjon er et av de mest alvorlige og samfunnsskadelige lovbruddene innenfor økonomisk kriminalitet. Erfaringer fra de siste årene peker på at bank- og finansnæringen både nasjonalt og internasjonalt er særlig utsatt.



Flere faktorer gjør ansatte i bank- og finanssektoren sårbare for korrupsjon

Det er flere eksterne drivere som kan være med på å forsterke korrupsjonsfaren i bank- og finansinstitusjoner. Krevende forutsetninger for finansinstitusjoner til å levere på finansielle mål øker risikoen for å ta «etiske snarveier» og/eller begå korrupsjon. Krig, etterdønninger av covid-19-pandemien og økende konkurranse fra ikke-tradisjonelle banker kan øke insentivene til bruk av ulovlige midler, som bestikkelser, for eksempelvis å vinne kontrakter og anbud.

I bank- og finansbransjen er det også andre kjennetegn som kan øke bankens eksponering for korrupsjon, herunder konkurranse, hemmelighold, komplekse transaksjoner av høy verdi, samt belønningsordninger for prestasjon. Interessekonflikter trekkes ofte frem som et risikoområde. Interessekonflikter kan oppstå i mange av en finansinstitusjons aktiviteter, blant annet i forbindelse med innkjøp, oppkjøp, kontraktstildeling, salg, forretningsutvikling og ansettelser. I tillegg kjennetegnes bransjen av høy interaksjon med offentlig sektor. Eksempler på dette kan være utstrakt bruk av lobbyvirksomhet, men også gjennom andre aktiviteter som offentlige tilsyn. I mange land representerer staten og statseide selskaper en viktig inntektskilde for finansinstitusjonene, noe som kan bidra til å øke eksponeringen for korrupsjon.

Økokrim trekker fram at ansatte i bank- og finanssektoren har nøkkelroller i samfunnet som innebærer høy grad av tillit. De har ofte god oversikt over regelverket, og dermed også hvordan det kan omgås. For organiserte kriminelle er derfor en innsider i en finansinstitusjon en attraktiv ressurs.

Erfaringer viser at korrupsjon blir benyttet som et virkemiddel for at de kriminelle får utbetalt uriktige lån. Den bakenforliggende motivasjonen til utro tjenere i slike saker har ofte vært økonomi. Derfor kan et dårligere økonomisk livsgrunnlag være med på å øke trusselnivået.

Senest i 2022 har det blitt avdekket korrupsjon- og bedragerisaker hvor mulige utro tjenere i DNB og en annen nordisk bank er siktet for siktet for korrupsjon, grov korrupsjon og medvirkning til grov korrupsjon. Siktelsene går ut på at de bankansatte har sørget for innvilgelse av lån til kunder på feilaktig grunnlag mot at de selv har mottatt utilbørlige fordeler. Sakene er fortsatt under etterforskning.

Et annet eksempel er «Encrochat», der fransk politi i samarbeid med Europol fikk tilgang til en kryptert kommunikasjonsplattform som avslørte at kriminelle over hele Europa hyppig benyttet bankansatte som innsidere. Rapporten viser til at metoden de kriminelle aktørene benyttet for å rekruttere innsiderne var nettopp korrupsjon. I Norge har Oslo politidistrikt delt erfaringer som tilsier at en eller flere ansatte i banken har direkte eller indirekte knytninger til kriminelle aktører og miljøer. Disse ansatte er særlig sårbare for påvirkning fra det kriminelle nettverket. Påvirkningen kan blant annet være korrupsjon i form av penger, verdigjenstander eller reiser.

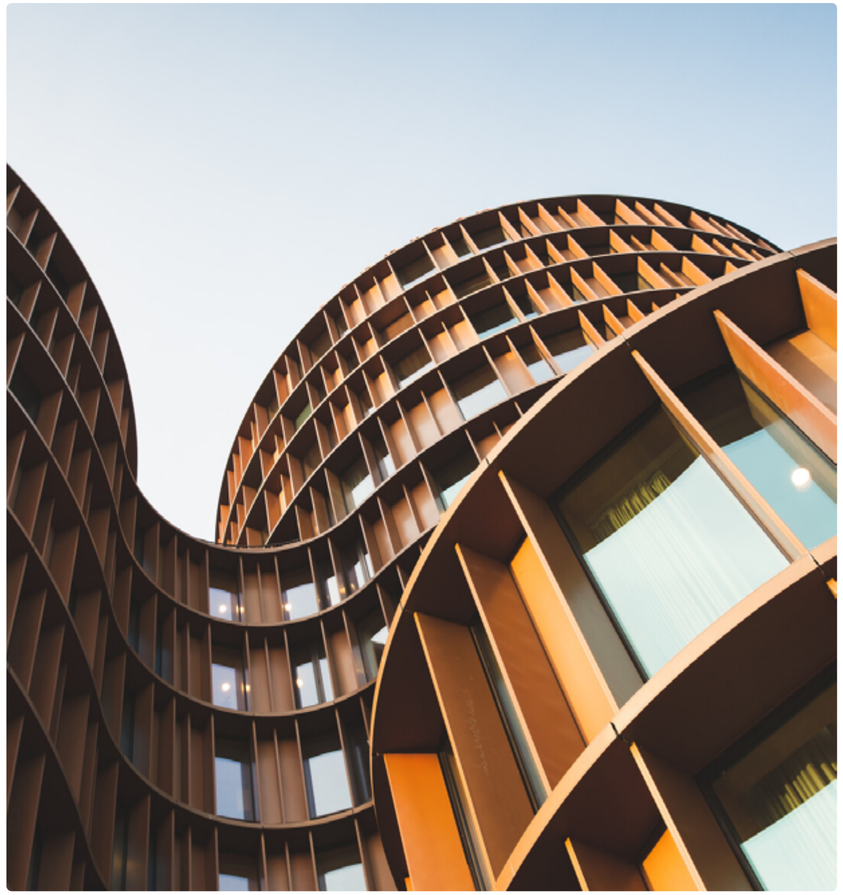
Bankenes tjenester utnyttes til korrupsjonsformål

I tillegg til at de ansatte i bankene kan utsettes for korrupsjon gjennom sine nøkkelroller, har banker en finansiell infrastruktur som også innebærer en korrupsjonsrisiko. Bankens kunder kan misbruke den finansielle infrastrukturen til å gjennomføre transaksjoner som har til hensikt å bestikke andre, for eksempel en utenlandsk offentlig tjenesteperson, eller utbetale et lån som blir misbrukt til bestikkelser. Et annet eksempel er at kunder benytter agenter i land/markeder med aksept for korrupsjon som alminnelig forretningsmetode for å oppnå tillatelser og godkjenninger, og fasiliterer dette ved transaksjoner via bankenes betalingssystemer. Internasjonalt sees trender med mer sofistikerte metoder, hvor bestikkelsen skjules og hvitvaskes i komplekse selskapsstrukturer eller går gjennom profesjonelle mellomledd. Dette gjør det krevende å følge pengetransaksjonen frem til reell mottaker. En rekke internasjonale korrupsjon- og hvitvaskingssaker har preget finansnæringen de siste årene.

Bank og finanssektoren – en sentral aktør i kampen mot korrupsjon

Banker og finansinstitusjoner er sentrale aktører i kampen mot økonomisk kriminalitet, herunder korrupsjon, noe utviklingen de siste årene innenfor både nasjonale og internasjonale regelverk understreker. DNBs innsats mot korrupsjon er forankret i regelverkene samt i rollen som en ansvarlig samfunnsaktør i en bærekraftig utvikling.

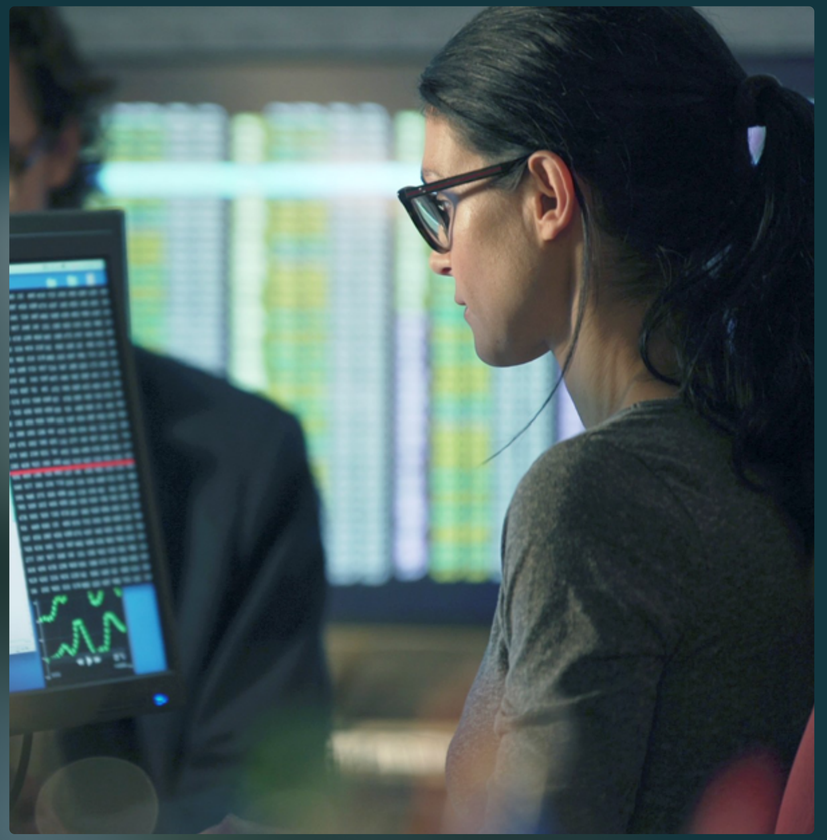
DNBs aktiviteter retter seg mot en rekke aktører, herunder kunder, leverandører, agenter, andre samarbeidspartnere og offentlige myndigheter. DNB er dermed utsatt for korrupsjonsrisiko gjennom flere relasjoner og aktiviteter. For å håndtere korrupsjonsrisikoen og bidra aktivt i kampen mot korrupsjon har DNB etablert et antikorrupsjonsprogram med hovedformål å forebygge og avdekke korrupsjon som kan forekomme gjennom DNBs virksomhet. DNB har iverksatt en rekke tiltak for å blant annet forebygge korrupsjonshendelser knyttet til ansatte i nøkkelposisjoner, men også for å håndtere korrupsjonsrisikoen både tredjeparter og kunder kan medføre. DNB har offentliggjort to iboende risikovurderinger knyttet til korrupsjon og hvitvasking med det formål om å bidra til mer åpenhet i kampen mot økonomisk kriminalitet.



Linkene tar deg til eksterne pdf-er om korrupsjon og hvitvasking

Misbruk av tillitsbaserte systemer

Trusselbildet innen hvitvasking preges av digitalisering og globalisering. Nye utviklingstrekk viser at kriminelle har stor tilpasningsevne, vilje og kapasitet til å misbruke og oppnå vinning fra systemer som innføres for å digitalisere og forenkle hverdagen vår.



Digitalisering av tillitsbaserte systemer skaper nye sårbarheter

Samfunnet arbeider systematisk for å fornye, forenkle og forbedre løsninger gjennom å utvikle og anvende ny teknologi. Der digitalisering kan bidra til økt verdiskapning, produktivitet og innovasjon kan det oppstå sårbarheter som åpner nye arenaer for kriminelle.

En slik arena åpnet seg under pandemien da samfunnet iverksatte en lang rekke støttetiltak for å redusere konsekvensen av nedstengingen. En rekke tiltak ble satt inn - statsgaranterte låneordninger, utvidet rett til dagpenger, lønnskompensasjonstiltak og så videre.

Fra DNBs perspektiv i hvitvaskingsarbeidet kunne det observeres hvordan disse støttetiltakene nesten umiddelbart ble utnyttet for å oppnå urettmessig vinning. Det fremstod som om kriminelle analyserte ordningene og fant ut hvordan de skulle gå frem for å kapitalisere av dem. For eksempel ble det omsatt lister med personnumre som ble benyttet for å registrere fiktive arbeidstakere og deretter som grunnlag for å bli tildelt lønnskompensasjon fra i et selskap, innrapportert lønn og deretter søkt lønnskompensasjon fra NAV.

Støtteordningene er senere avviklet, men gjennom antihvitvaskarbeidet ser DNB nå at kriminelle har videreutviklet kunnskapen de opparbeidet under pandemien og tar i bruk ferdighetene i misbruk av digitale løsninger inn på andre områder.

En slik ordning som har vist seg sårbar er bruken av elektroniske a-meldinger. Disse gir virksomheter mulighet for å rapportere inn opplysninger om ansattes inntekt og arbeidsforhold digitalt. En ordning som er nyttig for alle parter. Virksomheten kan de enkelt og effektivt innrapportere opplysninger gjennom sine regnskapssystemer, skatteetaten får inn skattegrunnlag løpende uten behov for å legge inn opplysninger manuelt og det åpner muligheter for nye måter å benytte informasjonen på. For eksempel vil NAV kunne benytte denne informasjonen som grunnlag for tildeling av sosial- og velferdsytelser og banker kan bruke informasjonen under kredittbehandling.

Ordningen har vist seg ekstra sårbar og tilrettelagt for utnytting ved at den tilbyr stor fleksibilitet til å endre opplysninger. For eksempel kan man rette lønnsopplysninger gitt gjennom a-meldinger inntil tre år tilbake i tid og det er mulig å innberette lønn i tidsrommet før et foretak er etablert.

DNB avdekker stadig nye måter kriminelle aktører misbruker systemer for egne vinning

DNB har avdekket en rekke saker der ordningen for samtykkebaserte lånesøknader (SBL) er misbrukt. Dette dreier seg om mulige lånebedragerier, ID-misbruk, trygdebedrageri, forsikringssvindel og korrupsjon. Misbruk av SBL-ordningen skjer også i sammenheng med at en utnytter svakheter i andre offentlige registre, eksempelvis ved registrering av stråpersoner i selskapsregistre og forsinkelser ved registrering av pant i løsøreregisteret.

Virksomhetene som benyttes i kriminaliteten er ofte etablert innenfor næringer som vi er kjent med er utsatte for arbeidslivskriminalitet. Det kan være innenfor transportbransje, bilvask eller vasketjenester. Det er i stor grad arbeidsintensive virksomheter med lave formalkrav og med stor benyttelse av utenlandsk arbeidskraft.

Aktørene som opererer med denne formen for bedragerier er ofte kjent i tilknytning til andre hvitvaskingssaker banken har avdekket. Gjerne innenfor lånebedragerier og også med mulig tilknytning til organiserte kriminelle miljøer. Flere har vært innom finansbransjen tidligere og dette belyser innsideproblematikken i disse sakene.

Et eksempel på et SBL-bedrageri kan være ved kombinasjonen av ID-tyveri og lånebedrageri. Her har kriminelle skaffet seg tilgang til en elektronisk identitet, eksempelvis BankID. Personene registreres som arbeidstaker i et firma og det innrapporteres gjennom a-meldinger at vedkommende har mottatt omfattende lønnsutbetalinger tilbake i tid. Deretter søkes det på vegne av vedkommende om et lån hos en finansinstitusjon som innhenter inntektsdata gjennom Skatteetaten. Lånet utbetales på uriktig grunnlag til en konto kontrollert av den kriminelle og utbyttet blir enten raskt videreført eller eksempelvis benyttet for kjøp av bil eller annen formuesgjenstand. Bilen kan siden bli meldt stjålet. Anmeldelsen skjer ved bruk av politiet digitale løsninger for å anmelde saker og man legitimerer seg gjennom den stjålne Bank-Iden. Denne anmeldelsen benyttes deretter som grunnlag for å kreve erstatning hos forsikringsselskapet. Etter lånene er utbetalt korrigerer virksomheten de tidligere innsendte a-meldingene slik at det ikke kommer krav om betaling av arbeidsgiveravgift.

For DNBs vedkommende er det avdekket bedragerier som kan utgjøre flere titalls millioner kroner. Vi er kjent med at andre banker er utsatt for samme modus, så det totale omfanget er betydelig større.

Digitaliseringen endrer samfunnet og den endrer kriminaliteten. Omfanget av saker vi har sett på området synliggjør at kriminelle har vilje og kapasitet til å utnytte sårbarheter i ny teknologi. Dette setter store krav til at det ved etablering av systemer ikke bare vurderes risiko ved stabilitet og funksjon, men at det også analyseres sårbarheter og etableres tiltak for å hindre at systemene benyttes til kriminalitet.

Sabotasje mot samfunnskritisk infrastruktur

Samfunnet er avhengig av at det er strøm i stikkontakten, men den siste tids utvikling viser oss hvor sårbart samfunnet er for utfordringer med strømforsyningen. Den minste mistanke om kraftforsyningen kan bli rasjonert eller delvis utilgjengelig har store ringvirkninger. Selv om større bedrifter som DNB har noe robusthet i egen strømforsyning hjelper ikke dette sluttkundene dersom de ikke selv har strøm til mobiltelefon og PC. DNB har videre begrensede muligheter til alternativ strøm over tid, og er avhengig av at leverandører og andre tredjeparter også har robusthet i egne forsyningslinjer.

I «NOU 2016:19 Samhandling for sikkerhet» er sabotasje definert som «tilsiktet ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, anlegg, eller funksjon, utført av eller for en fremmed stat, organisasjon, gruppering eller enkeltperson». Sabotasje kan altså være utført som en terrorhandling, men også som en del av konvensjonell krigføring, statskupp eller aktivisme. Faktisk er arbeidskonflikter i Frankrike den etymologiske bakgrunnen for begrepet.

Sabotasje mot elektronisk kommunikasjon gjør oss særlig sårbare

For DNB og finansnæringen er strømforsyning og elektronisk kommunikasjon (ekom) de innsatsfaktorene som er direkte avhengig av samfunnskritisk infrastruktur. Det meste av global ekom (ca. 97 %) foregår via undersjøiske kabler. Til sammen utføres det videre $10 trillioner i finansielle transaksjoner daglig via disse fiberkablene.

Som et tegn på fokuset samfunnskritisk infrastruktur har for tiden, var Equinor, Google og Svenska Kraftnät invitert til NATO-rådet for å diskutere sikkerheten til olje- og gassinstallasjoner, undersjøiske fiberkabler og strømnettet. Kan man i det hele tatt beskytte 9000 km med gassrør?
- Det går ikke, er konsernsjef Opedal i Equinor sitert på i Aftenposten.

At både gassrør og fiberkabler ligger undersjøisk, men ubeskyttet i internasjonalt farvann, gjør at det er mange likheter i sårbarhetsbildet for disse installasjonene. Saboteringen av Nord Stream-gassledningene ble av mange sett på som et paradigmeskifte innen sabotasje, men sabotasje som irregulært virkemiddel har historisk blitt benyttet både i konflikter og i fredstid. To dager før den russisk-støttede invasjonen av Georgia i 2008, ble oljeledninger i regionen rammet av en eksplosjon.

Systematisk bombing av infrastruktur for kraft og ekom er senest brukt av Russland i krigen i Ukraina, men også dette har historiske linjer tilbake til 2. verdenskrig og Korea-krigen.

Også ikke-statlige aktører utgjør en trussel

Det er ikke bare statlige eller profesjonelle aktører som har intensjon og kapasitet til å sabotere kritisk infrastruktur. Boken «How To Blow Up A Pipeline» av den svenske akademikeren Andreas Malm argumenterer for sabotasje som et logisk neste steg for klimaaktivister og refererer til historiske sabotasjeaksjoner mot olje og gassinfrastruktur blant annet i Sør-Afrika, Palestina og Nigeria. Også i Norge har klimaaktivister tatt til orde for å benytte sabotasje som et virkemiddel i kampen for klima.

I USA er det en økende trend at høyreradikale grupper utfører sabotasje mot kraftstasjoner. I løpet av de første åtte månedene i 2022 ble det rapportert 100 slike hendelser. Angrepet mot to transformatorer i Nord-Carolina ble utført med skytevåpen og førte til at titusener av mennesker var uten strøm så lenge at unntakstilstand og portforbud ble innført av myndighetene.
I Sverige ble en strømmast i 2016 utsatt for sabotasje fra det man antar var fremmede makter, og som svenske myndigheter beskrev som en stresstest.

Sabotasje mot systemer uten redundans gir størst konsekvens

Infrastruktur for kraft og ekom er distribuerte nett som gjør at funksjonaliteten ikke er avhengig av et sentralt kontrollsenter, og leveransene vil finne minste motstands vei så lenge det er ledig kapasitet i nettet. For eksempel er den norske elkraftforsyningen meget robust, og ikke avhengig av et fåtalls kjernekraftverk, men en rekke små og store vind- og vannkraftverk pluss muligheten for import. Norske kraftverk tas ut av nettet hele tiden, enten for vedlikehold eller for at vannverdien vurderes høyere enn den gjeldene kraftprisen.

Sårbarhetene for sabotasje av samfunnskritisk infrastruktur er derfor konsentrert til begrensede områder med få linjer til omverdenen. For eksempel skal Russland ha isolert Krim-halvøya fra Ukraina ved å ta kontroll over kun ett eneste samtrafikkpunkt for internett. I Norge er det tilsvarende sårbarheter i Finnmark hvor flere kommuner under en hendelse var uten fasttelefon, mobil og internett i over to døgn etter et kabelbrudd. Plassering og mangelfull sikring av disse kablene er påvist i media.

Høsten 2022 opplevde Frankrike et koordinert angrep hvor fiberoptiske kabler ble kuttet samtidig klokken fire på morgenen. Selv om dette var interregionale hovedkabler var forstyrrelsen begrenset til kortvarige utfall og tregt internett for kundene til en tilbyder. Dette viser verdien av redundans, både for samfunnet og for den enkelte borger eller bedrift. Selv om én av to fiberkabler til Svalbard var nede i januar 2022 beholdt øya internettforbindelsen, men uten reservekapasitet.

For fiberkabler er den hyppigste trusselen, som medfører 150-200 brudd i kabler i året, fra utilsiktet skade av fisketrålere og undersjøiske jordskjelv. Tilsiktede sabotasjehandlinger mot undersjøiske kabler kan skje enten ved bruk av ubåter, eller med overflatebåter som benytter autonome eller menneskestyrte undervannsdroner.

Fra et samfunnsikkerhetsperspektiv er derfor de mest interessante sårbarhetene knyttet til de infrastrukturene som ikke nødvendigvis er begrenset i geografisk forstand, men i bruksområde eller funksjonalitet. Dette kan være bedriftsnett (WAN), infrastruktur for operasjonsteknologi eller industrielle styringssystemer. Et nylig eksempel er sabotasje mot Deutsche Bahns internkommunikasjon hvor kabler ble kuttet flere steder av aktører som hadde kunnskap om systemet. Aksjonen stoppet fjerntog i Tyskland fra morgen til tidlig ettermiddag, og aktørene la ikke igjen noen krav eller forklaring på aksjonen.

Et annet eksempel på system uten redundans er det undersjøiske sensornettverket LoVe Ocean som gikk i svart etter at deler av kabelnettverket forsvant sporløst i april 2021. Både her og over fiberkablene til Svalbard ble russiske fartøy observert med mistenkelig aktivitet i tidsrommet før hendelsene.

Sårbare programvarekomponenter

I moderne systemutvikling er det svært vanlig å bruke ferdige programvarekomponenter for å akselerere utviklingen av nye løsninger. I stedet for å lage all funksjonalitet fra bunn av, brukes gratis eller betalbare komponenter. Komponenter i operativsystemet blir holdt vedlike gjennom periodiske oppdateringer (patching). Leverandører utgir jevnlig sikkerhetspatcher og open source produkter oppdateres når sårbarheter oppdages. Når ny versjon lanseres slutter leverandører å oppdatere gamle versjoner, som da krever brukerinteraksjon for å forhindre sårbarheter i programvaren. I mange tilfeller utsettes denne manuelle jobben av ulike årsaker. Konsekvensen blir at løsningen plutselig kan inneholde komponenter med alvorlige sikkerhetshull. Disse hullene kan gjøre løsningen utsatt for angrep eller gjøre den ustabil.

Programvarekomponenter utgjør for mange en ukjent sårbarhet i IT-systemene

Det er ikke uvanlig at moderne systemer inneholder hundrevis av komponenter fra ulike leverandører. Hvis disse komponentene blir valgt tilfeldig, er det stor risiko for at systemet inneholder sikkerhetshull som kan utnyttes av ondsinnede aktører. Når en utvikler har behov for en spesifikk funksjon og velger å benytte en komponent, er det ikke enkelt å se om komponenten kommer fra en pålitelig kilde. Som eksempel vil et søk etter komponenter i kjente og troverdige komponentbibliotek gi svært mange alternativer hvor det er ikke noen garanti for at alle er pålitelige. Når man publiserer til et komponentbibliotek, er det ingen kontroll på om komponenten inneholder ondsinnet kode.

En komponent er en del av et system som utfører en bestemt oppgave eller funksjon. Det kan være programvare eller hardware, og det kan være et eget system eller en del av et større system. Komponentene i et system kan være avhengige av hverandre, og det er viktig at alle komponentene fungerer som de skal for at systemet skal fungere som det skal.

Programvarekomponenter kan utgjøre en nulldagssårbarhet ettersom sårbarheten ikke er kjent for de som har ansvaret for utvikling av programvaren eller komponenten. Frem til sårbarheten er fjernet kan det være mulig for hackere å misbruke det til for eksempel å stjele data, gjøre systemer utilgjengelig eller overta ressurser for å angripe andre systemer. Kunnskap om nulldagssårbarheter selges/distribueres ofte på Dark Web. Samtidig er trusselen fra kjente sårbarheter langt større enn den fra ukjente, selv om de er langt enklere å beskytte seg mot.

En av de alvorligste konsekvensene ved svakheter i komponenter er når den tillater at ondsinnet kode kjøres på en ekstern datamaskin eller prosess. Spesielt alvorlig er det når denne koden kan kjøres med utvidede rettigheter, noe som kan gi en angriper tilgang til å overta hele eller deler av et system.

Også DNB har tidligere identifisert sårbarheter i egne komponenter

En av de mest alvorlige nulldagssårbarhetene oppdaget den senere tid var i en svært mye benyttet komponent. Log4J er en åpen kildekomponent fra Apache Software Foundation som benyttes i skytjenester fra Apple/AWS, i populære spill som Minecraft, Twitter og i et bredt antall systemer innen utvikling og sikkerhet. Oppgaven til komponenten er å ta vare på hendelser som skjer i programvaren og kommunisere disse hendelsene til systemadministratorer og brukere. Sårbarheten var at Log4J tillot brukere å sende inn kode som spesifiserte hvordan meldingen skulle se ut. Det viste seg at det ikke var satt noen begrensninger til denne koden, noe som medførte at en ondsinnet aktør enkelt kunne overta serveren for å stjele data eller ta kontroll over systemet. Sårbarheten ble raskt tatt i bruk av mange aktører. Et cybersikkerhetsselskap som innførte beskyttelse for sårbarheten for sine kunder, klarte å se og avvise 4,3 millioner forsøk på misbruk, hvor 46 % var fra kjente kriminelle grupper.

En nulldagssårbarhet (0-day vulnerability) er en sårbarhet som ikke er kjent for de som har ansvaret for utvikling av programvaren eller komponenten. Frem til sårbarheten er lukket kan det være mulig for hackere å misbruke det til for eksempel å stjele data, gjøre systemer utilgjengelig eller overta ressurser for å angripe andre systemer. Kunnskap om nulldagssårbarheter selges ofte på det mørke nettet.

Også DNB benyttet Log4J i flere av våre systemer. Da sårbarheten ble kjent ble det startet et stort kartleggingsarbeid for å finne systemer som benyttet seg av komponenten. Vi så raskt at ondsinnede aktører forsøkte å utnytte sårbarheten hos DNB, og et høyt antall mennesker spredd over mange av de tekniske miljøene ble involvert i hendelsen. Fra de som jobbet med patching av egne systemer, til generelle sikringstiltak plassert foran hele DNB sin infrastruktur, til detektering og gjennomgang av forsøkene vi så på å utnytte sårbarheten. DNB har tidligere erfart og håndtert flere tilfeller hvor sårbarheter i våre programvarekomponenter ble eksponert og forsøkt kompromittert.

Et annet eksempel som viser kompleksiteten i vedlikehold av komponenter, er sårbarheten som ble oppdaget i OpenSSL. OpenSSL er en åpen kildekode med komponenter som tilbyr funksjonalitet rundt kryptering og sikkerhet. Svakheten lå i sertifikathåndtering og kunne medføre ondsinnet fjernkjøring av kode. Til tross for at sårbarheten ble raskt rettet, peker dette til en annen utfordring. Denne komponenten er ofte benyttet av andre komponenter (i tillegg til i operativsystemer og servere). Det er derfor viktig å kun benytte komponenter fra kjente leverandører, teste i lukkede miljøer, bruke kjente versjoner, bruke verktøy for å søke etter ondsinnet kode og holde seg løpende orientert om sårbarheter når de dukker opp.

Et komponentbibliotek (package manager) er et sett med verktøy som automatiserer installasjon, oppgradering, konfigurering og fjerning av komponenter eller programmer. Eksempler er Node Package Manager (npm) som brukes mye for JavaScript og NuGet som brukes mye for Microsoft .NET

Åpen kildekode er programmer og komponenter som er allment tilgjengelig. Koden er som oftest tilgjengelig over internett og alle kan gjøre utvikling og videreutvikling av programvaren. Åpen kildekode er nødvendigvis ikke gratis hvis man skal benytte den kommersielt. Til tross for at koden er tilgjengelig kan den inneholde svakheter og bakdører som kan være vanskelige å finne.