



FINANSIELL TRYGGHET I EN USIKKER VERDEN

TRUSLER OG TRENDER FRA ET DNB-PERSPEKTIV 2024

Om rapporten

Denne rapporten er utarbeidet av fagmiljøene i DNB som daglig jobber med sikkerhet og bekjempelse av økonomisk kriminalitet.

Hensikten er å benytte data og informasjon for å forstå eget trusselbilde, samt gi en forståelse for de sikkerhetstiltakene vi må ha på plass som sørger for at vi leverer sikre og robuste tjenester.

Ved å offentliggjøre rapporten ønsker vi å bidra til at private og offentlige interesserenter får muligheten til å benytte kunnskapen som et utgangspunkt for å vurdere eget trusselbilde og gjøre riktige tiltak.



Digitale tredjepartsangrep gjør oss sårbare



Ansatte opplever stadig flere grove trusler fra kunder



Bedragerier har blitt primærinntekten til organisierte kriminelle



Økning i angrepsum og ofre utsatt for investeringsbedragerier



Trenden med økt forsikringssvinde fortsetter



Betydelig risiko for hvitvasking i bedriftssegmentet



Stormaktkonflikter fremmer bruken av sanksjoner som virkemiddel



Hacktivisme på fremmarsj



Størst omfang av hvitvaskingssaker med utbytte fra bedragerier

Finansiell trygghet og kampen mot økonomisk kriminalitet viktigere enn noen gang

I en usikker verden med et stadig mer komplekst og krevende geopolitisk bilde har finansiell trygghet blitt enda viktigere. Vi har over tid registrert en stor økning fra organiserte kriminelle som ønsker å stjele våre og kundenes penger, eller på annen måte skade finansnæringen for økonomisk vinning. I tillegg risikerer vi at de finansielle verdikjedene blir brukt av statlige og politiske krefter. Målet kan være å destabilisere vestlig økonomi, hindre et effektivt finansmarked og lage usikkerhet i samfunnet. Cyberangrep, gjerne i kombinasjon med manipulering er et vanlig virkemiddel for å oppnå disse målene.



Situasjonen ute i verden er alvorlig og preget av uro og konflikt. Krigen i Ukraina fortsetter etter fullskalainvasjonen februar 2022. Krigen på Gazastripen skaper usikkerhet rundt hva som kan skje videre i regionen og det er ingen tegn til positive endringer i polariseringen og retorikken mellom verdens stormakter. Her i Norge setter «dyrtiden» sine spor med større usikkerhet enn på mange år. Dette har ført til frustrasjon og en økning i antall trusler mot ansatte som jobber ut mot kundene.

I kampen mot økonomisk kriminalitet opplever vi økt profesjonalitet fra de som stjeler fra oss. De kriminelle behersker bruk av både sosial manipulering godt og bruker moderne teknologi og komplekse verdikjeder for å gjennomføre bedragerier. Vi ser nå en økt bruk av kunstig intelligens og automatisering for å skalere opp og øke kvaliteten og angrepsvolum.

Hvitvaskings- og sanksjonsområdet fortsetter å være et område hvor DNB legger inn stor innsats. Sterkere kontroll på opphav av penger og overføringer er viktig for å hindre at penger fra kriminalitet hvitvaskes eller havner i feil hender. DNB rapporterte i 2023 det høyeste antallet saker til Økokrim noensinne. Hele 40 prosent av de rapporterte sakene stammer fra bedragerier. Dette er saker som krever at vi tilpasser våre arbeidsmetoder. Internasjonale sanksjoner har også i 2023 økt i omfang som følge av krigen i Ukraina og vestlige sanksjoner. Dette krever at DNB har sterkt fokus på området.

DNBs rapport «Finansiell trygghet i en usikker verden» har som formål å

øke bevisstheten rundt trusler og hendelser vi håndterer både mot oss som konsern, mot våre kunder og mot samfunnet. Ved å dele våre erfaringer ønsker vi å bidra til at andre kan redusere sannsynligheten for å bli rammet eller redusere konsekvensene hvis man skulle være uehdig. DNB alene kan ikke stanse all økonomisk kriminalitet, men i alle tilfeller hvor vi sørger for at angriper eller den kriminelle mislykkes har vi lykkes. Vi er én aktør i den store verdikjeden som må stå samlet i kampen. Som tidligere er vårt budskap at vi står sammen mot de som truer vår sikkerhet og våre verdier, og dette viktige arbeidet har fortsatt behov for sterkt fokus fremover.



Anders Hardangen.

Anders Hardangen,
Sikkerhetsdirektør i DNB



Terje Aleksander Fjeldvær

Terje Aleksander Fjeldvær,
Konst. Hvitvaskingsansvarlig i DNB

Finansiell trygghet i en usikker verden

Fysiske trusler

Sammendrag

DNB opplever flere trusler innenfor det fysiske domenet, hvor motivasjonen til trusselaktørene varierer og konsekvensene av handlingene spenner fra det ubetydelig til hendelser hvor liv og helse kan gå tapt. Gjennom året har vi opplevd flere hendelser som har krevd håndtering av DNBs sikkerhetsavdeling. Dette gjelder særlig hendelser som omhandler trusler mot ansatte. Drivkraftene som påvirker samfunnet for øvrig, er også med på å endre trusselbildet DNB møter. Krig, klima og økonomiske nedgangstider har også vært med å påvirke den fysiske trusselen vi har møtt det siste året.

DNB hadde i 2023 en økning i antall saker som omhandler trusler og vold mot ansatte sammenlignet med tidligere år. Årsaken til dette henger ofte sammen med personlige forhold som mental helse og dårlig økonomi. Vi ser i tillegg at tiltak som re-legitimering av kunder og kundetiltak jf. Hvitvaskingsloven er eksempler på utløsende faktorer som fører til en økning i antall trusler. Det har vært en svak økning i antall voldssaker, samtidig erfarer vi at mange av truslene ansatte opplever er grove. Alvorligheten i truslene gjenspeiles i at halvparten av sakene politianmeldes. Hvis de økonomiske nedgangstidene fortsetter og privatøkonomien til mange forverres forventer vi at det høyet antallet trusler mot ansatte vil vedvare.

Aktivism fra klimabevegelsen mot bank- og finanssektoren i Europa og USA har pågått over flere år. I 2023 har mange av aksjonene i Norge vært rettet mot departementene gjennom Fosen-saken, men også mot virksomheter innen fossil

industri. Det har i mange av tilfellene blitt benyttet sivil ulydighet under aksjonene. I DNB erfarte vi en mindre, fredelig protest utenfor våre lokaler i Stockholm, men forventer at aksjoner med sivil ulydighet også kan treffe oss. Bank- og finanssektoren opplevde også økt aktivisme på bakgrunn av konflikten i Israel og Palestina og vi forventer at DNB vil fortsette å være et mål for aktivister på tvers av det ideologiske spekteret.

Den direkte terrortrusselen mot DNB er lavere enn mot samfunnet for øvrig. Dette fordi DNB ikke er en prioritert del av fiendebildet til hverken høyreekstreme eller ekstreme islamister. DNB har flere lokasjoner som ligger i nærheten av potensielle terrormål, og kan dermed indirekte bli offer for angrep. Videre vurderer vi at trusselen mot DNB øker ved deltagelse i arrangementer med forhøyet terrortrussel, som eksempelvis Pride, hvor DNB var hovedsponsor og hadde høy tilstedeværelse.

DNB opplever regelmessig ulike former av innsideaktivitet, spesielt innenfor informasjonstyveri. De fleste sakene har imidlertid lav konsekvens for DNB. Innsidetrusselen fra statlige aktører har ifølge PST økt i lys av den endrede geopolitiske situasjonen. DNB er også et mål for organiserte kriminelle som søker tilretteleggere i bank- og finanssektoren for blant annet hvitvasking og bedragerier. DNB må dermed ta høyde for stadig mer sofistikerte og profesjonelle trusselaktører, også i forhold til at disse kan forsøke å komme på innsiden av DNB.

Oppsummering 2023

Trusler mot ansatte øker

I 2022 rapporterte vi om en økning i antall saker hvor kunder truer ansatte, og i 2023 har dette antallet igjen økt. Det er få registrerte saker hvor det har vært utøvd vold mot ansatte, men også her har vi hatt flere hendelser enn tidligere år. Selv om det er få faktiske voldssaker, er mange av truslene som rettes mot DNBs ansatte grove.

På bakgrunn av utviklingen jobber DNB systematisk med å følge opp årsakene til hendelsene på en god måte, for å kunne gjennomføre tiltak som skal forsøke å forhindre at fremtidige hendelser oppstår eller får alvorlig konsekvens. Målet har vært å finne tiltak som beskytter ansatte mot hendelser vi opplever ofte og som utgjør de største risikoene. Flertallet av truslene mot ansatte i DNB skjer gjennom telefon og er rettet mot kunderådgivere. Gjennom hele 2022 erfarte vi at flere trusler bunnset i frustrasjon over krav om re-legitimering.

I 2023 er en fellesnevnerne at kunder ønsker hjelp med tjenester og ber om å få løst problemer som kunderådgiverne hverken har tilgang eller fullmakt til å gjøre. Eksempelvis ved forfalte regninger, igangsatt kundeavvikling eller forhold som gjør at kundene ikke får disponert pengene på konto slik de ønsker.

Et eksempel på en trusselhendelse er en kunde som truet med å spreng et bankkontor da kunden uten grunnlag mente at DNB hadde skyld i at pengene til personen ikke var på konto. Kunden mente også at DNB hadde trukket en del penger fra kundens konto. I en annen sak ringte en kunde og spurte om skattepengene hadde kommet inn på konto, noe kunderådgiver avkrevtet. Kunden truet da med å dra inn på et DNB kontor med et skytevåpen.



Figur 1. Hendelser 2021-2023

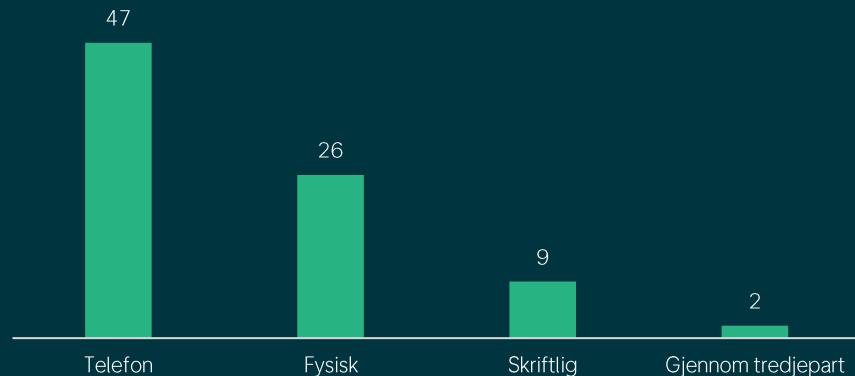
I mange av sakene fremstår det som om psykiske lidelser, økonomiske vanskeligheter og rus er en fellesnevner. NAV skriver at 55 prosent av NAV-ansatte oppgir psykisk lidelse som en medvirkende årsak til siste trussel eller voldshendelse¹. Kripos viser også til en økning i vold begått av personer med alvorlige psykiske lidelser de siste fem årene. Mest typisk beskrives gjerningspersonene som menn i alderen 20-50 år med alvorlige psykiske lidelser². Dette samsvarer med profilen DNB ser i mange av våre saker. I flere tilfeller har kunden kommet med direkte drapstrusler mot kunderådgivere. Ved fem anledninger har kunden sagt de skulle komme på et DNB kontor med kniv og i fem tilfeller var det fremsatt bombetrusler. Vi ser at det i noen tilfeller er de samme personene som over tid kommer med trusler mot ansatte. Ved et tilfelle i år ringte en kunde opptil ti ganger om dagen over flere dager, før kunden til slutt møtte fysisk opp ved en lokasjon, truet ansatte og ble til slutt pågrepet av politiet.

Alvorlige psykiske lidelser kan utgjøre en større risikofaktor for vold, spesielt i samspill med relasjonsbrudd, voldsutsatthet, økonomiske kriser eller problematisk bruk av alkohol eller andre rusmidler. NAVs ansatte opplyser at økonomi er en viktig årsak til at det har oppstått trussel- eller voldhendelse hos dem. Også i DNB fremstår det som at mange av trusselutøverne har økonomiske utfordringer. Det er derfor sannsynlig at økonomiske nedgangstider har vært en del av årsaken til økningen i antall saker i 2023.

Vi ser stadig flere aggressive kunder som opptrer truende, er ufine eller nekter å gå etter å ha blitt bortvist. I 2023 har nesten 200 saker blitt registrert som «uønsket kundeadferd» innen fysisk sikkerhet. Dette er saker hvor kunden ofte oppfattes å ha en ufin oppførsel overfor DNB-ansatte eller vektere, men hvor det ikke har vært fremmet klare trusler eller utøvet vold. Dette kan eksempelvis være kjefting, hærverk i lokalene

eller rasisme. Statistikken viser at i 32 tilfeller endte disse sakene med at vekteren bortviste kunden, og i 16 av sakene ble kunden enten anmeldt eller håndtert av politiet.

Som det kommer frem i eksempler fra 2023 er flere av truslene mot DNBs ansatte svært grove. Dette reflekteres også i antall anmeldelser registrert og trusselsituasjoner som har krevd direkte håndtering fra politiets side i form av pågripelser eller bortvisning. Grove trusler og anmeldelser omhandler typisk saker hvor det har kommet drapstrusler direkte mot kunderådgivere eller bombetrusler mot DNB.



Figur 2. hvordan truslene har blitt kommunisert

¹ Vold og trusler mot ansatte i NAV - nav.no

² Politiets trusselvurdering 2023



Aktivisten mot bank- og finansnæringer vil fortsette

Klimabevægelsen i Norge og Europa har i 2023 utført en rekke aksjoner, og bank- og finansnæringen har vært et aktuelt mål. I DNB erfarte vi kun én direkte aksjon med en håndfull aktivister som møtte opp utenfor våre lokaler i Stockholm. Selve protesten foregikk fredfullt og uten konsekvenser for DNB. Bakgrunnen for aksjonen var for å protestere mot utbyggingen av Rosebank-feltet i Storbritannia og mot utvinning av mineraler fra havbunnen. Selv om ingen av disse sakene direkte kan knyttes til DNBs operasjoner, aksjonerte de på bakgrunn av vår finansiering av denne typen virksomhet. I sin nylig publiserte transisjonsplan beskriver DNB hvordan netto nullutslipp av klimagasser skal nås innen 2050 for utlån, investeringer og egen drift. Samtidig understreker transisjonsplanen at DNB vil fortsette å investere i olje og gass, en sektor som anslås å ha investeringsvekst den kommende tiden.

DNB er også kjent med at en stor miljøorganisasjon i år kjøpte aksjer i DNB for å kunne delta og ta ordet under generalforsamlingen. Andre norske selskaper har opplevd tilsvarende aksjoner der klimaorganisasjoner også har fremmet forslag under generalforsamlingen. I andre europeiske land erfarte flere store selskaper en mer aggressiv tilnærming under deres generalforsamlinger hvor

aktivister brukte fysisk makt for å komme seg inn i møtene for å protestere.

I Norge har protestene fra miljøbevegelsen så langt vært av ikke-voldelig karakter, men flere av miljøorganisasjonene understreker at de vil ta i bruk sivil ulydighet i form av blokader, okkupasjon av privat grunn og unnlatelse av å følge politiets pålegg, slik vi har sett under bestemte aksjoner i 2023. Skadeverk i form av bruk av maling på fasade har også blitt benyttet.

For flere grupperinger er profitdrevne selskaper en felles antagonist. Noen protester og personer kan derfor også ha andre underliggende motiver for å aksjonere mot DNB. DNB erfarte i 2023 å bli satt under luppen som følge av økningen i utlånsrenter, og som et resultat fikk vi en offentlig politisk debatt og negativ medieomtale som kan påvirke opinionen. Konflikten mellom Hamas og Israel førte til en kampanje mot banker som gjennom fond investerer i selskaper med virksomhet på palestinske områder. DNB-ansatte opplevde i ettertid å bli konfrontert om dette av aktivister i det offentlige rom. Finansdepartementet og Norges Bank erfarte at et tjuetalls aktivister blokkerte inngang til deres lokaler i protest.

Terrortrusselen mot DNB er lav, men økte under deltagelse på enkelte arrangementer

DNB er utsatt for terrortrusselen på lik linje med resten av det norske samfunnet. DNB er ikke en del av det prioriterte fiendebildet til hverken høyreekstremister eller ekstreme islamister, og terrortrusselen for et direkte angrep mot DNB er derfor vurdert lavere enn samfunnet for øvrig. Samtidig har DNB lokasjoner og kontorer nær kjente landemerker og potensielle terrormål i flere byer. DNB deltar også på arrangementer og konferanser som kan ha forhøyet terrorberedskap, eksempelvis Arendalsuka. Dette gjør at DNB og DNBs ansatte også kan bli utsatt for et terrorangrep gjennom å være på feil sted til feil tid.

DNB har i mange år støttet opp om mangfold, inkludering, likestilling, samt LGBTQ+ miljøet. I 2023 var DNB også hovedsponsor for Oslo Pride. Dette er et arrangement som er en del av fiendebildet til både høyreekstremister og ekstreme islamister, og Pride er ifølge PST et attraktivt mål for disse miljøene. Selv om de fleste kommentarene rundt DNBs støtte til Pride har vært positive, har det også kommet inn flere negative kommentarer blant annet gjennom DNBs sider på sosiale medier. De fleste kritiske kommentarene har også virket å støtte anti-statlige, konspiratoriske og høyreekstreme meninger. DNB opplevde også at en person som ved hovedkontoret i Bjørvika aggressivt konfronterte ansatte på bakgrunn av DNB sin støtte til Pride og LGBTQ+ miljøet. DNB har feiret Pride med flagg, deltagelse i parade og stand under arrangementer. I lys av PSTs trusselvurdering gjorde DNB flere konkrete sikkerhetsmessige tiltak for å ivareta ansattes sikkerhet i deltagelsen under arrangementet.



Innsidetrusselen – Stadig mer kompleks og mangfoldig

Gjennom 2023 har DNB observert og fulgt opp ulike former for innsideaktivitet i banken. DNB opplever blant annet informasjonstyveri gjennomført av ansatte med jevne mellomrom. De fleste kjente tilfellene av informasjonstyveri forekommer i oppsigelsesperioden der den ansatte er på vei inn i en jobb hos en ny arbeidsgiver, og dette gjelder spesielt i provisjonsbaserte stillinger. Vi har sett eksempler det siste året der ansatte tar med seg kundeliste til ny arbeidsgiver, eller deler informasjon til ny arbeidsgiver om tidligere kollegaers salgstall for å kunne bruke det i rekrutteringsøyemed. En annen form for informasjonstyveri vi har sett i løpet av 2023 er lekkasjer av intern informasjon til media. Dette er vanligvis handlinger som får små konsekvenser for DNB.

DNB har i løpet av 2023 opplevd ett tilfelle av forsøk på bevisst manipulering av selskapets datasystemer. Dette ble gjennomført av en misfornøyd konsulent med administratorrettigheter som var i oppsigelsestiden sin. Endringene ble oppdaget og stoppet før det fikk stor konsekvens, men føgte til noe nedetid på et internt system. Manipuleringen ble oppdaget av årvåkne ansatte

som meldte fra om uvanlig driftsaktivitet, samt gode deteksjons- og håndteringsverktøy¹. Sabotasje knyttes ofte til mistfornøyd ansatte som er selvmotiverte, men utgjør også en sårbarhet opp mot rekruttering fra statlige aktører. I lys av den endrede geopolitiske situasjonen har de norske EOS-tjenestene advart mot innsidere rekryert av utenlandske etterretningstjenester som tilrettelegger for sabotasje, og ikke bare informasjonsinnhenting eller økonomisk vinning. DNB er en viktig del av norsk infrastruktur innenfor finansielle tjenester, og et potensielt mål for slik virksomhet da sabotasje av DNB sine systemer vil ha stor betydning for den finansielle infrastrukturen i Norge.

DNB har ikke avdekket saker knyttet til alvorlig økonomisk kriminalitet utført eller tilrettelagt av ansatte i 2023. I løpet av 2023 har en annen norsk bank opplevd et større bedrageri fra en ansatt på rundt 75 millioner kroner², noe som viser hvor stort skadepotensiale bedrageri fra en ansatt kan utgjøre.

For organiserte kriminelle er det veldig attraktivt å ha noen på innsiden av finans- og banknæringen. Innsidere kan både aktivt hjelpe til med hvitvasking og bedragerier, men også støtte mer passivt med å gi informasjon om

dtekstjonssystemer og smutthull i regelverk og rutiner. Svensk politi har i en nylig utgitt rapport pekt på undersøkelser som viser at innsidere i bank er en viktig del av hvitvaskingen av penger for organiserte kriminelle. Ifølge samme rapport er ingen banker upåvirket av dette, da tilnærmet alle banker og finansinstitusjoner i Sverige blir aktivt og målrettet forsøkt påvirket³. Selv om Sverige står i en annen situasjon enn Norge, er det trolig mye som er likt. Det er allerede en smitteeffekt fra Sverige, og fremover vil en trolig se mer av dette også i Norge.

DNB kartlegger høyrisikoroller i konsernet for å ivareta medarbeidere og anerkjenne sårbarheten som ligger i roller med tilgang til store verdier. Dette gjelder stillinger som eksempelvis har utvidede administratorrettigheter i datasystemene, eller har brede finansielle rettigheter. Det gjennomføres utvidet bakgrunnssjekk for personer med høyrisikoroller, og disse får ekstra oppfølging og opplæring for å håndtere den ekstra risikoen som ligger i deres stillinger. Dette gjøres for å sikre DNBs verdier, men også for å unngå at ansatte blir utsatt eller er bekymret for ytre press eller påvirkning.

¹ Denne hendelsen nevnes også i delrapporten om digitale trusler

² <https://www.nrk.no/trondelag/bankvikar-tiltalt-for-underslag-av-75-millionar-kroner-forklarar-seo-i-retten-1.16657675>

³ https://polisen.se/contentassets/0808-e4fd9d0545ad9a9f22f638bfebbb/finanspolisen_informerer_banker_som_brottswerkta.pdf/download

Trusselvurdering 2024

Antall trusler mot ansatte vil fortsette på samme nivå

Det er forventet at antall trusselsaker og saker med uønsket kundeatferd forblir på samme nivå. Dette vil skyldes et vedvarende press på den personlige økonomien som mange også opplevde i 2023 og som fremstår å være en bakenforliggende årsak til flere av truslene. Ifølge politiets straffesaksregister har det i perioden 2018-2022 vært en økning i anmeldelser med et hatmotiv. Vi forventer at denne utviklingen også vil fortsette å gjenspeiles i DNB, hvor mange av sakene om uønsket kundeatferd har vært blant annet rasisme mot ansatte. Politiet vurderte det i 2023 som meget sannsynlig at vold begått av personer med alvorlige psykiske lidelser og problematisk rusmiddelbruk vil fortsette å utgjøre en betydelig trussel. Psykiske lidelser og rusmiddelbruk er som nevnt tidligere ofte det som treffer DNBs kundebehandlere og vektere i møte med hissige og aggressive kunder. DNB har i perioden 2022-2023 anmeldt betraktelig flere saker enn tidligere år og dette er med på å vise alvorligheten i sakene som DNBs ansatte opplever. Vi har også opplevd flere voldssaker og denne trenden forventes å fortsette.

DNB vil forblie et mål for aktivister på tvers av det ideologiske spekteret

Frustrasjonen blant miljøaktivistene som opplever en utilstrekkelig framgang i spørsmålet om et null-utslippsamfunn gjør at DNB grunnet våre investeringer i fossil industri vil fortsatt være et mål for protester fra miljøbevegelsen. Vi forventer at eventuelle protester mot DNB vil være av ikke-voldelig karakter og i verste fall i form av sivil ulydighet. Samtidig kan en videre fragmentering av klimabevegelsen føre til at individer og mindre grupperinger radikaliseres og gjennomfører mer alvorlig handlinger,

eksempelvis skadeverk eller vandalismus mot infrastruktur. Et annet mulig scenario er at enda mer negativ retorikk mot bank- og finansinstitusjoner, samt økonomiske nedgangstider og resesjon, blir en katalysator for protester fra andre politiske grupperinger med for eksempel anti-kapitalistisk tankegods.

Terrortrusselen mot DNB påvirkes av samfunnet for øvrig

DNB påvirkes av terrortrusselen som samfunnet for øvrig, og endringer i dette trusselbildet vil også ha konsekvenser for DNB. Vi tror ikke at DNB vil bli et prioritert mål for hverken høyreradikale eller islamistiske terrorgrupperinger det neste året. Samtidig vil DNB forsette å være en pådriver for mangfold og inkludering i årene som kommer, noe som kan øke terrortrusselen mot DNB-ansatte gjennom deltagelse på ulike arrangementer og markeringer med forhøyet terrortrussel.

Innsidetrusselen vil kunne øke

Det er flere drivere som vil kunne påvirke og øke innsidetrusselen mot bank- og finanssektoren i 2024. Stadig bedre forsvar mot digitale trusler, samt bedre deteksjon og håndtering av bedrageri, hvitvasking og sanksjoner gjør det enda mer attraktivt å ha noen på innsiden av DNB for å omgå disse mekanismene. Undersøkelser i Sverige viser at organiserte kriminelle gjenger jobber systematisk for å skaffe seg innsidere innen bankvirksomhet. Dette er noe vi kan se mer av også i Norge fremover, både for å gjennomføre bedragerier, samt bistå i hvitvaskingen av penger fra kriminelle aktiviteter.

Økonomiske nedgangstider kan gjøre det mer attraktivt å gjennomføre innsideaktivitet, da både selvmotiverte og eksternt påvirkede ofte er økonomisk motivert. Sparetiltak og omorganisering som følge av økonomiske nedgangstider vil også kunne føre til misfornøyde ansatte som gjør dem sårbare for innsideaktivitet. Arbeidstakere skifter også arbeidssted oftere nå enn for noen år siden. En utfordring med dette er at sikkerhetskultur tar tid å bygge opp, samt at personer som skifter jobb ofte ikke nødvendigvis har samme lojalitetsbånd til arbeidsgiver som en hadde tidligere.

Den geopolitiske uroen i verden vil også kunne bidra til at innsidetrusselen øker gjennom at flere både statlige og ikke-statlige aktører vil kunne se seg tjent med å ha noen på innsiden av en finansinstitusjon. Målet for disse innsiderne kan være svært ulikt og spenne fra informasjonsinnhenting, finansielle midler, sabotasje og påvirkning.

Finansiell trygghet i en usikker verden

Digitale trusler

Sammendrag

Digitale trusler er dynamiske og skiftende av natur og gjenspeiler et samfunn som har blitt stadig mer digitalisert og sammenkoblet, men også polarisert.

Til tross for økte geopolitiske spenninger og krig var 2022 uvanlig rolig for norsk finansbransje, da aktørene som i stor grad kommer fra Russland, Ukraina, og Øst-Europa var oppatt med digital aktivisme som følge av krigen. Rapporter fra forsikringsbransjen støtter dette og antall løsepengenvirusangrep, gjenopprettingskostnader og betalinger til ofre for løsepengenvirus ble redusert i 2022. Det var få som forventet at denne utviklingen skulle fortsette – og som mange forventet, ser vi nå økt aktivitet og en tilbakevending til normalen for cyberhendelser for 2023, der løsepengenvirus fortsatt er den største digitale trusselen.

DNBs Cyber Defense Center (CDC) har i løpet av 2023 håndtert 20 208 cybersikkerhetshendelser. Dette er en økning på 2 prosent fra 2022. Videre håndterte CDC 11 hendelser med høy potensiell negativ påvirkning på DNB. Dette er færre hendelser enn tidligere år og en reduksjon fra 15 alvorlige hendelser i 2022. Den primære driveren for dette er DNBs løpende moderniseringsarbeid og robusthet i konsernets IT-systemer. Et robust dybforsvar gjør at flere angrep blir stoppet i en tidligere fase, men også får lavere konsekvens. Utover dette jobbes det proaktivt med deling av trusseletterretning og erfaringer på tvers av responsmiljøene innenfor finans. Dette bidrar til økt robusthet og understøtter finansiell stabilitet i samfunnet.

De mest fremtredende hendelsene i 2023 var kjennetegnet av tredjepartshendelser, hacktivism og manipulering fra en misfornøyd konsulent. Etter 2022 har vi sett flere

tredjepartshendelser. Dette har ført til økt fokus på oppfølging av hendelser gjennom hele verdikjeden vår, uavhengig av om tjenesten driftes internt i banken eller av en tjenesteleverandør. Den kontinuerlige digitaliseringen og utstrakt bruk av skytjenester er de viktigste driverne bak denne trenden, og vi forventer at tredjepartshendelser vil bli enda mer framtredende i årene som kommer.

Når det gjelder hacktivism, ser vi økt aktivitet siden eskaleringen og krigen i Ukraina. Hacktivistgrupper som støtter Russland har rettet angrep mot selskaper i land som gir økonomisk eller militær støtte til Ukraina. Finanssektoren har opplevd flere slike angrep – også DNB. Til slutt har vi i løpet av 2023 håndtert en sak der et internt system ble bevisst manipulert av en misfornøyd konsulent. Selv om konsekvensen var minimal, representerer dette en kategori trusler som ofte underkommuniseres, men som fortjener økt oppmerksomhet og ørvåkenhet i en tid med økt polarisering og usikkerhet.

Når vi ser framover, forventer vi at bruken av kunstig intelligens vil gjøre det enklere for kriminelle aktører å skreddersy sosial manipulering, som for eksempel phishing. Dette, i kombinasjon med økt digitalisering og økt bruk av skytjenester, vil sannsynligvis føre til flere tredjepartshendelser på tvers av det som for mange organisasjoner representerer komplekse og lange verdikjeder. Større datainnbrudd hos tjenesteleverandører er en annen alvorlig bekymring, ettersom skytjenester og IT driftstjenester domineres av noen få utvalgte leverandører og dette fører til en avhengighet for de fleste bransjer og organisasjoner. Uavhengig av hva framtiden bringer, må organisasjoner være robuste, ørvåkne og tilpasningsdyktige for å håndtere trusler som utvikler seg raskere enn noen gang før.

Oppsummering 2023

Økning i antall sikkerhetshendelser – men færre med høy alvorlighetsgrad

DNBs Cyber Defense Center (CDC) har ansvaret for å oppdage, analysere og håndtere cyberangrep og IT-sikkerhetshendelser rettet mot DNB. Enheten har et beredskapsteam som følger en global 24-timers vaktordning med ansatte i ulike tidssoner. Hendelsene som ble håndtert av CDC i 2023 illustrerer noen sentrale cybertrusler, trender og sikkerhetsutfordringer som selskapet står overfor.

CDC har registrert utviklingen i sitt arbeid med sikkerhetshendelseshåndtering siden 2013. Grafen nedenfor viser at den generelle trenden er en jevn økning i håndterte hendelser fra år til år (med unntak av en korrekjon etter økt overvåking under overgangen til hjemmekontor under covid-19-pandemien). I 2023 undersøkte CDC flere potensielle hendelser enn noen gang tidligere. Totalt ble 20 208 sikkerhetshendelser analysert. Volumet av analyserte sikkerhetshendelser gjenspeiler både økt deteksjonskapasitet og et stadig mer sammensatt trusselbilde.



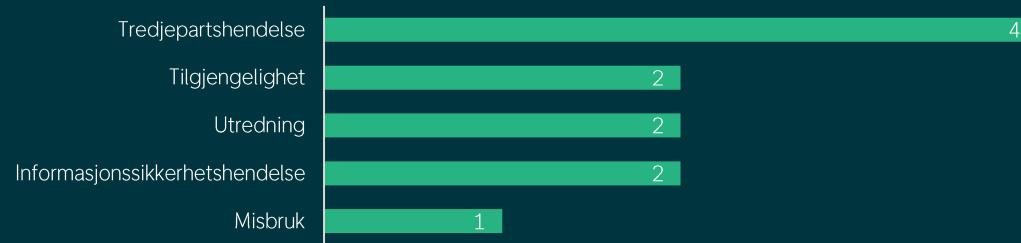
Figur 1. Svak økning, men færre hendelser med høy alvorlighet

Mens antall håndterte hendelser øker, har vi opplevd en nedgang i hendelser med høy alvorlighetsgrad de siste fire årene. Vi mener at årsakene til dette er sammensatte. I DNB har vi forbedret sikkerheten ved å øke robustheten av våre sikkerhetskontroller som en del av et dybdeforsvar, modernisering og overgang til moderne skytjenester med bedre forsvar mot dagens trusselbilde, samt økt fokus på sårbarhetshåndtering. Sikkerhetsherding og forebygging av angrep har vært et forbedringsområde for å sikre at de fleste cyberangrep stoppes før de får noen innvirkninger på banken. Sikkerhetsherding forbedrer DNBs robusthet og muliggjør en forsvarbar infrastruktur for å kunne stoppe avanserte angrepsforsøk.

I tillegg til disse interne faktorene har noen eksterne krefter sannsynligvis også bidratt til nedgangen i hendelser med høy alvorlighetsgrad. Noe av dette kan forklares ved at de fleste cyberkriminelle er opportunistiske og vil velge de enklere målene – eller rett og slett et mål som er mer tilgjengelig.



Figur 2. Hendelsesoversikt

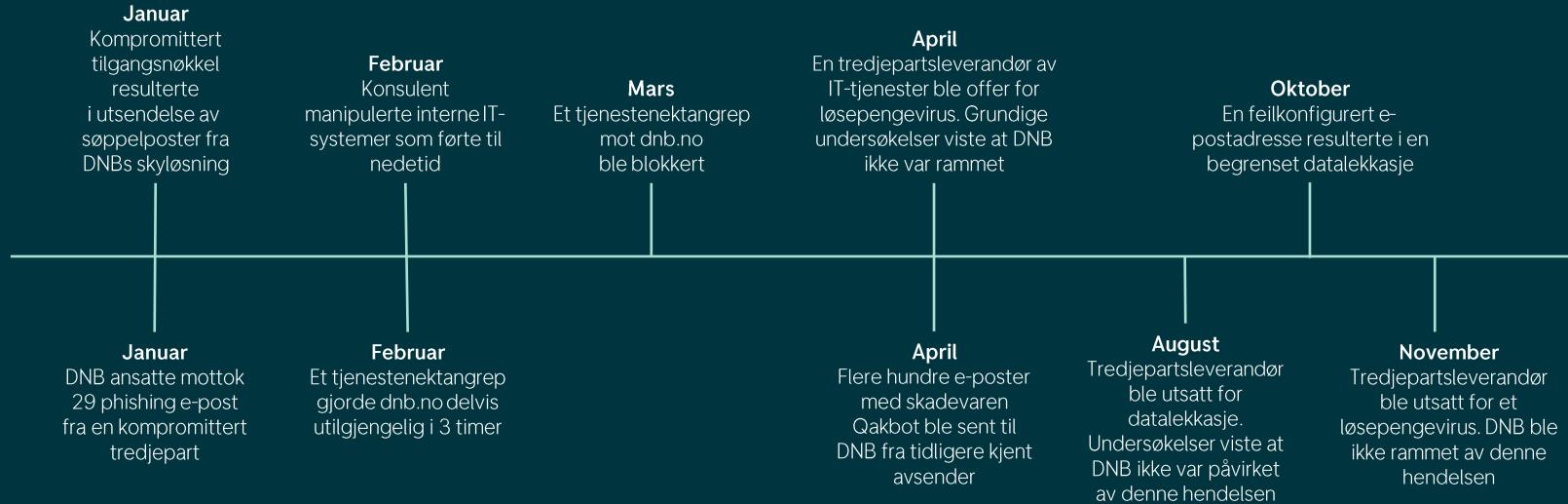


Figur 3. Kategorioversikt alvorlige hendelser

Det er også noen generelle endringer i det digitale trusselbildet. Russiske cyberkriminelle har vært aktive på andre fronter siden tidlig 2022, og digitale bankran blir hovedsakelig utført mot kryptobørsen. DNB ser at antallet digitale banktransforsøk har avtatt, mens angrep mot kryptoplatfromer har økt. Til slutt kan det være at cyberkriminelle gjennomfører færre, men større cyberangrep. I løpet av de siste årene har det vært mange rapporter om store leverandørkjedeangrep og svært alvorlige hendelser med løsepengenvirus. Det ser ut til at noen av de mest avanserte cyberkriminelle foretrekker å gjennomføre færre, men større angrep mot tjenesteleverandører. Dette for å treffe flere mål og motta større utbetaling, i stedet for flere mindre angrep.



Hendelser



Figur 6. Tidslinje med beskrivelse av et utvalg sentrale hendelser håndert av DNB Cyber Defense Center i 2023.

Det digitale trusselbilde er i stadig endring

Det digitale trusselbildet endrer seg kontinuerlig og har i økende grad blitt et samfunnsprosblem, da cyberangrep påvirker ordinære tjenester vi tar for gitt, samtidig som personopplysninger eksponeres og blir lekket. For selskaper kan cyberangrep føre til betydelig skade med konsekvenser som tap av omdømme, tapte inntekter, forpliktelser overfor kunder og tilgjengelighet av finansielle tjenester. Nedenfor er et utvalg av nøkkelhendelser som ble håndtert av CDC i 2023, samt en kort beskrivelse av nøkkelhendelsene og hendelser som ble håndtert av konsernets funksjon for håndtering av sikkerhetshendelser. Disse digitale truslene blir vurdert og i detalj, og delt inn i følgende digitale trusselkategorier:

- Løsepengevirus
- Phishing
- Tjenestenektangrep
- Tredjepartshendelser
- Menneskelig svikt og systemkonfigurasjonsfeil

Løsepengevirus fortsatt den største truselen

Vi anser løsepengevirus som den største og mest alvorlige digitale truselen som DNB står overfor. Kostnadene og omfanget av løsepengevirusangrep har

stadig vokst over flere år, og vi forventer at denne trenden vil fortsette inn i 2024. Årsakene er sammensatte, men hovedsakelig er det fordi løsepengevirus fungerer, og mange selskaper velger å betale når slike cyberhendelser setter driften og hele virksomheten i fare. I tillegg er rettsforfølgelse av aktørene bak løsepengevirus svært vanskelig, og krever vanligvis mange årsverk og samarbeid mellom flere internasjonale politistyrker. Risikoen for straffeforfølgelse er dermed lav. På samme måte som for tjenestenektangrep, har DNB en svært høy suksessrate når det gjelder å avverge slike angrep. Likevel er de potensielle konsekvensene av slike hendelser så store at løsepengevirus er vår største cybertrussel.

I løpet av de siste årene har det vært mange saker der høyt profilerte selskaper har blitt utpresset gjennom løsepengevirus. Det første sikkerhetsbruddet skjer stadig oftere gjennom et leverandørkjedeangrep der en kjent tredjepart er det første offeret.

Phishingvolumene øker, men gir lite utslag

Mange cyberangrep begynner med en e-post, og vi ser vedvarende høye nivåer av phishing, spear phishing og forsøk på digital spionasje og informasjonstyveri mot DNB. I 2023 ble utrolige 44 millioner innkommende e-

poster stoppet fra å nå DNBs ansatte på grunn av lav troverdighet (hovedsakelig spam).

Det tilsvarer 120 000 e-poster hver dag, eller et daglig gjennomsnitt på 11 per ansatt. Omrent 25 millioner e-poster der avsenderen utga seg for å være fra DNB, ble hindret fra å nå sine tiltenkte ofre på grunn av implementeringen av nye sikkerhetstiltak for e-post.

I tillegg til disse tallene ble 177 000 innkommende phishing-e-poster til DNB stoppet, da en automatisk sikkerhetsanalyse fastslo at innholdet var skadelig. Dette er en økning fra 120 000 året før. Hovedformålene med disse phishing-meldingene var tyveri av personopplysninger, etterfulgt av løsepengevirus og eksfiltrering av data.

DNB stopper slike e-poster før de når mottakeren i mer enn 99 prosent av tilfellene, men vi må være ørvåkne, da de potensielle konsekvensene av et vellykket phishing-angrep kan være svært alvorlige. Vi forventer at trenden med fortsatt økning i phishing-meldinger og angrepsforsøk via e-post vil fortsette i 2024.

Politiske tjenestenektangrep (DDoS) fortsetter, men er hovedsakelig støy

Vi ser sporadiske forsøk på tjenestenektangrep mot DNB. Det var en massiv økning i det generelle volumet av slike cyberangrep etter eskaleringen av krigen i Ukraina i 2022, og det er en kjent taktikk for russiske cyberkriminelle grupper. Disse gruppene pleier å velge et nytt land eller en ny sektor etter noen få dager, og CDC overvåker aktivt denne trusselen.

Siden begynnelsen av 2023 har nordiske finansinstitusjoner opplevd en økning i tjenestenektangrep, ettersom angrep mot finansinstitusjoner oppfattes som en effektiv måte å påvirke det sivile samfunn på. DNBs DDoS-forsvar er robust og klarer å stoppe de fleste angrep før banken blir påvirket. Av denne grunn, selv om vi forventer at forsøk på tjenestenektangrep vil fortsette, anser vi det som lite sannsynlig at disse angrepene vil påvirke vår virksomhet eller våre kunder. Det er likevel viktig å være klar over at selv om beskyttelsesgraden vår er veldig høy, er de potensielle konsekvensene av et vellykket tjenestenektangrep alvorlige, da de kan føre til at kundetjenester blir utilgjengelige.

Tjenestenektangrep utføres sporadisk mot banken, der målet er å skape forstyrrelser og gjøre tjenestene våre utilgjengelige. Vi så flere slike forsøk i 2023, eksempelvis erfarte vi i februar et tjenestenektangrep i kombinasjon med en feilkonfigurasjon av sikkerhetssystemer ført til tre timers nedetid for dnb.no. Totalt sett ble fem tjenestenektangrep mot banken håndtert i 2023. De fleste av disse angrepene var lite sofistikerte, og påvirkningen var begrenset

DNB ble utsatt for et tjenestenektangrep i midten av februar. Angrepet ble raskt forhindret av konsernets forsvarsmekanismer. Imidlertid ble legitim trafikk også blokkert på grunn av en sikkerhetskontroll utført av en leverandør i verdikjeden, noe som resulterte i sporadisk nedetid på tjenester tilknyttet dnb.no i en periode på tre timer. Selv om det ikke var mulig å tilskrive dette angrepet til en spesifikk gruppe, var russiske hacktivister åpne om at de utførte tjenestenektangrep mot svenske banker i samme tidsrom.

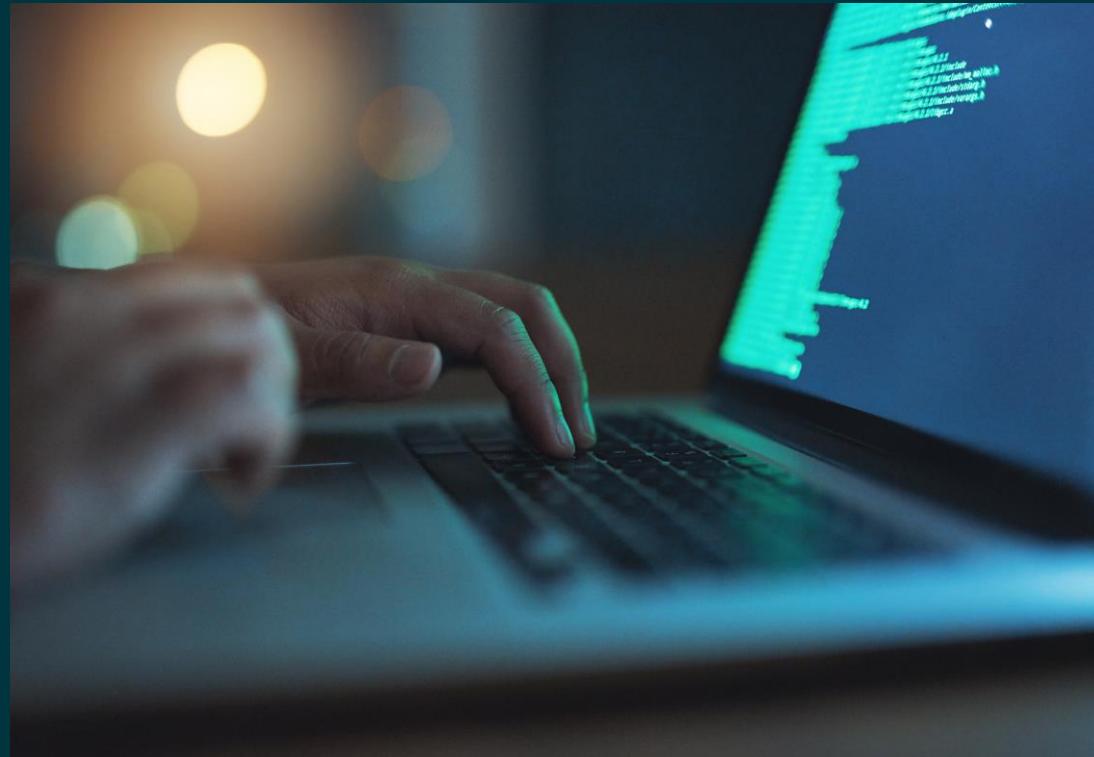
Den 2. mars, i et par minutter rundt kl. 03:00, ble et relativt lite tjenestenektangrep automatisk forhindret av våre DDoS-beskyttelsestjenester og hadde ingen innvirkning. Angrepet var sannsynligvis en test for å sjekke vår DDoS-beskyttelsesevne og kan ha blitt utført i forkant av en større tjenestenektangrep av den pro-russiske hacktivistgruppen «NoName057(16)» mot norske enheter den påfølgende morgenen. I løpet av 2. mars angrep hackergruppen ca. 10 norske virksomheter på grunn av norsk støtte til Ukraina i krigen mot Russland. Den 3. mars gikk gruppen videre til mål i andre land.

Den 25. mars ble dnb.no rammet av et lite tjenestenektangrep som varte i et par minutter. Mesteparten av trafikken ble blokkert, og DNBs tjenester ble ikke påvirket.

Stadig flere cyberangrep starter hos en tredjepart

CDC håndterer flere undersøkelser for datainnbrudd og hendelser i tilknytning DNBs leverandører i et verdikjedeperspektiv. Dette er en fortsatt økning fra fjoråret og en framvoksende trussel på grunn av økt digitalisering og et sammenkoblet samfunn.

Det siste året har vært preget av at mange av våre større undersøkelser har dreid seg om å forhindre konsekvenser av tredjepartshendelser. Slike hendelser spenner fra phishing-e-poster sendt fra betroddde partnere etter at e-postkontene deres ble kompromittert, til IT-tjenesteleverandører som blir kompromittert i cyberangrep. Det kan være svært utfordrende å etterforske slike saker. Konsekvensen av slike hendelser for DNB har til nå vært begrenset til minimale driftsforstyrrelser der vi har måttet stenge tilganger eller tjenester som er eksponert for tredjeparter påvirket av cyberangrep. Rask håndtering og god kommunikasjon med våre leverandører har redusert risiko for spredning av cyberangrep fra leverandørens systemer til DNBs systemer. Det har ikke vært noen datalekkasjer forårsaket av tredjepartshendelser i 2023.



Tredjepartshendelser håndtert av DNB i 2023

- ***Business Email Compromise (BEC) – januar***

Totalt ble det sendt 29 phishing-e-poster til DNBs ansatte fra en kompromittert, betrodd tredjepart. To brukere klikket på lenker, men ble hindret fra å få tilgang til skadelig innhold av sikkerhetsinnstillingene i nettleserne deres.

- ***Konsulent manipulerte interne IT-systemer – februar***

Etter neden tid i et spesifikt IT-system en helg, ble det oppdaget at en misfornøyd konsulent med administrative rettigheter bevisst hadde manipulert systemkonfigurasjoner og innstillinger for datalagring. Dette resulterte i begrenset neden tid for tjenester knyttet til overføring av data mellom interne systemer.

- ***Fleire tilfeller av Business Email Compromise (BEC) – april***

I april rapporterte flere ansatte at de mottok mistenkelige e-poster fra kjente kontakter, der e-posten var en fortsettelse av en tidligere e-posttråd, men fra en forfalsket avsender. Undersøkelser avdekket forsøk på levering av hundrevis av slike e-poster til våre ansatte. Disse e-postene inneholdt lenker som ville ha ført til forsøk på nedlasting av skadegjørende kjent som Qakbot, som er kjent for å bli brukt som det første steget i løsepengevirusangrep. Denne hendelsen hadde ingen konsekvenser for DNB, da det skadelige innholdet ble uskadeliggjort av sikkerhetskontroller i e-postsystemene.

- ***Tredjeparts cybersikkerhetsbrudd – april***

Det skjedde et tredjepartsbrudd hos en nordisk IT-tjenesteleverandør den 25. april,

og DNB ble klar over bruddet den 4. mai. DNB ble ikke påvirket, men vi iverksatte proaktive sikkerhetstiltak for å forhindre eventuell skade som følge av bruddet hos leverandøren. Dette påvirket tilgjengeligheten til en mindre DNB tjeneste, som var tilgjengelig for rundt 5 000 kunder i fire og et halvt døgn. DNB rapporterte hendelsen til Finanstilsynet.

- ***Datainnbrudd hos tredjepart – august***

Angrepet var rettet mot en spesifikk gruppe av leverandørens kunder i et forsyningsskjedeangrep, men undersøkelser avdekket at det ikke hadde noen innvirkning på DNB.

- ***Sårbarhet i skytjeneste (SaaS) – oktober***

En nulldagssårbarhet i noen konfigurasjoner av ServiceNow ble offentliggjort i midten av oktober. En uautorisert bruker benyttet seg av sårbarheten til å hente ut spesifikke datasett (rutinenavn og skjemanavn) fra noen av de forhåndsinstallerte plattformoppsettene til ServiceNow, inkludert en løsning som ble brukt av DNB. Sårbarheten ble raskt håndtert etter at den ble oppdaget, og det ble fastslått at de potensielt eksponerte dataene var av begrenset interesse, og konsekvensene av eksponeringen var lav.

- ***Løsepengevirusangrep hos tredjepart – november***

Selskapet ble rammet av et løsepengevirus fra hackergruppen LockBit i november. Selskapet er en leverandør til DNB, men det ble bekreftet ved undersøkelser at DNB ikke ble påvirket av denne hendelsen.



Menneskelige svikt og systemkonfigurasjonsfeil

Menneskelig svikt er årsaken til mange IT- og cybersikkerhetshendelser. Noen ganger skjer disse feilene i designet eller vedlikeholdet av systemet. IT-bransjen har blitt svært profesjonalisert og granulert, der det finnes tusenvis av spesialiseringer. Nedenfor er tre eksempler på slike hendelser som ble håndtert av DNB i 2023. Vi vil fortsette vår innsats for å forhindre og håndtere slike hendelser, men vi må erkjenne den iboende utfordringen og trusselen som ligger i komplekse IT-systemer – og de grunnleggende sårbarhetene til menneskene som bruker disse.

Kompromittert e-postkonto – januar

AWS varslet DNB om spam fra en test-e-postkonto. Totalt ble det sendt 50 000 spam e-poster fra en DNB-e-postadresse på grunn av den utilsiktede lekkasjen av en tilgangsnøkkel på et eksternt nettsted. Hendelsen ble rapportert til Finanstilsynet, men hadde ingen konsekvenser for DNB da den raskt ble håndtert og ingen konfidensielle eller personlige data var tilgjengelige gjennom den eksponerte kontoen.

Feilkonfigurasjon av tilgangsrettigheter – januar

Den 16. januar fikk 67 interne DNB-brukere tilgang til en

spesifikk privilegert tilgangsrolle. Dette skyldtes en misforståelse og menneskelig svikt. Tilgangene ble fjernet innen noen få timer, og det ble gjennomført en intern revisjon. Revisjonen viste at ingen tilgangsopplysninger hadde blitt eksponert eller misbrukt. Saken ble rapportert til Finanstilsynet.

Datalekkasje grunnet systemkonfigurasjonsfeil – oktober

En systemkonfigurasjonsfeil førte til at banken sendte systemoppdateringer til en feilaktig e-postadresse, noe som resulterte i en utilsiktet datalekkasje. Da dette ble oppdaget, ble det gjennomført tiltak for å rette opp i problemet. Hendelsen ble rapportert til Datatilsynet og Finanstilsynet.

Trusselvurdering 2024

Som tidligere år vurderer vi at det er meget sannsynlig at det er økonomisk motiverte organiserte cyberkriminelle som kommer til å utgjøre den største digitale trusselen mot DNB i 2024. Av de anvendte angrepsteknikkene anser vi leverandørkjedeangrep og løsepengevirusangrep som cyberangrepene med høyest skadepotensial, og at trusselen øker.

Løsepengevirus er fortsatt den største digitale trusselen

Kostnadene og omfanget av løsepengevirus – når de skjer – har økt jevnt over flere år, før en markant nedgang i 2022. I 2023 økte slike angrep til nye høyder, og vi forventer at denne trenden vil fortsette inn i 2024. Dette gjør løsepengevirusangrep til den største digitale trusselen mot DNB, selv om en slik hendelse anses som mindre sannsynlig på bakgrunn av robuste sikkerhetskontroller.

Kunstig Intelligens (KI) vil føre til mer effektiv sosial manipulering

Med den raske veksten og bruken av KI-tjenester forblir sosial manipulering en svært relevant angrepsteknikk og kan bli enda vanskeligere å oppdage. Phishing-e-poster utformes og tilpasses mer spesifikt for hver enkelt mottaker, og klikkratene kan øke som et resultat av dette. Opplæring i IT-sikkerhet og regelmessige phishing-tester er et effektivt risikoreduserende tiltak og kan motvirke noe av den økte risiko fra KI-drevne forbedringer av sosial manipulering.

Tredjepartsrisiko vil fortsette å øke

Det er sannsynlig at angrepsteknikkene som leverandørkjede- og tredjepartsangrep vil fortsette å øke i framtiden. Vellykkede angrep gir mulighet til å treffe mange eller godt sikrede mål. Trusselaktøren kan kompromittere ett selskap og utnytte deres legitime tilgang til andre selskaper. I tillegg representerer driftsstans hos kritiske skytjenester en ytterligere tredjeparts cyberrisiko som vi antar vil fortsette å vokse i årene som kommer, i tråd med global digitalisering i samfunnet.

Geopolitisk uro vil fortsette å påvirke digitale trusler

Endringer i det digitale trusselbildet har blitt drevet av geopolitiske spenninger og deres direkte og indirekte konsekvenser. Hackere fortsetter å bruke cyberangrep som en del av politiske og aktivistiske agendaer, rettet mot både private og offentlige institusjoner. I 2023 så vi fortsatt hacktivismisme i forbindelse med krigen i Ukraina, samt eskaleringen av krigen mellom Israel og Palestina. Disse to konfliktene fortsetter inn i 2024, og vi kan anta at disse konfliktene – og andre eventuelle geopolitiske forhold som måtte oppstå i 2024 – fortsatt vil påvirke det digitale trusselbildet.

Finansiell trygghet i en usikker verden

Internasjonale sanksjoner

Sammendrag

DNB er underlagt flere sanksjonsregelverk på grunn av sin internasjonale virksomhet. Antallet sanksjonerte personer, grupper og selskaper («listeførte») øker, og har spesielt tiltatt etter Russlands invasjon av Ukraina. Det medfører økt risiko for at det forsøkes gjennomført transaksjoner som er underlagt frysforpliktelse gjennom DNB.

DNB hadde i starten av 2022, i forkant av invasjonen av Ukraina, lav direkte kreditt-eksponering mot Russland. Den ikke-finansielle eksponeringen har blitt redusert i takt med at sanksjoner er innført mot landet. DNB ser også et markant fall i antall transaksjoner hos bedriftskundegrupper som tradisjonelt har hatt transaksjoner med Russland.

Geopolitiske spenninger og stormaktkonflikt kan medføre økt bruk av virkemidler som sanksjoner. Sanksjonerte regimer kan utnytte cyberkriminelle for å få tilgang til midler. DNB ser derfor sanksjonsetterlevelse i sammenheng med et større utfordringsbilde, med illegitime og ulovlige transaksjoner.

Internasjonale sanksjoner

Sanksjoner er en samlebetegnelse for ikke-militære tiltak som innføres av stater eller internasjonale organisasjoner, som for eksempel EU og FN, som del av deres utenriks- og sikkerhetspolitikk. Det innebærer at det innføres økonomiske, diplomatiske eller andre typer restriksjoner som begrenser handlefriheten eller rettighetene til en stat, grupper, enkeltpersoner, selskaper eller andre enheter. Formålet med sanksjoner er å påvirke adferden til aktøren det innføres sanksjoner mot, ved å fremvinge endring

gjennom økonomiske incentiver eller å begrense aktørens økonomiske og materielle evne til å begå de uønskede handlingene.

Økonomiske frystiltak er en utbredt form for sanksjoner. Dette virkemiddelet benyttes av blant annet FN, EU og USA. Frystiltak rettes i all hovedsak mot enkeltpersoner eller selskaper som er direkte involvert i handlingene det reageres mot. Det gjøres ved at personene eller selskapene oppføres på en liste under det aktuelle sanksjonsregimet. Dette omtales gjerne som å være «listeført».

Frystiltakene innebærer påbud om at listeførtes penger eller formuesgoder skal fyses, og forbud mot å stille til rådighet eller gjøre tilgjengelig penger eller formuesgoder for vedkommende. Det kan typisk innebære å sperre tilgang til en bankkonto og forvaltede midler, eller at en transaksjon blir stanset.

Oppsummering 2023

DNBs ansvar og rolle i etterlevelsen av frystiltakene

Hver dag går flere titalls tusen transaksjoner til og fra Norge gjennom DNB. Som Norges største finansforetak, en av verdens største shippingbanker, og med betydelig internasjonal tilstedeværelse, har DNB en unik posisjon i både det norske og det internasjonale finanssystemet.

Tilgang til det internasjonale finanssystemet er avgjørende for at både forretninger og privatpersoner skal kunne håndtere sine forpliktelser.

Dette gjør at DNB har en viktig rolle i å påse etterlevelse av frystiltakene. DNB skal bidra til å forhindre at listeførte får tilgang til midler som er underlagt frystiltak. I tråd med kravene i den norske hvitvaskingsforskriften har DNB blant annet et elektronisk overvåkningssystem for å identifisere kunder og transaksjoner tilknyttet personer og enheter som er underlagt sanksjoner og restriktive tiltak gjennomført i norsk rett¹. Dette innebærer at vi «screener» kunder og transaksjoner mot lister over sankjonerte personer og entiteter.

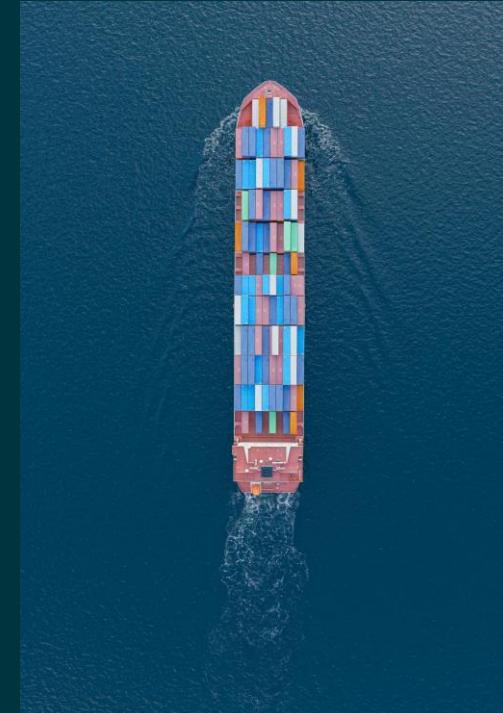
Treff i sankjonsscreeningen mot listeførte kan også utløse

undersøkelsesplikt etter hvitvaskingsloven. Der det er mistanke om at midler kan stamme fra brudd på sanksjonsregelverk, og dermed utgjøre mulig hvitvasking eller terrorfinansiering, vurderer DNB dette også i henhold til kravene om undersøkelse og rapportering i hvitvaskingsloven. Se årsrapport AML i denne publikasjonen.

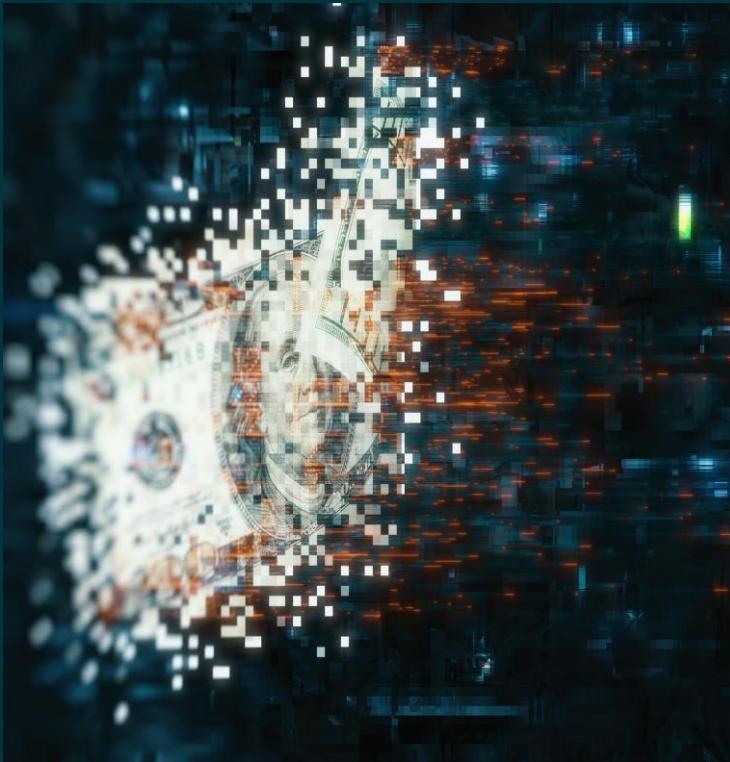
DNBs ansvar etter frysforpliktelsen

DNB er i henhold til norsk lov forpliktet til å fryse midlene til listeførte personer og selskaper som er underlagt økonomiske frystiltak. Det innebærer at dersom DNB i transaksjonene som screenes får treff mot en listeført person eller et selskap, stanses transaksjonen til treffet er avklart.

Dersom treffet er positivt – altså om en av partene i transaksjonen er den listeførte – fryses midlene på en egen konto. Midlene kan kun friges etter at Utenriksdepartementet har gitt en tillatelse. Det er normalt den som har fått midlene sine fryst som må fremme søknad til Utenriksdepartementet om frigivelse i henhold til unntakene i forskriften.



¹ Hvitvaskingsforskriften § 7-3.



Datakraft og hjernekraft

Det høye antallet grensekryssende transaksjoner som går gjennom DNB hver dag, krever et omfattende, elektronisk system for screening mot sanksjonslister. Hvis systemets logikk tilsier at en transaksjon må undersøkes nærmere, for eksempel der mottaker har samme navn som en listeført person, går en alarm og transaksjonen vurderes manuelt av fagspesialister. De fleste transaksjoner avklares etter en innledende sjekk, men i noen tilfeller må transaksjonen undersøkes nærmere.

I takt med at antallet listeføringer har økt, har også antallet alarmer som må vurderes og avklares manuelt økt. Måneden etter at Russland invaderte Ukraina og den første bølgen med sanksjoner mot Russland ble vedtatt, økte antallet alarmer som krevde nærmere undersøkelse med 27 prosent. Dette innebar både en økning i reelle treff på sanksjonslister og treff som ble undersøkt og avklart som falske positive.

For å unngå at økningen i antallet listeførte fører til uhåndterlige volumer av falske positive alarmer,

jobber DNB kontinuerlig med å tilpasse det elektroniske screeningsystemet, for å forsterke treffsikkerheten i sanksjonsscreeningen og redusere falske positive treff. På grunn av dette arbeidet med treffsikkerheten i DNBs elektroniske screeningsystem, har ikke økningen i antall listeførte ført til markant økt arbeidsmengde over tid. På samme tid ser DNB en økning i antallet saker som sendes til utvidet undersøkelse, altså saker hvor en analytiker må innhente og sammenstille informasjon for å avklare treff.

Undersøkelser av om en alarm er et reelt treff på en listeført eller ikke, kan være utfordrende. Det krever medarbeidere med god fagkunnskap på sanksjonsområdet og analytiske evner, noe DNB har og vektlegger i rekrutteringen.

Sanksjonene mot Russland

Årene 2022 og 2023 har spesielt vært preget av sanksjoner som følge av krigen mot Ukraina.

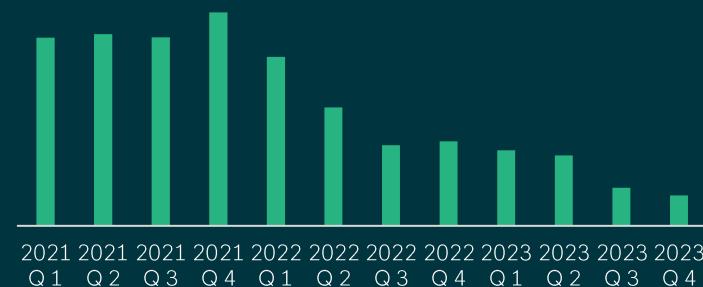
I dag er Russland verdens mest sanksjonerte land målt i antall listeførte. Sammenliknet med 31.12.2021 har antall listeføringer økt svært kraftig. Det oppføres stadig nye personer og enheter på sanksjonslistene vedtatt av EU, USA, Storbritannia og andre land. Mens det er betydelig overlapp mellom disse listene, er det mange eksempler på listeføringer fra én, men ikke alle partene. Som eksempel har EU per desember 2023 listeført rundt 1 950 russiske personer og entiteter. USA har på sin side listeført i overkant av 2 000 selskaper og organisasjoner i tillegg til et stort antall personer, noe som indikerer et betydelig gap mellom EUs og USAs lister.

DNB hadde i utgangspunktet lav direkte kredittekspesjonering mot Russland i forkant av invasjonen av Ukraina. Denne eksponeringen er nå borte. Sanksjonene innført mot landet har også redusert den ikke-finansielle eksponeringen

vesentlig, ved at antallet transaksjoner fra Norge til Russland som går gjennom DNB har gått kraftig ned etter februar 2022.

Siden fjerde kvartal 2021 er volumet av transaksjoner hvor mottaker har bank i Russland blitt redusert med rundt 85 prosent. Nedgangen har vært gradvis som følge av stadig flere sanksjonspakker som har rammet nye deler av den russiske økonomien, og en økning i antallet listeførte russiske personer og selskaper. Det er også en markant endring i hvilken valuta handelen foregår i.

DNB oppfordrer alle kunder til å sette seg godt inn i regelverket, herunder hvilke forbud som gjelder for handel med Russland, hvilke leveranser som krever tillatelse fra UD før eksport eller import, og hvilke utenlandske aktører det ikke er tillatt å handle med.



Figur 1. Utvikling i utgående betalinger til Russland, 2021-2023



Figur 2. Betalinger til Russland, fordelt på næringer

Geopolitiske spenninger og sanksjonsbruk

Den over tid kraftige økningen i bruken av sanksjoner som utenriks- og sikkerhetspolitisk virkemiddel, og økende kompleksitet i sanksjonsregimer, skyldes flere forhold internasjonalt.

Globale, multilaterale fora og arenaer for samhandling er påvirket av geopolitiske spenninger. Som eksempel har FN-sikkerhetsråd ikke vedtatt nye internasjonale, folkerettlig bindende sanksjoner for å adressere kriser som har brutt ut i løpet av 2023, eksempelvis borgerkrigen i Sudan². Lederen for FN-s generalforsamling har påpekt at organisasjonen i økende grad er "paralyseret"³. Dette gir økt rom til stater eller allianser av stater som innfører mer unilaterale virkemidler, og økt samarbeid og koordinering av sanksjoner mellom stater som USA og Storbritannia etter invasjonen i Ukraina. Videre er G7-landene en viktig premissgiver for utarbeidelse av nye sanksjoner mot Russland. Ved å koordinere utarbeidelsen av nye sanksjonspakker gir det større effekt ved implementeringen. Samtidig er det en rekke land i verden som ikke følger europeiske eller amerikanske sanksjoner mot Russland, noe som har medført endringer i russiske handelsmønstre.

Frontene i verden er svært tilspisset. Mens Russlands invasjon av Ukraina medførte en internasjonal sjokkbølge og en eksponentiell vekst i antallet sanksjoner innført mot landet, er også de pågående spenningene mellom Kina og USA en kilde til økende sanksjonsbruk – og det fra begge kanter. USA har eksempelvis innført sanksjoner mot det kinesiske selskapet Huawei for å hindre deres tilgang til viktige mikrobrikker. Videre har USA innført sanksjoner mot kinesiske embetsmenn for brudd på menneskerettighetene mot minoritetsgruppen Uigur-folket i Kina. Kina har ført opp amerikanske selskaper på egne sanksjonslister samt vedtatt egne frysbestemmelser.

Til sist vedtas det i økende grad sanksjoner mot personer som er involvert i cyberkriminalitet, terrorisme, korruption eller menneskerettsovergrep. For eksempel gir USA-s Magnitsky Act hjemmel til å sanksjonere personer involvert i korruption. Storbritannia har tilsvarende lovverk, mens EU vedtok i 2023 å innføre liknende hjemler. I diskusjonene om å styrke unionens innsats mot korruption er det varslet at jurisdiksjoner oppført på EUs liste over skatteparadiser eller som er forbundet med høy hvitvaskingsrisiko kan komme i målskiven for sanksjoner.

EUs sanksjoner mot Russland er preget av at ulike medlemsland har ulike interesser. Dette bidrar til økt kompleksitet i regelverket. Et eksempel er EU og G7-landenes pristak på russisk olje og oljeprodukter hvis formål er å begrense Russlands inntekter, samtidig som oljemarkedet globalt skal holdes i balanse. I forhandlingene om dette virkemiddelet krevde Polen og de baltiske statene et lavere pristak, mens shippingnasjoner eksponert mot Russisk oljetrafikk som Hellas, Kypros og Malta, krevde et høyere pristak. Kompromisset ble å vurdere pristaket hver annen måned.

Det blir stadig mer krevende å forutse omfang og innhold i sanksjonsregimer og hvilke parter som støtter opp om nye sanksjoner. Det er også verd å merke seg myndighetenes økte fokus på å forebygge at sanksjoner omgås, som blant annet har kommet til uttrykk gjennom nye lovbestemmelser og myndighetsveileddninger om «omgåelsesmodus» og «røde flagg» for å avdekke sanksjonsomgåelse. Omgåelse av sanksjoner er et selvstendig forbud under sanksjonsregimene vedtatt av eksempelvis EU, Norge, UK og USA. Det vil si at det er forbudt å forsettlig delta i aktiviteter som har som formål eller virkning å omgå sanksjonene.

² Sikkerhetsrådet har i løpet av 2023 likevel oppnådd enighet om forlengelse av flere allerede eksisterende sanksjonsregimer, men har ikke lykkes i å forlenge andre, som sanksjonsregimet mot Mali (Russland nedla veto).

³ Security Council reform a must, to end 'paralysis' | UN News

Trusselvurdering 2024

For DNB er den største trusselen at sanksjonerte aktører forsøker å benytte banken for å få tilgang til midler de ikke skal ha. Også geopolitisk utvikling skaper uforutsigbarhet på sanksjonsfeltet.

Den store økningen i antallet listeførte medfører økt trussel for at det gjennomføres transaksjoner underlagt frysforpliktelser gjennom DNB. Listeførte vil svært sannsynlig være kreative i innsatsen for å oppnå tilgang til det internasjonale finanssystemet.

Transaksjoner kan gjerne gå gjennom flere ledd før de ender opp hos en motpart. Flere rapporter viser til økt etablering av russisk tilknyttede selskaper i en rekke land, også i NATO-land. De russiske handelsstrømmene har endret seg, og rutes via nye tredjeparter. Dette innebærer en risiko for at norske aktører med hensikt eller uforvarende involveres i sanksjonsomgåeler.

Ulike risikoområder som fremover kan påvirke hverandre, er knytningen mellom sanksjoner og bedragerier, eller andre former for kriminalitet utført på nett. En trussel er at aktører underlagt sanksjoner benytter seg av profesjonelle cyberkriminelle for å få tilgang til midler, og at inntektene fra bedrageriene deretter hvitvaskes inn i den legale økonomien. Nord-Koreas tyverier av kryptovaluta for å finansiere landets atomprogram, noe som i perioden mellom januar og august 2023 genererte inntekter på anslagsvis USD 200 millioner, er et eksempel på en fremgangsmåte som flere sanksjonerte stater kan tenkes å benytte seg av.

Geopolitisk utvikling

Når sanksjoner benyttes som et virkemiddel for geopolitisk posisjonering, øker det usikkerheten DNB og andre finansinstitusjoner må håndtere. Den pågående utviklingen

forholdet mellom Kina og USA/Europa er et godt eksempel på hvordan handel, sikkerhetspolitikk og geopolitikk påvirker hverandre, og bidrar til slik usikkerhet. I tillegg til at handelsrestriksjoner mot Kina strammes til og blant annet begrenser Kinas tilgang til teknologier og produkter som kan tenkes å bidra til Kinas militære utvikling, har også Kina et omfattende lovverk i den såkalte "Anti-foreign sanctions law" som hjemler vidtrekkende tilsvær. Kinesiske myndigheter har tidligere vist vilje til å ta slike virkemidler i bruk som straffereaksjon mot land som utfordrer kinesiske interesser.

Til tross for tegn til en mer konstruktiv dialog mellom kinesiske og amerikanske myndigheter mot slutten av 2023, er forholdet fremdeles preget av sterke, underliggende spenninger. Det fremstår eksempelvis som lite sannsynlig at Kina vil skrinlegge ambisjonene om å oppnå kontroll over Taiwan, et krav som er nedfelt i kinesisk lov. En alvorlig tilspissing i forholdet mellom Kina og vestlige nasjoner som følge av Taiwan-spørsmålet vil øke sannsynligheten for det innføres sanksjoner og andre handelsrestriksjoner mot deler av den kinesiske økonomien. Et amerikansk lovforslag om sanksjoner mot Kina, dersom landet skulle forsøke å ta kontroll over Taiwan med makt, er blitt fremmet i Kongressen og Senatet. Om innført kan slike sanksjoner bli fulgt av omfattende kinesiske mottiltak mot stater som slutter seg til et sanksjonsregime mot landet. Både DNB og våre kunder kan dermed komme i krysspress mellom vestlige sanksjonsregimer og andre handelsrestriksjoner, og kinesiske politiske mottiltak, dersom den geopolitiske situasjonen tilspisser seg mellom Kina og vestlige land.

Av vestlige, også norske, myndigheter, har de geopolitiske spenningene blitt oppsummert som at *Om Russland er stormen, er Kina klimaendringene*. Dette kan også være beskrivende for sanksjonsbildet.

Finansiell trygghet i en usikker verden

Hvitvasking og terrorfinansiering

Sammendrag

DNB rapporterte i 2023, 2 563 forhold til Økokrim på grunnlag av mistanke om hvitvasking. Dette er det høyeste antall forhold DNB noensinne har rapportert.

Antall rapporterte forhold økte med 37 prosent sammenlignet med 2022 og er fordoblet siden 2020. Årsaken til veksten i antall rapporterte forhold i 2023 er i hovedsak:

1. Sterk vekst innen visse kriminalitetsformer - spesielt hvitvasking fra digitale bedragerier der vi har sett en dobling hvert halvår siden 2020
2. Mer effektiv transaksjonsmonitorering – i 2023 avdekket vi 50 prosent flere saker gjennom transaksjonsmonitorering sammenlignet med i 2022
3. Økt fokus og forståelse av hvitvasking – vi ser at sakene som rapporteres internt er relevante og at en økende andel rapporteres videre til Økokrim

Sett mot antall kunder rapporterte DNB mer enn dobbelt så mange kunder i bedriftssegmentet som i personsegmentet. Dette er i tråd med risikovurderingene til DNB og naturlig da det kan være mer egnet å hvitvaske midler gjennom en bedriftskonto (eks. gatekjøkken, bilvask og transportfirma) enn et ordinært personkundeforhold.

Den viktigste trusselen på hvitvaskingsområdet nå er hvitvasking av utbytte fra digitale bedragerier. I år beregner vi at mer enn 330 millioner kroner fra bedrageriutbytte vil bli forsøkt hvitvasket gjennom DNB.

Hvitvasking fra bedragerier skiller seg ut fra alle andre hvitvaskingssaker DNB jobber med. I tradisjonell hvitvasking handler det om at midler plasseres, tilsløres og integreres for å skjule at de stammer fra kriminalitet. I bedragerisakene dreier det seg om et kappløp mellom de kriminelle og bankene der bedragerne forsøker å få penger ut av banken for å plassere dem i en annen jurisdiksjon eller et annet pengesystem. Det betyr at hvis vi skal lykkes med å hindre at utbyttet fra bedrageriene havner i hendene til de kriminelle vil vi måtte arbeide på en helt annen måte med hvitvasking og i stor grad håndtere tidtransaksjoner i realtid.

Våre rapporter er et bidrag til det finansielle etterretningssystemet som politiet og kontrollmyndigheter bruker i kriminalitetsbekjempelsen. Av forhold som DNB rapporterte i 2023 har Økokrim tatt inn ca. 7 prosent «til analyse». Dette er en økning på to prosent sammenlignet med 2022, men betyr likevel at over 90 av 100 saker ikke har blitt benyttet av Økokrim. De viktigste endringene fra i fjor er at vi ser en sterkere prioritering av bedragerisaker, mens Økokrim i mindre grad prioritiserer klassisk økonomisk kriminalitet og narkotikaomsetning. Videre ser vi at det er relativt få saker som oversendes andre kontrolltater som NAV og Skatteetaten ettersom det er få saker innen de aktuelle kriminalitetsområdene som tas til analyse.

Kriminalitetsbildet endres, og nye trusler dukker opp. Det forventes at trusselbildet fremover vil preges av sterke drivere der organiserte kriminelle benytter seg av digitalisering og utnytter nye geopolitiske risikoer.

Organiserte kriminelle fremstår som mer profesjonaliserte og har tatt i bruk ny teknologi og profesjonelle medhjelpere. Det er utviklet et marked for kjøp og salg av spesialiserte kriminelle tjenester som benyttes for hvitvasking. Vi ser en økt kapabilitet og sterkere innveving mot tradisjonelt næringsliv der organiserte kriminelle oppnår konkurransefordeler ved bruk av korupsjon, skattesvindel og andre kriminelle metoder.

Digitalisering innebærer mulighet for å fornye, forenkle og forbedre samfunnet gjennom å utvikle og anvende ny teknologi. Digitalisering åpner også nye arenaer og verktøy for kriminelle. DNB forventer en økning der kriminelle utnytter tillitsbaserte ordninger rettet inn mot å digitalisere og forenkle virksomheters dialog og rapportering til myndighetene. Eksempel på dette er feilrapporteringer til skatteetaten som deretter benyttes til lånebedragerier, ID-misbruk, trygdebedrageri, forsikringssvindel og korupsjon.

Vi forventer også en økt vekst og nye kapasiteter innenfor bedrageriområdet der målet for kriminaliteten er midler som personer og selskaper har i banken. Dette utfordrer bankene rundt samarbeid, teknologi og kapasitet til å arbeide i realtid med transaksjonene.

Geopolitiske konflikter og økt bruk av sanksjoner har ført til at det er utviklet et parallelt hvitvaskingsnettverk der det benyttes mellommenn, dokumentforgårsfalskning, skjult

eierskap mv. for å omgå og redusere virkingen av sanksjonene. Det er store verdier som sirkulerer i et grått marked og vil bli ønsket hvitvasket gjennom banksystemet.

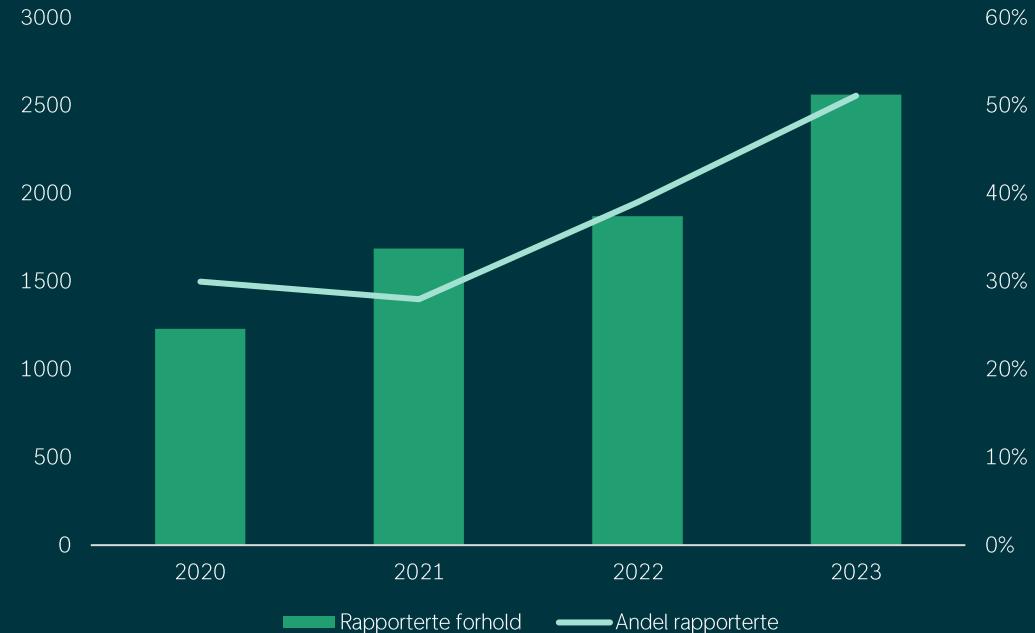
Oppsummering 2023

Økning i antall rapporterte forhold

I 2023 rapporterte vi 2 563 forhold til politiet grunnet mistanke om hvitvasking. Dette er det høyeste antall forhold DNB noensinne har rapportert. Sammenlignet med 2022 rapporterte DNB 37 prosent flere saker til Økokrim og vi har fordoblet antall rapporteringer siden 2020.

Årsakene til vekst i antall rapporteringer skyldes i hovedsak:

1. Vekst innenfor særskilte kriminalitetsområder
2. Mer effektiv transaksjonsovervåkning
3. Gjennomgående økt forståelse for hvitvaskingsrisiko og kjennetegn på hvitvasking - Dette ser vi blant annet ved at rapporteringsandelen øker på sakene som sendes til DNBs utredningsenhet.



Figur 1. Antall rapporterte forhold per år og andel interne meldinger som rapporteres

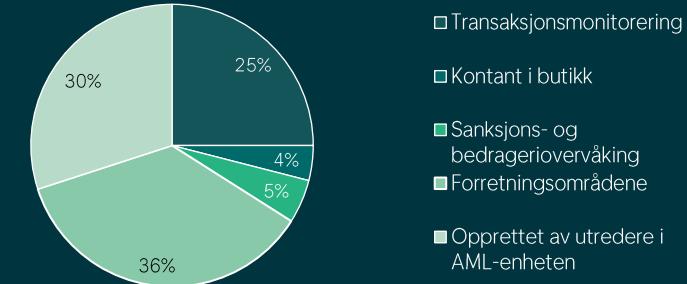
Mer effektiv transaksjonsmonitorering

DNB avdekker indikasjoner på hvitvasking gjennom ulike deler av bankens antihvitvaskingsystem der alle delene utfyller hverandre:

- Alarmer fra bankens transaksjonsovervåking som blir vurdert å være en indikasjon på mulig hvitvasking
- Interne meldinger fra bankens forretnings- eller støtteområder der det avdekket transaksjoner eller andre forhold ved kunde som kan være indikasjon på hvitvasking. Disse undersøkelsene kan også være initiert på bakgrunn av en transaksjonsalarm.
- Saker som opprettes av utredere i AML-enheten på bakgrunn av informasjonsutveksling med andre rapporteringspliktige i forbindelse med deres undersøkelser og vurdering av utleveringspålegg fra politi og andre offentlige kontrollorganer eller saker som av andre grunner opprettes av utredere i AML-enheten.
- Rapporter fra bankens spesialistmiljøer innen bedrageri- og sanksjonsovervåkning
- Melding om indikasjon på hvitvasking gjennom Kontant i butikk samarbeidet - altså innskudd og uttak av kontanter gjennom bankterminaler i butikk

Samlet sett avdekkes rapporterte saker slik fordelt på kanal hvor indikasjon for hvitvasking eller terrorfinansiering er avdekket.

I 2023 rapporterer **DNB** om lag 52 prosent flere saker direkte fra transaksjonsovervåkningen sammenlignet med 2022. Bakgrunnen for dette er et omfattende arbeid med å styrke styring og risikodekning på transaksjonsovervåkningen som har gitt gode resultater spesielt innen personmarkedet.



Figur 2. Oversikt over opprinnelsen til rapporterte saker



Figur 3. Antall rapporterte forhold fra transaksjonsmonitorering og andel eskalerte alarmer som rapporteres

Størst risiko for hvitvasking i bedriftssegmentet

I DNB er personsegmentet (PM) det klart største forretningsområdet med over 2,1 millioner kunder. Deretter kommer bedriftssegmentet (CB) med i overkant av 250 000 kunder og til slutt Private Banking (PB) med ca. 20 000 kunder¹.

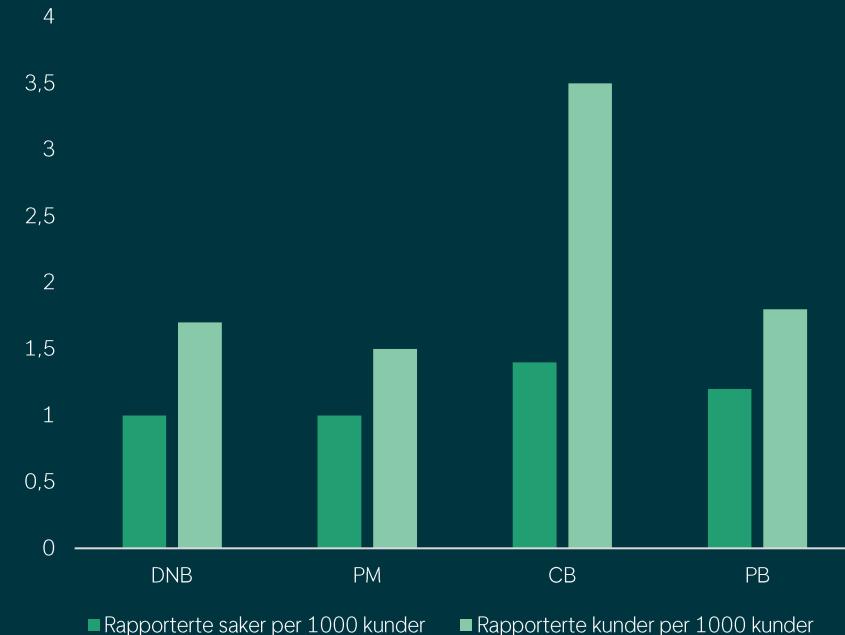
Antall rapporterte forhold følger i stor grad størrelsen på kundemassen, der PM har rapportert ca. 2 143 forhold, CB 363 og PB 121 forhold.

Likevel ser vi at hvitvaskingsrisikoen varierer for mellom forretningsområdene i DNB på bakgrunn av kundetyper, segment og hvilke produkter som tilbys.

Sett mot antall kunder så rapporterer DNB mer enn dobbelt så mange kunder fra bedriftssegmentet enn som fra personsegmentet. Dette er i tråd med risikovurderingene til DNB og naturlig da det kan være mer egnet å hvitvaske midler gjennom en bedriftskonto eksempelvis et gatekjøkken, bilvask og transportfirma enn et ordinært personkundeforhold.

Vi ser også at sakene i bedriftssegmentet er mer komplekse, med høyere summer og flere involverte parter.

Det rapporteres også noe flere saker for kundegrupper med sammensatte kundeforhold for eksempel med stor grad av grensekryssende transaksjoner og omfattende formuesplasseringer som for eksempel innen Private Banking segmentet



Figur 4. Andel rapporterte forhold (per 1 000 kunder) og gjennomsnittlig rapporterte antall kunder i hvert forhold

¹ DNB har også forretningsområdet Markets. Markets har relativt få konsernrike kunder og 97 prosent av kundene har sitt primærkundeforhold i PM, CB eller PB. Hoveddelen av rapporterte forholds som involverer bruk av Marketsprodukter er rapportert gjennom forretningsområdet der kunden har sitt primærkundeforhold.

Nr.	Kriminalområde	Andel rapporterte forhold	Antall rapporterte forhold	Endring antall	Endring prosent
1	Bedrageri	40 %	1028	521	103 %
2	Annен vinningskriminalitet	39 %	987	568	136 %
3	Skattesvik	30 %	764	70	10 %
4	Arbeidslivskriminalitet	9 %	232	25	12 %
5	Økonomisk utroskap, korupsjon og underslag	5 %	131	-13	-9 %
6	Brudd på regnskaps- og aksjeloven	4 %	100	-31	-24 %
7	Narkotikakriminalitet	3 %	85	48	130 %
8	Misbruk av sosiale ytelsjer og trygd	2 %	58	-10	-15 %
9	Konkurskriminalitet	1 %	29	-14	-33 %
10	Terrorfinansiering	0 %	11	-4	-27 %

Størst omfang i saker med hvitvasking fra bedragerier

Ved nærmere undersøkelser av saker foretar uteader en vurdering av hvilken primærforbrytelse det er sannsynlig at hvitvaskingen kan knyttes til. En slik vurdering må tolkes med forbehold da det er uteaderens subjektive vurdering i lys av opplysningsene som er tilgjengelig på tidspunktet saken undersøkes. Det er også viktig å merke seg at en sak kan knyttes til flere kriminalitetsområder, for eksempel vil arbeidslivskriminalitet også kunne omfatte skatteunndragelser.

Tradisjonelt har DNB rapportert flest tilfeller innen skatte- og avgiftsområdet. Det er ikke unaturlig i og med at dette er et stort kriminalitetsområde som innebefatter mange lovbrudd, samt at det for banken vil være forholdsvis enkelt å avdekke avvik mellom inntektsinngang og betalte skatt/avgifter, spesielt i bedriftssegmentet.

I år er imidlertid første året der vi ser at et annet kriminalitetsområdet enn skatt/avgift som det rapporteres flest saker på.

Bedrageri

Den største trusselen på antihvitvaskingsområdet fremstår å være hvitvassing av utbytte fra digitale bedragerier. DNB har sett en kraftig utvikling på området med en gjennomsnittlig årlig dobling av antall slike hvitvaskingssaker siden 2020.

I år beregner vi at mer enn 330 millioner kroner i bedrageriutbytte vil bli forsøkt hvitvasket gjennom DNB.

Hvitvassing fra bedragerier skiller seg ut fra alle andre hvitvaskingssaker DNB jobber med. I tradisjonell hvitvassing handler det om sirkulering av midler. For bedrageriutbytte er det et kappløp mellom de kriminelle og bankene for å få ut pengene fra banken og plassere dem i en annen jurisdiksjon eller et annet pengesystem slik at ikke bankene skal klare å slå kloa i pengene.

Den hyppigste overføringsmetoden er at midlene overføres fra bedrageriofferet til en 'muldyrkonto'. Altså at en person stiller sitt kontoforhold til disposisjon for bedrageriutbyttet og når midlene kommer inn på kontoen så overføres midlene

videre eksempelvis via andre betalingsleverandører, kortkjøp, overføring til kryptovekslere eller ved uttak av kontanter.

I 2023 har DNB registrert ca. 1 600 personer som stiller kontoforholdet sitt til rådighet og på den måten medvirker til bedrageri og hvitvassing. Dette er ofte unge personer som opplever liten risiko ved å la andre benytte sitt kontoforhold på grunn av at de har lite penger i banken.

Når det avdekkes bedragerier samarbeider bankene på tvers for om mulig å tilbakeføre utbyttet som er bedratt fra kunden. Tilbakeført utbytte er femdoblet siden 2020. Dette er midler som kriminelle ellers ville fått tak i.

90 000 000

80 000 000

70 000 000

60 000 000

50 000 000

40 000 000

30 000 000

20 000 000

10 000 000

0

2020

2021

2022

2023

Figur 5. Oversikt over utbytte fra bedragerier som er sikret og tilbakeført

Narkotikakriminalitet

Vi rapporterer stadig mer hvitvasking fra narkotikakriminalitet. Dette økte mye i 2022 og er mer enn fordoblet i 2023. Veksten av hvitvasking fra narkotikakriminalitet ser vi i sammenheng med redusert kontantbruk og at oppgjør for salg av narkotika skjer ved hjelp av nye betalingsløsninger som for eksempel VIPPS. Slik sett dreier dette seg om distribusjonsnettverk drevet av personkunder i 16-30 års aldersgruppen som mottar utbyttet fra narkotikasalg på bankkontoen. For personer lengre opp i næringskjeden ser vi ofte at disse har en parallel økonomi med liten bruk av egen bankkonto og at de i større grad bruker kontanter eller medhjelpere til å betale for eget forbruk. Her ser vi oftere at de også har etablert selskap innen arbeidsintensive bransjer slik som transport, flytte- og vaskeritjenester eller lignende.

Annен vinningskriminalitet

Annen vinningskriminalitet vokser mest både i andel og antall. I utgangspunktet betyr dette at vi ikke kan identifisere primærforbrytelsen, men det kan kanskje også skyldes at primærforbrytelsen er av en mindre vanlig type som vi ikke har egen kategori på, eksempelvis utbytte fra salg av overgrep på nettet.

Ved gjennomgang av sakene ser vi at den hyppigste årsaken til at denne kategorien øker er at sakene fremstår mer komplekse og med innslag av multikriminalitet der vi kun klarer å forstå deler av primærforbrytelsene.



Det er et forbedringspotensial for å kunne gi økt verdi til finansiell etterretning

DNB sender sine rapporter til Økokrim som har et nasjonalt kompetansesenter for hvitvassing og terrorfinansiering. De skal bearbeide, berike, analysere og videreforside informasjon til politi, kontroll- og tilsynsmyndigheter samt utenlandske tjenester.

Rapporter fra de rapporteringspliktige er en sentral del av finansiell etterretning som igjen skal bidra til kriminalitetsbekjempelse og inndragning av utbytte fra kriminaliteten.

De viktigste endringene fra i fjor er at vi ser en sterkere prioritering av bedragerisaker, mens Økokrim i mindre grad prioriterer klassisk økonomisk kriminalitet og narkotikaomsetning. Vi ser også at det er relativt få saker som oversendes andre kontrolltater som NAV, Skatteetaten og A-krim ettersom det er få saker innen de aktuelle kriminalitetssområdene som tas til analyse. Tabellen nedenfor gir en viss innsikt i om arbeidet hos de rapporteringspliktige er prioritert riktig.

Nr.	Kriminalitetssområde	Andel Analyse Økokrim	Endring «til analyse» 2022	Andel saker totalt
1	Terrorfinansiering	64 %	17 %	1 %
2	Bedrageri	11 %	7 %	40 %
3	Annen vinningskriminalitet	8 %	2 %	39 %
4	Økonomisk utroskap, korruption og underslag	6 %	-7 %	5 %
7	Narkotika	6 %	-5 %	3 %
5	Arbeidslivskriminalitet	4 %	1 %	9 %
6	Konkurskriminalitet	3 %	3 %	1 %
8	Skattesvik	2 %	-1 %	30 %
9	Brudd på regnskaps- og aksjeloven	2 %	-1 %	4 %
10	Misbruk av sosiale ytelser og trygd	0 %	-1 %	2 %

Trusselvurdering 2024

Kriminalitetsutviklingen viser at den klassiske vinningskriminaliteten reduseres, eksempelvis ved at vi ser et stort fall i anmeldt kriminalitet. Samfunnet blir på mange måter tryggere. Samtidig ser vi at kriminalitetsbildet endres og nye trusler vokser frem. Vi forventer at trusselbildet fremover vil preges av sterke drivere der organiserte kriminelle benytter seg av digitalisering og utnytter nye geopolitiske risikoer.

Organisert kriminalitet – Økt bruk av legale og komplekse strukturer for hvitvasking

Organiserte kriminelle har gjennom tiår hentet ut store inntekter fra omsetning av ulovlige rusmidler. Stabile og store inntekter ser ut til å ha styrket og profesjonalisert kriminelle nettverk. De har tatt i bruk ny teknologi og fått bistand fra profesjonelle medhjelpere til hvitvasking. Det er utviklet et marked for kjøp og salg av spesialiserte kriminelle tjenester som vi også ser benyttes innen hvitvasking. Dette øker kapabiliteten til kriminelle nettverk og vi ser en utvikling der organisert kriminalitet innlemmes i det tradisjonelle næringsliv og oppnår konkurransefordeler ved bruk av korruption, skatte- og avgiftsunndragelser og andre ulovlige metoder.

Digitalisering – nye sårbarheter og nye verktøy

Digitalisering innebærer mulighet for å for å fornye, forenkle og forbedre samfunnet gjennom å utvikle og anvende ny teknologi. Der digitalisering kan bidra til økt verdiskapning, produktivitet og innovasjon kan det også oppstå sårbarheter som åpner nye arenaer for kriminelle.

DNB har avdekket en rekke saker der kriminelle utnytter tillitsbaserte ordninger rettet inn mot å digitalisere og forenkle dialogen og rapportering mellom private selskaper og offentlige myndigheter. Et eksempel på dette er hvordan ordningen for registrering av a-meldinger er misbrukt til lånebedragerier, ID-misbruk, trygdebedrageri, forsikringssvindel og korrasjon.

Utbyttet i slik kriminalitet vil som regel være midler som er utbetalt gjennom stat eller statlige organ. Virksomhetene som benyttes og der hvitvasking av utbyttet foregår 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 utstrakt bruk av utenlandsk arbeidskraft.

Det forventes at kriminelle vil raffinere og ta i bruk nye løsninger og at midlene i stor grad vil hvitvaskes gjennom bankene.

Digitaliseringen av samfunnet med redusert kontantbruk fører til at det er pengene som personer og selskaper har i banken som blir det fremste målet både for norske og internasjonale kriminelle. Vi har som fortalt tidligere sett en dobling av hvitvassingssaker fra bedrageri hvert halvår siden 2020 og forventer fortsatt en økt vekst i bedragerier.

Bankene er i et intenst kappløp med de kriminelle for å hindre at midlene føres ut av bankene, der kriminelle nå åpenbart raffinerer metodikken og bruker «crime as a service» - altså profesjonelle medhjelpere for å ta ut midlene raskt og effektivt.

Geopolitisk risiko - sanksjonsomgåelse et nytt område for hvitvaskere

DNBs sanksjonsekspert viser i sin rapport til at det at det internasjonale samfunnet i økende grad benyttet sanksjoner som et virkemiddel i geopolitiske konflikter. Denne utviklingen får også konsekvenser for antihvitvaskarbeidet hvor vi har plikt til å rapportere eventuell hvitvasking etter brudd på sanksjonsregelverket.

Det er etablert en rekke metoder for å omgå sanksjonene, inkludert å skjule reelt eierskap, bruk av mellommenn, dokumentforgalskning mv. Slik sett har det blitt etablert et parallelt hvitvaskingsnettverk, som også kan benytte seg av bistand fra profesjonelle medhjelpere og «crime as a service» i forbindelse med omgåelse av sanksjoner.

Finansiell trygghet i en usikker verden

Bedragerier

Sammendrag

Omfangen av bedragerier fortsatte å øke gjennom 2023 og forbindelsene til annen alvorlig organisert kriminalitet ble tydeligere. I løpet av året ble det utført bedrageriforsøk for 1 811 millioner kroner. Dette er en økning på 45 prosent fra 2022. DNBs bedrageriforebyggende tiltak forhindret 85 prosent av bedrageriene mot DNB og våre kunder.

De største endringene vi har observert innen digitale bedragerier det siste året:

- Safe account fraud, en ny type bedrageri i Norge hovedsakelig rettet mot eldre.
- En kraftig økning i investeringsbedrageri, spesielt innen kryptovaluta.
- Profesjonelle kriminelle organisasjoner ble mer synlige i tilknytning til bedragerier.

I løpet av fjoråret ble de første sakene kjent som safe account fraud registrert, der kriminelle ringte offeret og utga seg for å være politiet eller banken. Ofrene fikk beskjed om at noen hadde tatt opp et lån i deres navn eller hadde tilgang til deres nettbank. De ble deretter rådet til å flytte pengene sine til en «sikker konto» som angivelig tilhørte banken eller politiet, men som i realiteten var kontrollert av de kriminelle. På denne måten ble ofrene manipulert til å frivillig overføre pengene sine. Flere av ofrene ble forklart at de var involvert i en pågående politiaksjon og at de ikke skulle avsløre dette til noen, inkludert banken. Denne varianten av sosial manipulering er spesielt alvorlig, da den retter seg mot eldre som er spesielt sårbare for denne typen manipulering.

Flere trusselaktører er fortsatt involvert i store, automatiserte phishingangrep mot våre kunder. Disse angrepene varierer fra små angrep av dårlig kvalitet til store kampanjer rettet mot spesifikke personer eller grupper, og i ett tilfelle involverte det bruk av en falsk basestasjon.

Selv om vi registrerte en svak nedgang i antall bedragerier rettet mot våre bedriftskunder, var det en økning på 88 prosent i angrepssum. Bedragerier som retter seg mot bedriftskunder er alvorlige, og det potensielle tapet ofte svært høyt. Det finnes også veletablerte trusselaktører som har spesialisert seg på bedragerier mot bedriftskunder. Vår trusseletterretning indikerer at organiserte kriminelle er i ferd med å rette seg mot bedrifter i større grad enn tidligere.

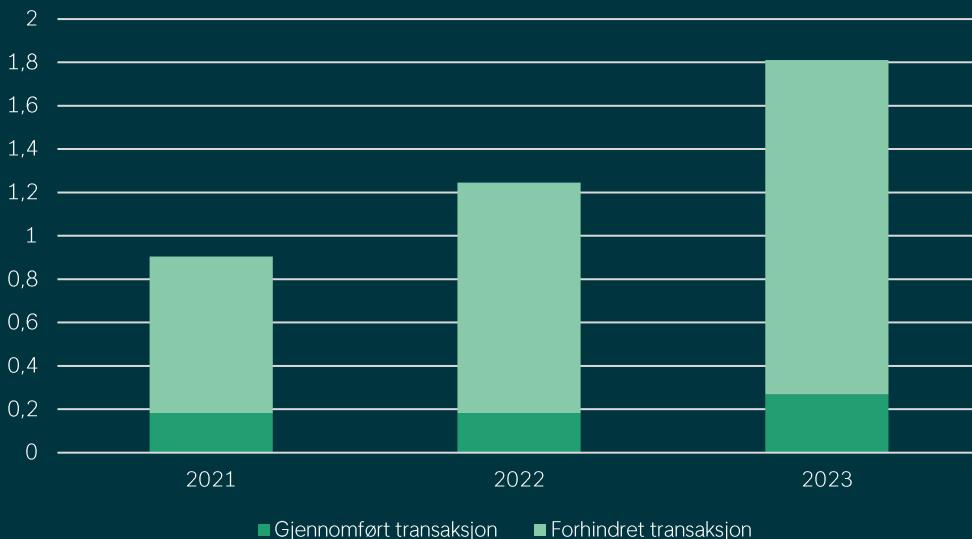
På grunn av økt konfliktnivå mellom kriminelle grupper i Sverige i 2023 fikk vi innsikt i svensk organisert kriminalitet. Handlingene til disse kriminelle gruppene gir et klart bilde av organiserte trusselaktører som er involvert i bedrageri, våpen, narkotika, hvitvassing og vold. Trusselen disse multikriminelle gruppene utgjør i årene som kommer, og deres tydelige og økte tilstedeværelse i Norge, må etter vår mening tas på alvor.

Oppsummering 2023 – DNB Bank

I 2023 stanset DNB bedrageri for 1 543 millioner kroner av en angrepssum på 1 811 millioner kroner. Angrepssummen har økt med 45 prosent fra 1 246 millioner kroner i 2022. 64 prosent av bedrageriene ble gjennomført på kort og 36 prosent i digitale kanaler. Digitale kanaler omfatter også betalinger initiert av tredjeparter utenfor DNB. Denne oppsummeringen er basert på informasjon fra digitale kanaler.

DNB håndterte i digitale kanaler 9 723 tilfeller av bedrageri fordelt på 5 010 kunder, dette er på nivå med 2022. I midlertid økte angrepssummen fra 500 millioner kroner til 618 millioner kroner, en økning på 24 prosent fra 2022. Bankens deteksjonssystemer forhindret 70 prosent av forsøkene, noe som utgjorde 435 millioner kroner.

Det er to hovedårsaker til denne økningen. For det første har antall tilfeller av investeringsbedrageri og den tilhørende angrepssummen økt til 189 millioner kroner, noe som tilsvarer mer enn en dobling fra året før. For det andre har det kommet en ny bedragerimetode, der bedragere utgir seg for å være fra politiet eller banken og overtaler kunder til å selv flytte pengene sine til en «sikker konto». Angrepssummen av denne type bedrageri utgjorde 48 millioner kroner.



Figur 1. Bedrageriforsøk, milliarder NOK

Vishing og safe account fraud

Banken observerte en økning i antall vishingsaker mot kunder i 2023. Det var 242 ofre, med en angrepssum på 51 millioner kroner. DNB har forhindret et tap på 31 millioner kroner. I mer enn halvparten av vishingsakene utga bedragerne seg for å ringe fra DNB eller politiet. I disse sakene ble kundene bedt om å oppgi personlige passord og godkjenne forespørsler ved hjelp av BankID. På denne måten fikk de kriminelle tilgang til ofrenes nettbank eller mobilbank og gjorde uautoriserte overføringer.

I februar 2023 så DNB de første tilfellene av safe account fraud i Norge. Denne typen bedrageri har vært utbredt i Danmark og Sverige i flere år. Det innebærer at kunder blir oppringt av noen som utgir seg for å være fra politiet eller banken og overbeviser kunden om at pengene deres er i fare. Kunden blir deretter fortalt at politiet eller banken har opprettet en sikker konto der de kan plassere pengene sine, og de blir bedt om å overføre alle pengene sine til denne kontoen. I mange tilfeller blir kundene bedt om å holde denne informasjonen hemmelig hvis de blir kontaktet av banken, fordi de er en del av en pågående etterforskning.

For å gjennomføre safe account fraud er det nødvendig for de kriminelle å skape tillit hos ofrene. Bedragerne bruker mye tid på å snakke med ofrene for å opparbeide tillit. Ofrene blir fortalt at de har liten tid til å redde pengene sine, og at de må handle raskt. Vårt inntrykk er at kriminelle har gjennomført testing og undersøkelse gjennom åpne kilder og har god kjennskap til DNBs systemer, både i nettbanken og mobilbanken.

Noen få tilfeller av safe account fraud dukket opp på våren 2023 og antallet økte betydelig i løpet av sommeren. I løpet av året utgjorde angrepssummen i disse sakene omtrent like mye som den totale angrepssummen for alle vishingsaker. DNB registrerte saker mot 108 personer med en samlet angrepssum på 48 millioner kroner, og forhindret et tap på 23 millioner kroner. Bedrageritypen retter seg ofte mot eldre kvinner. I 67 prosent av tilfellene er ofrene over 70 år, og 92 prosent er kvinner. I andre vishingsaker er kun 42 prosent av ofrene over 70 år og 59 prosent er kvinner.

Selv om safe account fraud dukket opp som en ny bedragerimetode i Norge i 2023, ser vi en fortsatt økning i andre vishingsaker.



Figur 2. Bedrageriforsøk per måned, millioner NOK

Investeringsbedrageri

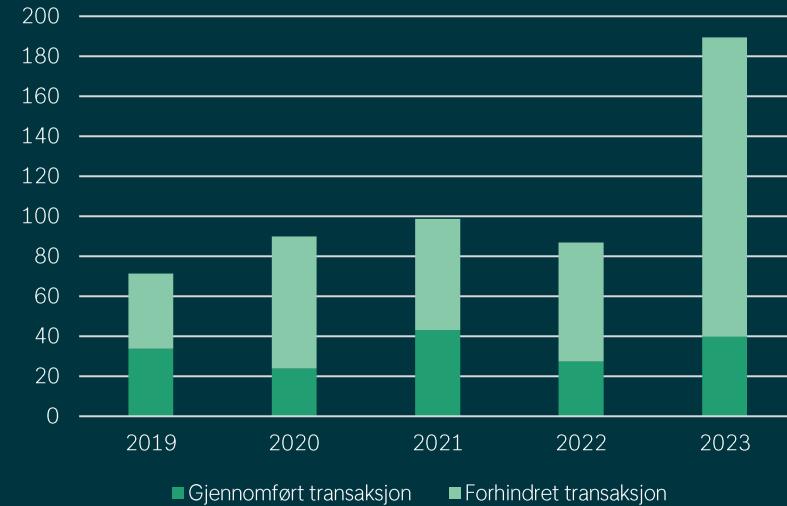
Investeringsbedrageri har tradisjonelt utgjort en betydelig del av bedragerier mot DNBs kunder, og i 2023 opplevde DNB en stor økning av disse bedrageriene. Antallet bedrattede kunder økte til 896 i 2023, med en samlet angrepssum på 189 millioner kroner, mer enn dobbelt så mye som året før. Dette er den største angrepssummen blant de ulike bedragerikategoriene i 2023.

Investeringsmulighetene ble i mange tilfeller presentert for ofrene gjennom falske nyhetsartikler, hvor kjente personer ble misbrukt for å skape troverdighet.

Nyhetsartikkelen markedsføres i sosiale medier, hvor også deepfake-videoer med fremtredende personer som diskuterer investeringer i kryptovaluta ble observert.

Bedragerne utnyttet ofrenes manglende kunnskap om investeringer i kryptovaluta, hvor ofrene ble bedt om å overføre penger via legitime tilbydere av kryptovaluta eller andre pengeoverføringsstjenester. Ofrene mottok ofte bistand av falske investeringsrådgivere gjennom fjernstyringsprogrammer.

Disse sakene er ofte utfordrende å undersøke fordi kriminelle får ofrene til å gjøre overføringer via legitime tilbydere av kryptovaluta eller digitale betalingstjenester. Når kundene blir kontaktet av banken, har de vanligvis mottatt spesifikke instruksjoner angående informasjonen de skal oppgi til banken om betalingen og dens formål for å overbevise banken om å tillate overføringen.



Figur 3. Investeringsbedrageri, millioner NOK

Phishing

I 2023 håndterte DNB 4 354 saker, en nedgang fra året før. Phishing er fortsatt den typen bedrageri som rammer flest kunder, med 2 973 ofre. Det var en tydelig nedgang i saker i begynnelsen av året, men antall tilfeller økte i løpet av sommermånedene og forble høye resten av året. Det har vært en liten nedgang i forsøk i digitale kanaler, men det har vært en vesentlig økning av korttransaksjoner.

Angrepssummen i digitale kanaler var 177 millioner kroner.

Ved hjelp av automatisert monitorering stansas ofte bedrageriforsøk før en betaling blir registrert. I disse tilfellene har vi estimert en angrepssum basert på tap i tidligere saker. I phishingsaker estimerer vi et tap på 60 tusen kroner per kunde. Vi har nedjustert dette beløpet fra tidligere år, noe som fører til at reduksjonen i angrepssum er større enn reduksjonen i antall saker. Vi har også stanset tilfeller av safe account fraud før det ble registrert betaling. Her er det potensielle tapet mye høyere og vi har benyttet et estimat på 330 tusen kroner per kunde.

Kjente merkevarer blir misbrukt i phishingkampanjer for å skape troverdighet. Eksempler på dette er phishing som bruker merkevarer knyttet til kjøp av bruktværer, offentlige myndigheter, inkassoselskaper og selskaper i finansbransjen. Ofre for phishing via inkassoselskaper er vanligvis yngre, mens ofrene for phishing via selskaper i finansbransjen er eldre. Vi ser fortsatt phishingangrep som misbruker DNBs merkevarer og retter seg mot kundene våre, både i vanlige phishingkampanjer og i ett tilfelle ved bruk av en falsk basestasjon eller IMSI-catcher.

Det ble også registrert tilfeller av målrettet phishing mot bedriftskunder og personer med ledende roller i et selskap. Dette skjer ofte kort tid etter at selskapet har gjort endringer i offentlige registre, og man antar at informasjonen blir brukt for at phishingforsøkene skal framstå som en legitim henvendelse.



Bedrageri mot bedriftskunder

Det er hovedsakelig tre typer bedragerier som er spesifikt rettet mot bedriftskunder: falske fakturaer, direktørbedrageri og beneficiary account change.

Falske fakturaer blir normalt masseprodusert og sendt til mindre organisasjoner som for eksempel idrettslag. Dette er både fordi slike organisasjoner kan ha dårligere sikkerhetsrutiner og fordi de ofte har informasjon som er offentlig tilgjengelig og kan misbrukes av bedragere for å skape tillit.

Direktørbedrageri utføres vanligvis via e-post der bedragerne utgir seg for å være en person i selskapet, ofte konsernsjef (CEO) eller finansdirektør (CFO), som sender en e-post til en regnskapsfører eller en ansatt og ber om å få utført en betaling.

Direktørbedrageri retter seg mot store bedrifter, men også mot mindre frivillige organisasjoner som idrettslag, lokale politiske grupper og andre interesseorganisasjoner.

Beneficiary account change eller endring av kontonummer for mottaker er ofte mer sofistikert, da bedragerne i slike tilfeller kan ha fått tilgang til e-postkontaoer eller andre systemer som gjør at de kan sende e-post fra legitime kontoer og dermed unngå behovet for spoofing. Dette gir bedragerne tilgang til informasjon over tid. Ved å ha tilgang til betalingsinformasjonen kan de endre betalingsdetajlene på en troverdig måte.

I 2023 var det en reduksjon i antall bedragerier rettet mot bedriftskunder, totalt 172 tilfeller mot 210 i 2022. Den gjennomsnittlige angrepssummen per kunde ble i samme periode nær doblet, fra 337 tusen kroner i 2022 til 660 tusen kroner i 2023. Den totale angrepssummen knyttet til bedriftskunder var 85 millioner kroner, en økning på 88 prosent fra året før.

Bedragerier mot bedriftskunder er sjeldnere enn mot private kunder, men det potensielle økonomiske tapet per sak er betydelig høyere. Som et eksempel opplevde en bedriftskunde et tap på 1,9 millioner amerikanske dollar som et resultat av et direktørbedrageri i 2023.

Som rapportert i 2022, tror vi at bedragerier mot bedriftskunder er underrapporterte og at det faktiske antallet tilfeller er høyere. Det er flere mulige grunner til dette, for eksempel at selskaper velger å holde tilbake informasjon for å forhindre omdømmetap. Økt rapportering vil bidra til å forbedre både bedragerforebygging og rettsforfølgelse.

Sosial manipulering

Andre typer sosial manipulering inkluderer kjærlighetsbedragerier og bedragerier som innebærer betaling av gebyrer (advance fee fraud). Bedrageriene er basert på å manipulere ofrenes følelser, vanligvis ved å skape et tillitsforhold. Vi har sett en økning i antall tilfeller og angrepssum for kjærlighetsbedragerier, mens antall advance fee fraud har vært omrent på samme nivå som i 2022.

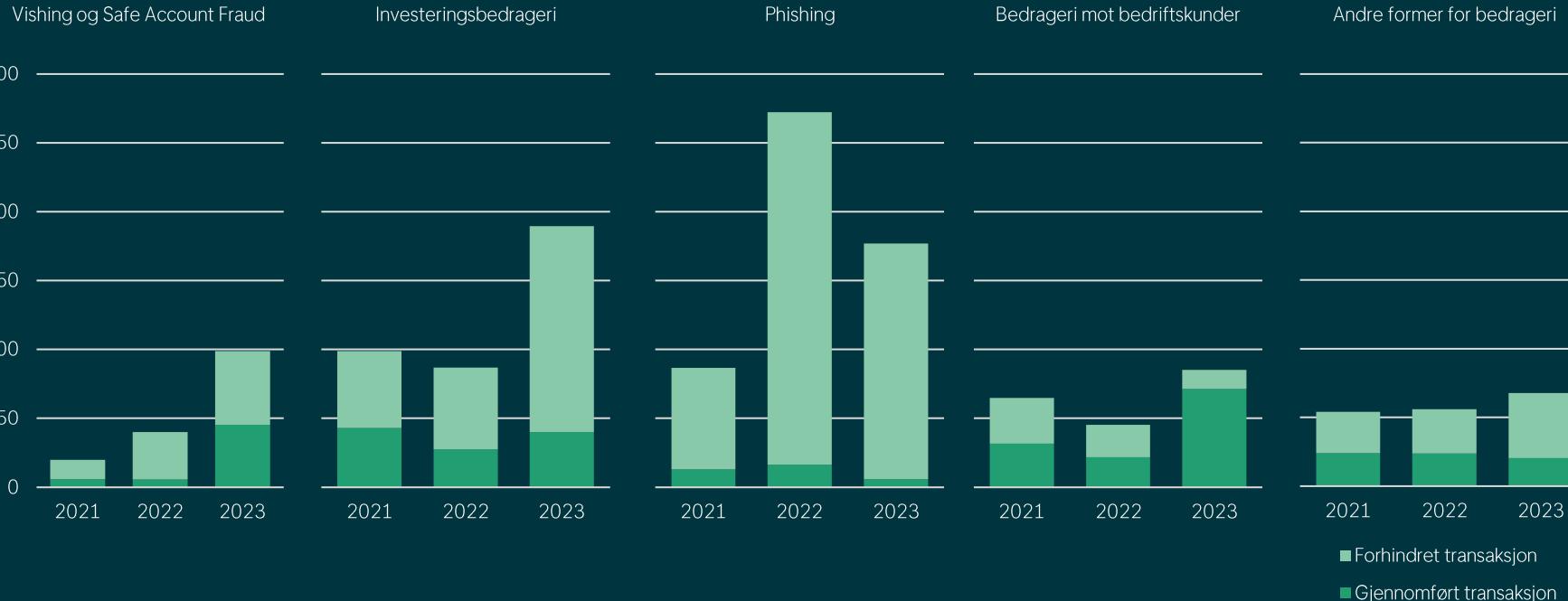
Fysiske bedragerier

Digitale bedragerier dominerer trusselbildet, men det forekommer fortsatt tilfeller av bedrageri som gjennomføres fysisk mot offeret. Det kan involvere venner og slektingar, eller de kan involvere ukjente personer som dukker opp hjemme hos offeret for å bedra dem. Det har også vært tilfeller rettet direkte mot DNB som har involvert bruk av falske dokumenter og identitetstyveri.

I denne type bedrageri er bedrageren vanligvis en opportunistisk kriminell, som for eksempel et familiemedlem av offeret, men kan også være en håndverker eller helsearbeider for eldre ofre. De skaffer seg urettmessig adgang til offerets BankID og annen påloggingsinformasjon, eller ber offeret gi fra seg dette frivillig. Bedrageren logger seg deretter inn i offerets nettbank og gjennomfører betalinger eller søker om forbrukslån og kredittkort.

Kriminelle er kjent for å utgi seg for å være ansatte i kabel-tv-selskaper, internettleverandører eller dørselgere for å få tilgang til hjemmet til eldre ofre for å stjele verdier, betalingskort eller DNB-kodebrikker og lurer ofrene til å avsløre PIN-koden sin eller sitt personlige BankID-passord.

Det har vært tilfeller hvor bedragere har oppsøkt DNB-filialer for å hente ut informasjon som blir brukt til å gjennomføre bedrageri. Første trinn er vanligvis å skaffe enten falske eller ekte ID-dokumenter med sitt eget bilde, med offerets navn og personnummer. Deretter registreres det et mobiltelefonabonnement i offerets navn. De utgir seg videre for å være offeret ved en DNB-filial for å skaffe seg kontoutskrifter, inkludert oversikter over siste kontooverføringer, lønnsutbetalinger og kortbetalinger. Dette gjøres sannsynligvis for å få så mye informasjon om offeret som mulig for å begå andre bedragerier. Neste steg er å lure ansatte ved DNBs kundesenter til å utføre overføringer fra offerets bankkontoer, endre deres kontaktinformasjon, bestille betalingskort osv.



Figur 4. Bedrageriforsøk per kategori, millioner NOK

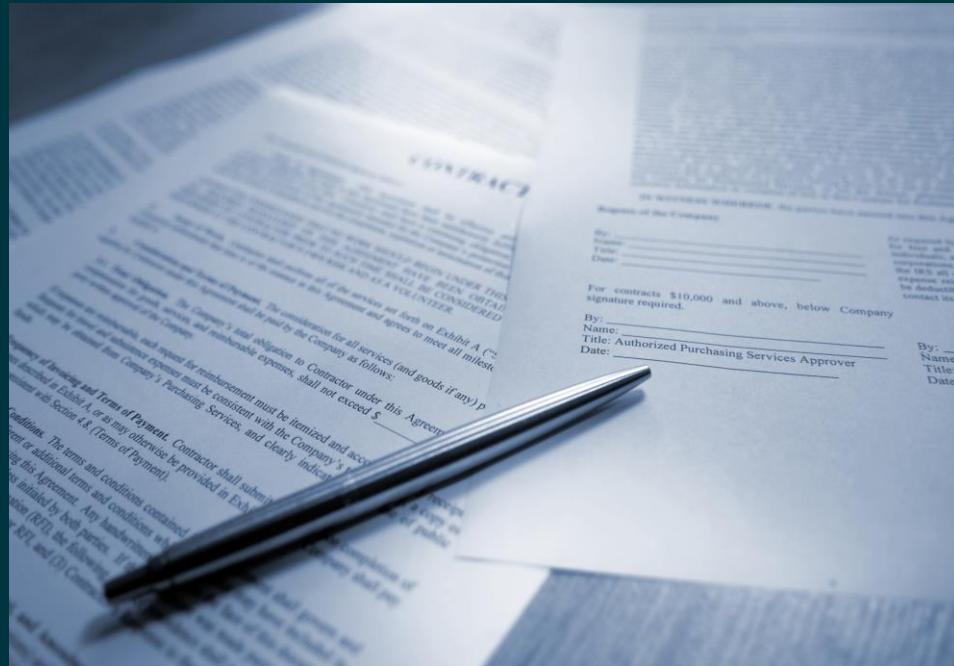
Oppsummering 2023 – DNB Livsforsikring

Trenden med økt forsikringssvindel fortsetter

Økonomiske nedgangstider påvirker ofte utviklingen av økonomisk kriminalitet, også forsikringssvindel mot personskade- og uføreforsikringer. Første halvår i 2023 ble det i bransjen totalt sett avdekket forsikringssvindel for rundt 300 millioner kroner. Dette er nesten dobbelt så mye som samme periode i fjor. DNB Livsforsikring har særlig sett at svindel mot uføreforsikringer øker.

Historisk mange unge uføre

I løpet av de siste ti årene har andelen unge uføre mer enn doblet seg. Tallet er nå historisk høyt og i 2022 var det 21 610 mottakere av uføretrygd i aldersgruppen 18-29 år. Utover å være en betydelig utfordring for hele velferdsstaten peker også tallene mot en mulig økt trussel for forsikringssvindel, da en undersøkelse viser at den yngste aldersgruppen kommer markant svakest ut på generelle holdninger til forsikringssvindel. Potensielle bedragerier utført av yngre mot uføreproduktene utløser betydelige forpliktelser for selskapet på grunn av den langvarige utbetalingsperioden.



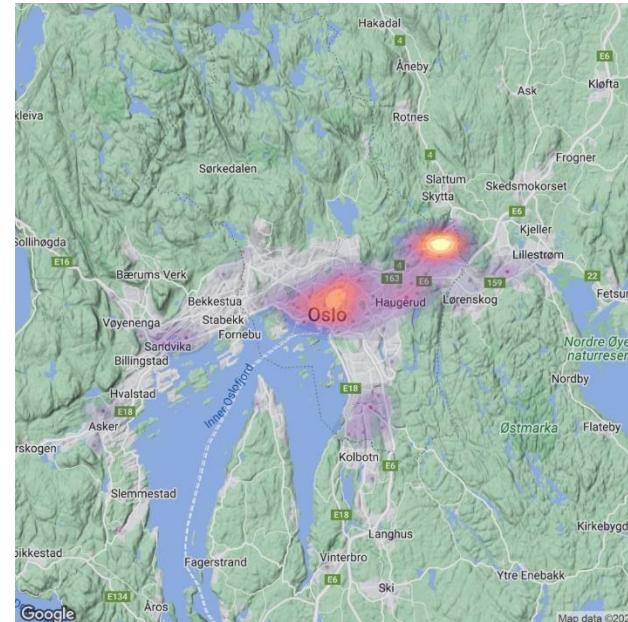
Trusselvurdering 2024 - DNB Bank

Kriminelle nettverk og bedragerier

Ifølge norsk politi er omrent 100 organiserte kriminelle nettverk aktive i Norge. Det svenske organiserte kriminelle nettverket kjent som «Foxtrot» er aktivt i de fleste norske politidistrikter.

DNB følger med på et spesifikt svensk organisert kriminelt nettverk som er aktivt i Norge. De begår bedragerier mot norske DNB-kunder og bruker norske DNB-kontohavere som pengemuldyr. De er også involvert i ulovlig handel med narkotika og våpen. Nettverket er ifølge svensk politi i stand til å utøve ekstrem vold. Nettverket er godt organisert og utfører bedragerier mot norske bankkunder på en svært sofistikert måte. Hittil er inntektene fra bedragerier mot norske ofre små sammenliknet med Sverige. Hvis de får lov til å operere uten forstyrrelser, vil nettverket sannsynligvis etablere seg i Norge.

Evnens til å flytte penger fra offerets konto til kontoen til en person som fungerer som pengemuldyr er et kritisk trinn i ethvert bedrageri. De kriminelle har behov for et stort antall personer som stiller sin konto til disposisjon. Disse har hovedsakelig vært unge menn basert i visse geografiske områder, ofte involvert i narkotikahandel på et lavt nivå i Oslo.



Figur 5. Kart over mottakere av bedragerimiddler

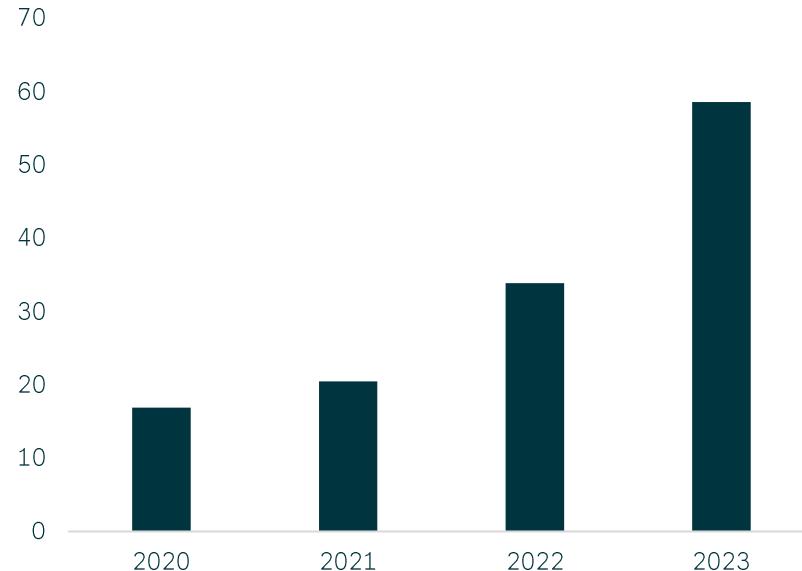
Bedragerier, organisert kriminalitet og geopolitikk

I 2023 ble det avdekket et stort bedrageri mot DNBs kunder hvor det ble opprettet fiktive abonnement. Betalingene har blitt kanalisiert til virksomheter i ulike land, hovedsakelig i Europa og USA. Fra 2020 til 2023 mer enn tredoblet den totale angrepssummen seg fra 16 millioner til 58 millioner kroner. Det har i perioden vært et totalt tap på rundt 66 millioner kroner. Gjennomsnittsbeløpet per transaksjon er under 300 kroner, men på grunn av det høye volumet av transaksjoner blir det totale beløpet høyt. Fra mars 2022 er det avdekket betalinger knyttet til abonnementsbedragerier til Kypros og volumet av betalinger økte raskt. Norsk politi og andre finansinstitusjoner utreder sakene, og det er rapportert til Europol.

Russlands invasjon av Ukraina i februar 2022 har isolert landet fra store deler av den globale økonomien. Finansielle sanksjoner betyr at internasjonale markeder i stor grad er stengt for russiske selskaper. Russiske teknologiselskaper har flyttet til Kypros etter invasjonen. Kypros har vært en foretrukket destinasjon for russisk økonomisk kriminalitet, som vises i "Cyprus confidential"-prosjektet. Selv om det på ingen måte er konkluderende, indikerer dette en korrelasjon mellom bedrageri, geopolitisk utvikling og effekt av sanksjoner.

Det høye antallet bedragerier vil fortsette

Det er ingen faktorer som tilsier at intensiteten eller kompleksiteten i bedragerier mot DNB vil avta. Begge variablet vil øke og utfordre DNBs evne til oppdagelse og håndtering av økonomisk kriminalitet. Drivkrefter som store geopolitiske omveltninger, makroøkonomi, demografi og migrasjon, og teknologisk utvikling virker inn på kriminalitetsbildet generelt. For bedragerier vil regulatorisk utvikling, ressursmangel i norsk politi, lav oppdagelsesrisiko for økonomisk kriminalitet og problemstillinger relatert til nasjonal sikkerhet, virke inn på trusselen bedragerier utgjør.



Figur 6. Abonnementsvindel, millioner NOK

Dårligere år for demokratiet vil føre til økt økonomisk kriminalitet

Verden er preget av en forvitring av demokratiske spilleregler. Når over 70 land skal gjennomføre valg i løpet av 2024 vil det utvilsomt være flere eksempler på fredelig og demokratisk overføring av regjeringsmakt – men i en rekke land vil valgene også bidra til at mindre demokratiske krefter kommer til makten. En gradvis undergraving av demokratiske prosedyrer og institusjoner henger sammen med en forvitring av frie markeder, uavhengige kontrollorganer, og økt vilkårlighet i anvendelse av lover og reguleringer som forhindrer og bekjemper økonomisk kriminalitet.

Ulike risikoområder vil smelte sammen

I takt med økt geopolitisk spenning, sanksjoner og handelsrestriksjoner, øker risikoene for at statlige og ikke-statlige aktører vil forsøke å benytte seg av kriminalitet og kriminelle nettverk for å tilegne seg midler. Dette innebærer at finansinstitusjonenes rolle for å understøtte nasjonale sikkerhetsinteresser blir tydeligere.

Økte forventninger og krav til teknologiske løsninger utfordrer kontrollfunksjoner

Den teknologiske utviklingen i finansindustrien går svært raskt. Innovasjon innen finans kommer kundene til gode, men det gir også nye sårbarheter kriminelle kan utnytte. Bedragerne vil fortsette sin utvikling av metoder og verktøy for å gjennomføre bedragerier mot våre kunder.

Trusselvurdering 2024 - DNB Livsforsikring

Bedrageritrusselen tilknyttet livsforsikring vil fortsatt være høy i 2024 og vi forventer å oppleve en økning av svindelforsøk hvis økonomiske nedgangstider vedvarer. Enkelte ansatte i hardt rammede bedrifter vil forsøke å utnytte ulykkes- eller uføreforsikringer da disse kan gi høyere utbetalinger enn arbeidsledighetstrygd.

Vi forventer at det er «vanlige kunder» som vil stå bak de aller fleste forsøkene på forsikringssvindel mot DNB Liv i 2024, med en mulig dreining mot en stadig yngre del av kundegruppen. Vi forventer ikke at DNB Liv vil bli rammet av sofistiskert forsikringssvindel fra kriminelle miljøer.

DNB