Trusselvurdering 2021

DNB

TRUSSELVURDERING 2021

Årlig trusselvurdering 2021 er utarbeidet av Group Security og Financial Cyber Crime Center med bidrag fra DNB Livsforsikring og NewTechLab/DNB.

Trusselvurderingen består av vurderinger av trusselnivået for DNB innenfor åtte ulike kategorier og seks artikler som omhandler generelle tema.

Rapporten tar sikte på å gi en bredest mulig vurdering av relevante sikkerhetstrusler mot DNBs virksomhet i en tidsramme av ett til tre år frem i tid.

Layout ved DNB Creative.

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

Innhold

Om årlig trusselvurdering

En strukturert tilnærming til trusselvurdering er et viktig verktøy for at sikkerhetsarbeid og forebygging av bedrageri skal fokuseres riktig. Det å lære av tidligere hendelser og trender for å se hvor trusselaktørene er på vei betyr at vi kan legge inn tiltak der det er mest hensiktsmessig.

I år som i tidligere år er det trusselaktiviteten i det digitale rom som øker mest. Året 2020 har vært preget av store utfordringer som resultat av Covid-19, og mer av vår aktivitet foregår digitalt. Mens verden går igjennom en av de største krisene siden andre verdenskrig, utnytter både enkeltindivider, organiserte kriminelle og statlige aktører situasjonen til å tilegne seg fordeler og økonomisk vinning.

For DNB er godt sikkerhetsarbeid en basis i det å sikre landets finansielle tjenester også igjennom utfordrende tider. For å øke bevissthetene gir vi derfor ut denne trusselvurderingen årlig, sammen med andre publikasjoner rundt cyberangrep og bedragerier. Dette håper vi skal bidra til god forståelse for de sikkerhetstiltak vi må ha på plass for å sørge for sikre og robuste tjenester, og for at de som leser den skal bruke den som utgangspunkt for å vurdere eget trusselbilde.

Vi står sammen i kampen mot dem som vil skade eller stjele fra oss.

Anders Hardangen
Sikkerhetsdirektør, DNB

Forord

Kriminalitetstruslene er mange, komplekse og stadig i endring. Endringene preges særlig av stadig økt globalisering av økonomien og virtualisering – mer av kriminaliteten flyttes på ulike måter inn i det digitale rom. Det gjelder både i forhold til hvordan kriminaliteten utøves og hvordan utbytte sikres. Politiet har selv beskrevet dette kriminalitetsbildet i flere rapporter det siste året, og Økokrim beskrev dette i vår trusselvurdering for 2020. De økonomiske tapene kriminaliteten påfører enkeltpersoner, næringslivet og samfunnet som sådan er enorme.

På toppen av dette er det grunn til å tro at Covid-19-pandemien på mange måter forsterker trusselen. Ikke bare utsettes ulike økonomiske Covid-19-støtteordninger for bedragerier, men utstrakt bruk av hjemmekontor har sannsynligvis også gjort både enkeltindivider og virksomheter mer sårbare for kriminalitet.

Trusselen kommer både fra enkeltindivider og kriminelle nettverk i Norge, men Økokrim mener at også trusselen fra internasjonale kriminelle nettverk er økende. Blant annet har vi pekt på kriminelle nettverk knyttet til fiskerikriminalitet, hvor det ligger store verdier, muligheter for fortsatt stor vekst, og inntil videre begrensede muligheter for effektiv kontroll fra myndighetenes side.

Selv om Norges relativt sett solide økonomi gjør oss attraktive for kriminelle aktører, er kriminalitetsbildet i stor grad del av en internasjonal utvikling. I Storbritannia mener flere at digitalt støttede bedragerier nå har et så stort omfang og genererer så stor profitt, at det truer nasjonal sikkerhet.

Arbeidet med å bekjempe disse truslene kan ikke alene gjøres av politiet eller av de enkelte virksomhetene hver for seg. Vi må arbeide sammen, og vi må arbeide tettere sammen. Innenfor de rettslige rammene må vi dele informasjon om truslene med hverandre mer systematisk enn hva vi klarer i dag. Bare slik kan vi forebygge kriminalitet på en god måte. DNB sitt arbeid med denne trusselvurderingen, og delingen av den, er derfor sett fra Økokrim sitt ståsted velkomment. På samme måte som jeg håper politiets og Økokrim sine trusselvurderinger brukes aktivt til å forebygge kriminalitet, er mitt håp at DNB sine kunder og andre bruker informasjonen i denne trussel-vurderingen til bedre å forebygge at de utsettes for kriminalitet. Delt kunnskap forebygger.

Oslo, 24. februar 2021
Pål K. Lønseth
Sjef for Økokrim

Nøkkelfakta

Voice-phishing og sosiale medier

ansatte vil utsettes for sosial manipulering også i 2021

Ingen norske selskaper er **immune mot innsidetrusler**

Nye muligheter og nye utfordringer

PSD2

Ansatte

fortsetter å bli truet på jobb

Løsepengevirus

det farligste digitale angrepet

Internasjonal datatrafikk

overvåkes hver eneste dag

En innsidehendelse

vil kunne utgjøre en betydelig belastning for en virksomhet

Bedragere angriper kundene våre

betydelig oftere enn de angriper DNB

DNB ser i dag sterk kobling til **grupperinger med stort voldspotensiale**

Kryptering

En forutsetning for tillit – kan kryptering knekkes?

****

I 2020 håndterte DNB

31 potensielt alvorlige saker

i det digitale domenet

Kriminelle

«outsourcer» og kjøper tjenester

Fysiske bankran

skjer sjeldent i Norge

Leveranse-kjedeangrep

mot IT-systemer

Terror

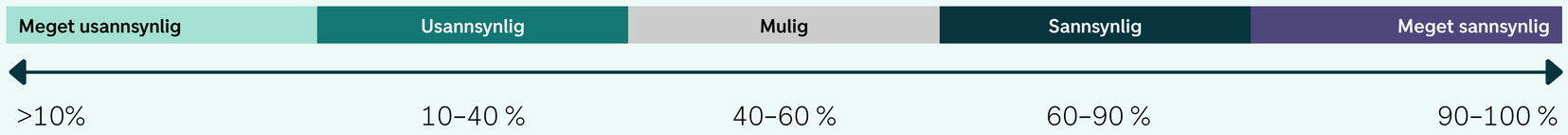
Like truet som samfunnet rundt oss

DNBs Financial Cyber Crime Center håndterte over

5000 saker i 2020

Trusselvurdering

Trusselnivå/sannsynlighet for hendelse	Beskrivelse av trusselnivå
KRITISK	Det er meget sannsynlig at DNB vil bli angrepet av avanserte ***eller*** koordinerte ***eller*** flere sammenfallende trusselaktører med intensjon ***og*** kapasitet til å påføre betydelig skade.
HØY	Det er sannsynlig at DNB vil bli angrepet av trusselaktør(er) med intensjon ***og*** kapasitet til å påføre betydelig skade.
MODERAT	Det er mulig at DNB vil bli angrepet av trusselaktør(er) med intensjon ***og*** kapasitet til å påføre betydelig skade.
LAV	Det er usannsynlig at DNB vil bli angrepet av trusselaktør(er) med intensjon ***og*** kapasitet til å påføre betydelig skade.
UBETYDELIG	Det er meget usannsynlig at DNB vil bli angrepet.



Digitale trusler

I flere år har de nasjonale etterretnings- og sikkerhetsorganisasjonene rapportert om et komplekst trusselbilde i det digitale rom. Årets vurderinger føyer seg inn i denne rekken. Det digitale risikobildet vurderes som skjerpet, og trusselaktører viser vilje og kapasitet til å ramme flere av Norges aller mest sentrale funksjoner og virksomheter. I DNB ser vi hver eneste dag at aktører forsøker å trenge inn i vår digitale infrastruktur. Det er et bredt spekter av trusselaktører der ute. Noen er ute etter økonomisk vinning, mens andre har industrispionasje som intensjon.

De kriminelle aktørene kjøper tjenester hos hverandre. Noen spesialiserer seg på å få tak i innloggingsdetaljer hos en virksomhet, noen er eksperter på å få tilgang til nettverk, og andre er eksperter på skadevare. De kjøper tjenester de behøver. På denne måten trenger ikke trusselaktørene å besitte all kunnskapen om hvordan et hackerangrep gjennomføres fra A til Å. E-post som inneholder ondartede lenker eller vedlegg, og digital infrastruktur som er eksponert på internett, er fortsatt de mest vanlige infeksjonsvektorene.

INFORMASJONSTYVERI

DNB besitter store mengder konfidensiell informasjon. Kundeinformasjon, innside-informasjon og ikke minst teknologi som gir oss en konkurransefordel, kan være interessant både for andre virksomheter og kriminelle, men også for fremmede stater. Likevel ser vi at de aller fleste forsøkene på å trenge inn i DNBs IT-systemer ikke handler om spionasje, men er økonomisk motivert.

DIGITALT BANKRAN

I løpet av 2020 har vi sett en nedgang i antall forsøk på digitale bankran. Vår hypotese er at banker generelt har brukt mer ressurser på å sikre sine systemer og betalingsløsninger, slik at det har blitt vanskeligere å gjennomføre digitale bankran. I stedet har flere av aktørene som tidligere begikk digitale bankran gått over til å bruke løsepengevirus for å oppnå økonomisk vinning.

Det at antall forsøk på digitale bankran viser en nedadgående trend, er likevel ingen hvilepute. Trusselaktørene fortsetter å utvikle seg, og historisk har det kun vært et tidsspørsmål før de er tilbake med nye metoder som kan forsere etablerte sikkerhetsmekanismer. Vi ser allerede at flere trusselaktører automatiserer inntrengingsforsøkene sine, og vi forventer at de vil fortsette med dette i større grad. Dette vil medføre en høyere kapasitet ved at de kan angripe flere mål, raskere. Det finnes eksempler på at kriminelle tar i bruk kunstig intelligens, og vi forvente at dette vil øke samtidig som teknologien utvikler seg.

I 2020 håndterte DNB 31 potensielt alvorlige saker i det digitale domenet.

LEVERANSEKJEDEANGREP

Leveransekjedeangrep er så aktuelt at det har fått en egen artikkel i starten av denne vurderingen. DNB, som alle andre virksomheter, benytter seg av en rekke programvarer og er avhengige av mange tjenesteleverandører. I leveransekjedeangrep utfører trusselaktøren cyberangrepet via en tredjepart, som ofte har dårligere sikkerhet enn sluttmålet. Vi må derfor stille tilsvarende krav til sikkerhet hos leverandørene som for oss selv, slik at de ikke blir et svakt punkt inn i vår infrastruktur. Det er også behov for å vurdere hvilke tilganger disse underleverandørene og programmene har behov for inn i DNBs nettverk.

I 2020 opplevde ett av DNBs utenlandskontorer at et program som benyttes for skatte-rapportering, hadde fått innlagt en bakdør i en sikkerhetsoppdatering. DNBs Cyber Defense Center undersøkte hendelsen, og konkluderte med at bakdøren til systemet ikke var benyttet, selv om de som hadde plassert den der hadde hatt muligheten. Datamaskinen som hadde dette programmet installert var ikke koblet til DNBs digitale infrastruktur, men var en frittstående datamaskin kun til dette formålet. Dersom bakdøren hadde blitt brukt, ville aktøren derfor kun fått tilgang til informasjon på denne maskinen – ikke til hele DNBs nettverk.

Destruktive angrep

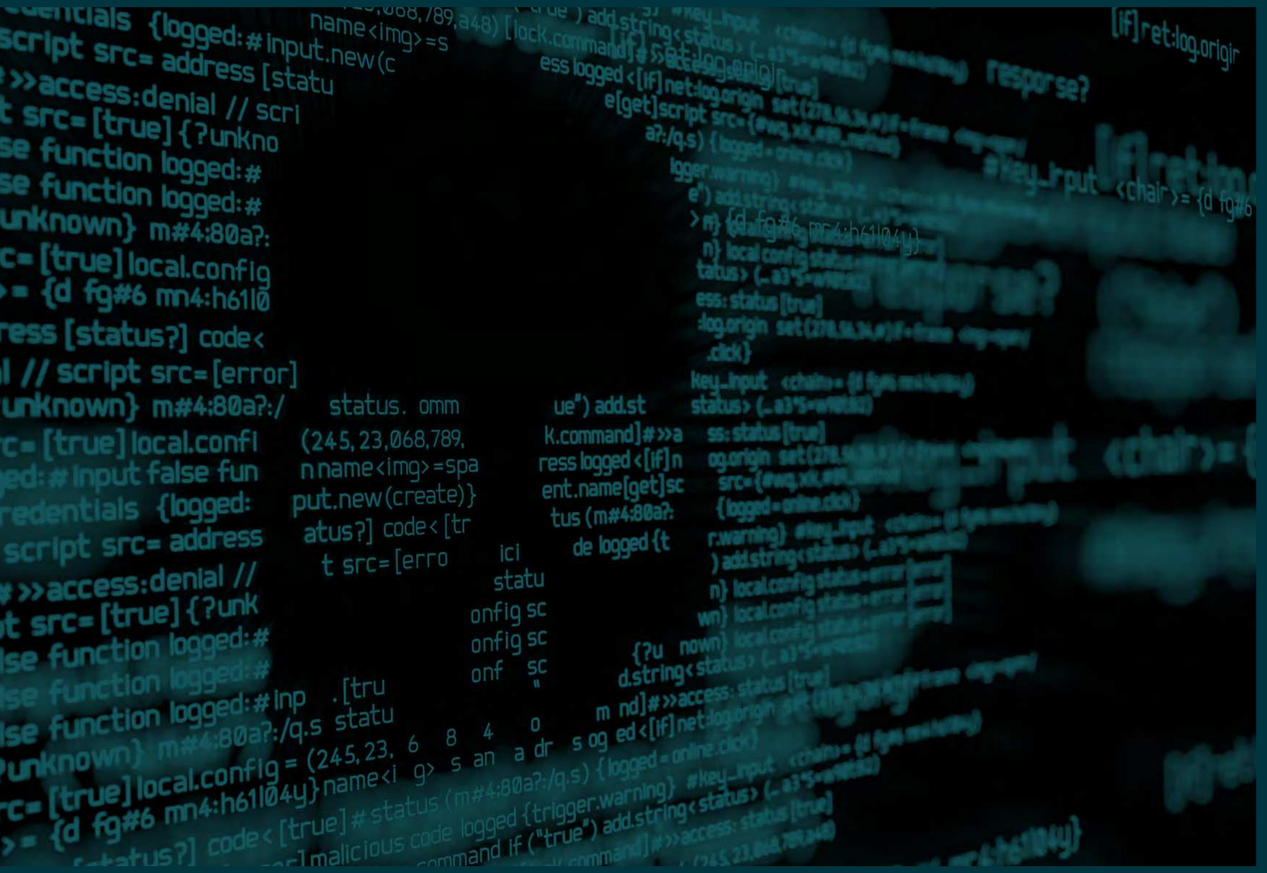
Når man snakker om destruktive angrep, snakker man om dataangrep hvor angriper forsøker å ødelegge noe for sitt offer. Motivasjonen kan være økonomisk vinning, å spre frykt, eller rett og slett sabotasje.

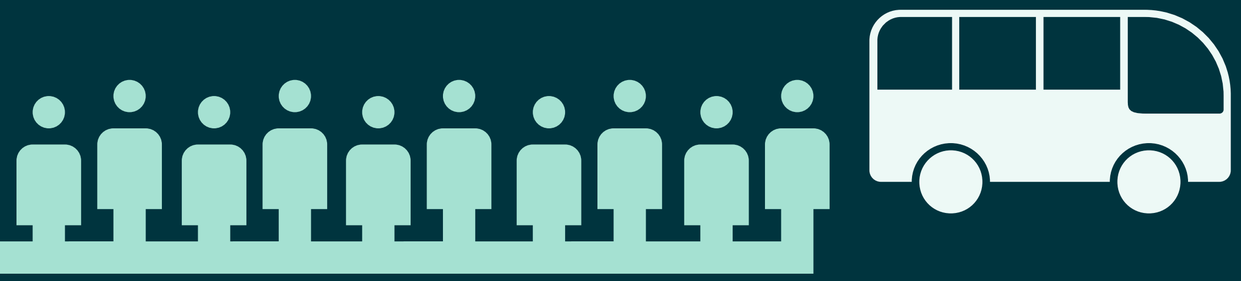
LØSEPENGEVIRUS

Løsepengevirus, eller krypteringsvirus, vurderes i dag som den største digitale trusselen mot DNB. Etter å ha hacket seg inn i den digitale infrastrukturen, krypterer angriperen alle filene på systemet slik at de blir utilgjengelige for brukeren. For å låse opp filene, krever angriperen løsepenger fra offeret.

Denne trenden har tatt seg opp det siste året, og vi leser stadig om nye virksomheter som blir rammet av løsepengevirus. Angriperne har videreutviklet metoden for å lykkes i å presse offeret for penger. Dersom offeret ikke betaler løsepenger for å låse opp filene, truer angriperen med å publisere interne dokumenter på internett, eller selge informasjon til høystbydende. Forretnings-idéen til angriperen er enkel: De ønsker å tjene penger på angrepet. Hvis ikke offeret ønsker å betale selv, håper de at andre er villige til å betale. Dette setter offeret i et skikkelig dilemma: Skal man betale løsepenger, eller risikere at intern informasjon om for eksempel klienter og deres transaksjoner publiseres? Dersom sensitiv informasjon kommer på avveie, kan det i tillegg resultere i brudd på personvern og bøter fra for eksempel Datatilsynet.

Slike angrep utføres ikke nødvendigvis av en aktør alene. Det har blitt mer og mer vanlig at en aktør har som oppgave å skaffe tilgang til et nettverk, for så å selge denne tilgangen til andre aktører som har kapabilitet til å gjennomføre selve krypteringen og innkrevingen av pengene.





TJENESTENEKTANGREP

For noen år siden var «tjenestenektangrep» en utbredt metode som rammet mange virksomheter. Dette innebærer at en angriper sender så mye datatrafikk mot en nettside at denne blir overbelastet og utilgjengelig. Se for deg at du skal ta bussen til jobb. Normalt sett er det kanskje 7–8 andre personer som skal ta bussen fra din holdeplass, men i dag har 7–800 personer møtt opp og vil inn på bussen! Det sier seg selv at ikke alle får plass, og at de vanlige passasjerene kanskje heller ikke kommer med. Samme prinsipp ligger til grunn i et tjenestenektangrep. For eksempel tar man med i beregningen at ca. 1 million brukere skal besøke nettbanken hver dag, og dimensjonerer den for det. Når noen velger å sende trafikk mot nettbanken tilsvarende flere hundre millioner kunder, klarer ikke nettbanken å håndtere alle forespørslene, og tjenesten blir utilgjengelig.

I oktober i fjor ble DNB utsatt for et slikt tjenestenektangrep som fikk konsekvenser for enkelte av bankens IT-tjenester en kort periode. En aktør sendte et trusselbrev til DNB, hvor det ble fremsatt krav om løsepenger for å stanse angrepet. Trusselaktøren startet det ble beskrevet som en forsmak på angrepet, og ga DNB en uke på å betale løsepenger. Ettersom DNB ikke betalte, startet de et oppfølgingsangrep ca. 3 uker senere. Innledningsvis førte dette til nedetid for noen av konsernets tjenester, men DNB fikk raskt stanset angrepet i samarbeid med sine leverandører på sikkerhetstjenester.

Flere andre finansinstitusjoner, også i Norden, ble rammet av samme typen angrep. Denne typen angrep krever ikke særlig høy teknisk kompetanse og forårsaker kun nedetid for den rammede virksomheten. Slike angrep gir ikke angriper tilgang til informasjon eller innsiden av nettverket.

UTSIKTER MOT 2022

Destruktive angrep har vist seg å være svært effektive, og vi forventer at trusselaktørene vil fortsette å utføre disse så lenge de oppnår økonomisk vinning.

Lokal, fysisk spionasje og informasjonstyveri

Politiets sikkerhetstjeneste skriver i sin åpne trusselvurdering for 2021 at nettverks-operasjoner vil utgjøre den største delen av russisk og kinesisk etterretningsaktivitet mot Norge. Like fullt vurderes også rekruttering av kilder og innsidere som en kjerneaktivitet for de statlige etterretningstjenestene. Det er ikke slik at trusselen fra fysisk spionasje hører fortiden til. Saken der en norsk statsborger sommeren 2020 ble siktet for spionasje til fordel for Russland har flere likhetstrekk med tilfeller fra våre naboland Sverige og Danmark som er offentliggjort siden 2019.

Vi må legge til grunn at DNB-konsernet besitter mye informasjon som kan være relevant både for etterretningstjenester og kriminelle. Som en naturlig del av bankvirksomheten besitter DNB person-opplysninger om individer med ulike roller og tilknytninger. Våre ansatte får innsyn i sensitive forhandlingsprosesser og blir tidvis kjent med innovative prosjekter og teknologi før disse treffer offentlighetens øye. DNBs forretningsforbindelser og kunder kan være det egentlige målet, både i et strategisk etter-retningsperspektiv, for industrispionasje eller for utpressingsformål.

DNB-ansatte kan utsettes for sosial manipulering og rekrutteringsforsøk fra profesjonelle aktører som arbeider for fremmed etterretning eller kriminelle nettverk. Dersom disse aktørene lykkes med sine fremstøt, kan dette få omfattende negative konsekvenser for DNB. Ingen norske virksomheter er immune mot innsidetrusselen – heller ikke DNB. I årets trusselvurdering har vi valgt å belyse innsidetrusselen i en egen artikkel. Dette gjør vi både for å skape bevissthet rundt problemstillingen internt i DNB, men også for å ta ansvar ved å løfte diskusjonen utad.

KARTLEGGING AV ANSATTE OG MILJØER I KONSERNET

DNB utsettes jevnlig for vishing, eller voice-phishing. Dette innebærer at ansatte blir ringt opp av aktører som under falskt flagg ber om opplysninger. Ofte fremstår dette som tilfeldig, men andre ganger kan DNB være mål for mer målrettede kampanjer der en trussel-aktør forsøker å tilegne seg informasjon om ansatte i et spesifikt område eller tilknyttet en bestemt avdeling. Slik kartlegging foregår også via sosiale medier. Også dette året har DNB avdekket og tatt ned flere falske profiler som sannsynligvis har uærlige hensikter.

UTSIKTER MOT 2022

Vi forventer at DNB vil utsettes for forsøk på kartlegging av enkeltmiljøer gjennom ulike former for informasjonsinnsamling.

DNB vil også kunne utsettes for fysisk spionasje og informasjonstyveri fra utenlandsk etterretning eller organiserte kriminelle grupper. Det er sannsynlig at ansatte vil bli utsatt for sosial manipulering fra aktører som forsøker å tilegne seg intern informasjon.

Ran og voldelig utpressing

Banker, postkontor og verditransporter ranes sjeldent i Norge. Det er en viss interesse for mål i Norge fra svenske ransligaer. Trusselen vurderes foreløpig å være redusert som følge av Covid-19 tiltak.

I 2020 ble ingen bankfilialer eller postkontor i Norge ranet. Dette er en nedgang fra foregående år hvor det har vært et stabilt nivå på ett til to tilfeller i året. Ranene i de to foregående årene har vært dårlig planlagt og utført av enkeltpersoner som har blitt pågrepet i løpet av kort tid.

Fravær av gjennomførte ran i Norge i 2020 må sees i sammenheng med nedstengningen som følge av Covid-19. Det norske samfunnet vil på et tidspunkt åpne opp igjen, og dette vil igjen gi publikum bedre tilgang til banklokaler.

Selv om dårlig planlagte ran utført av enkeltpersoner fremstår som amatørmessige, vil de likevel være farlige for kunder og ansatte. Ran og ransforsøk medfører også en betydelig psykisk belastning for de som blir truet, eller er i umiddelbar nærhet.

I de senere år har organiserte ran i Norge vært rettet mot andre mål enn kontanthåndteringskjeden til banker. Kriminelle har sett gullsmeder og virksomheter som omsetter luksusvarer som mer egnede mål.

I Sverige har Brottsförebyggande rådet fra 2019 til 2020 registret en nedgang av væpnede ran mot banker og verditransporter fra 10 til 6 , dvs. fortsatt betydelig høyere enn i Norge. Det er en vedvarende bekymring at svenske eller østeuropeiske organiserte ransmiljøer skal krysse inn fra Sverige. Mange av ransmiljøene i Sverige er godt organisert og har høyt voldspotensiale. Det har ikke vært konkrete hendelser fra svenske organiserte ransligaer mot bank og postkontorer i Norge på mange år, men i 2020 ble tre svenske statsborgere dømt for tre ran av butikker og et «sjokkbrekk» mot en minibank. Det siste var et væpnet ran av en gullsmed med en påfølgende dramatisk politijakt sentralt i Oslo i juli 2019. Som følge av Covid-19 restriksjoner og grensekontroll vurderes foreløpig trusselen fra svensk side som svært lav.

Gisseltakinger av nærstående til ansatte, med videre utpressing, forekommer meget sjeldent. Etter vår kjennskap har det ikke vært meldt om slike hendelser i Vest- og Nordeuropeisk bank- og finansvirksomhet i løpet av 2020, men rapportering av slike hendelser er trolig mangelfull og det er sannsynlig at det forekommer mørketall.

UTSIKTER MOT 2022

Antall ran mot bank- og postfilialer i Norge vil sannsynlig ligge på null til ett per år. Eventuelle ran vil sannsynlig utføres av enkeltpersoner.

Det er en meget liten, men likevel relevant, mulighet for at utenlandske ransligaer med sterkere organisering velger å rane et norsk bankkontor, postkontor eller verditransport. Det er en forutsetning at grensekontrollen mot Sverige som følge av Covid-19 oppheves for at et slikt scenario skal bli mulig.

Vold og trusler mot ansatte

I 2020 ble det registrert 28 tilfeller hvor DNBs ansatte i Norge ble utsatt for trusler eller utagerende atferd. Antall hendelser i 2020 er noe høyere enn i 2019 og tilsvarer om lag samme nivå som i 2018. Slike hendelser er trolig underrapporterte.

Det var flere hendelser i månedene juni til september sammenlignet med resten av året. Fordelingen er tilnærmet lik mellom tilfellene hvor truende eller utagerende personer var fysisk til stede, og tilfellene hvor truslene ble fremsatt per telefon, e-post eller chat. I årets siste måneder kom trusler kun pr telefon antakelig på grunn av nedstengninger i samfunnet på grunn av Covid-19.

I ett tilfelle ble en DNB ansatt utsatt for vold. Den ansatte ble delvis truffet av slag og påført mindre fysiske skader. Det blir ofte fremmet trusler med meget alvorlig ordlyd, og det er relativt vanlig at det trues med forskjellige former for voldshandlinger og drap. Slike hendelser påfører ansatte psykisk stress i varierende grad. For enkelte utgjør det en betydelig psykisk belastning, og det kan foreligge fare for psykiske ettervirkninger.

Det er privatkunder som fremmer trusler. Disse fremsettes ofte i situasjoner hvor kunden ikke får tilgang til penger og i noen tilfeller ikke får tilgang til banktjenester. Noen få av tilfellene, blant annet hendelsen hvor en ansatt ble lettere skadet, kan knyttes til tiltak ifb. Covid-19 nedstengning. To av tilfellene skyldtes misnøye under eiendomstransaksjoner.

Som følge av potensialet for personskade vurderes hendelser hvor den truende/utagerende personen er i umiddelbar nærhet av kunder, ansatte og/eller vektere som mest alvorlig. Det var et noe høyere antall trusler og utagerende adferd etter at Covid-19 nedstengningen traff det norske samfunnet, men i siste kvartal er dette tilbake på samme nivå som før tiltakene ble iverksatt. Når samfunnet igjen åpnes opp, forventes det igjen en lik fordeling mellom trusler som fremsettes i banklokaler og via telefon/chat/e-post.

Ingen av truslene rettet mot ansatte i 2020 har kunnet knyttes til organisert kriminell virksomhet. Sett opp mot utviklingen av organisert kriminalitet, som beskrives i temaet «En ny arena for organisert kriminalitet» lenger frem i denne vurderingen, er det et potensiale for at DNB ansatte vil bli utsatt for trusler fra organiserte kriminelle. Slike trusler kan ta forskjellig form, uttrykkes over lang tid og mulig uttrykkes såpass subtilt at de ikke faller klart inn under eksplisitte trusler mot liv og helse. Dersom det skulle forekomme trusler mot DNB ansatte fra organiserte kriminelle, kan det derfor være vanskelig å fange opp.

UTSIKTER MOT 2022

Omfanget og alvorlighetsgraden av trusler mot ansatte drives delvis av ytre samfunnsforhold og antakelig i noen grad av DNBs handlinger overfor kundene. I den videre vurderinger av antall trusler og utagerende adferd er det tatt hensyn til og justert for at det er mørketall i vår rapportering. Det vurderes at antallet hendelser hvor ansatte blir truet med fysisk skade, eller står overfor fysisk utagerende personer, vil ligge på 50–70 tilfeller per år i perioden frem til det norske samfunnet åpnes opp.

Avhengig av når og i hvilket omfang publikum igjen vil få tilgang til våre banklokaler forventes det at antallet trusler pr telefon/chat går noe ned mens vi igjen vil få en svakt økende andel hendelser hvor personen som truer eller utagerer befinner seg fysisk i våre banklokaler. Antallet hendelser ventes i denne perioden å avta til 35–50 hendelser per år.

Like truet som samfunnet rundt oss

DNB I NORGE

PST vurderer at ekstrem islamisme og høyreekstremisme utgjør den største terrortrusselen mot Norge. Det er mulig at både ekstreme islamister og høyreekstremister vil forsøke å gjennomføre terrorhandlinger i løpet av 2021 Videre har PST vurdert trusselen fra ekstreme islamister som skjerpet siden utgangen av 2020 som følge av økt spenning mellom ytringsfrihet og det mange muslimer opplever som krenkelser av islam.

Eventuelle terrorangrep motivert av ekstrem islamisme vil mest sannsynlig forsøke å ramme folkerike mål i det offentlige rom, eller symbolmål som kan assosieres med hån av islam, samt politi- og forsvarspersonell. PST vurderer videre at eventuelle høyreekstreme terrorangrep mest sannsynlig vil komme fra enkeltpersoner og rettes mot mål som inngår i det høyreekstreme fiendebildet. Samlingssteder for personer av ikke-vestlig opprinnelse, samt representanter for myndigheter og politikere som oppfattes å tilrettelegge for innvandring er blant mulige mål.

DNB I UTLANDET

DNB har en betydelig internasjonal virksomhet, og flere av landene vi har en tilstedeværelse i har vært utsatt for terrorangrep de seneste årene. Til tross for at terrortrusselen først og fremst har hatt sin grobunn i ekstrem islamisme har høyreekstreme strømninger fått økende fotfeste i flere land i Europa. Også i USA har økt polarisering i samfunnet medført at myndighetene vurderer trusselen fra høyreekstreme som skjerpet.

Ingen informasjon tilsier at DNB utpeker seg som et aktuelt mål for terrorhandlinger. DNB er like utsatt for terrortrusselen som samfunnet vi er en del av – både i Norge og utlandet.

UTSIKTER MOT 2022

Det er ingen informasjon som indikerer at DNB inngår i fiendebildet til ekstreme islamister eller høyreekstreme aktører verken i Norge eller i utlandet. Til tross for dette vil DNB kunne rammes indirekte av en eventuell terrorhandling rettet mot mål i umiddelbar nærhet til våre lokasjoner, eller dersom DNB-ansatte skulle oppholde seg på «feil sted til feil tid».

IKKE-VOLDELIG POLITISK AKTIVISME

DNB har en svært bred portefølje og virksomhet knyttet til mange ulike sektorer. Deler av vår virksomhet vil kunne oppfattes som kontroversiell av enkeltpersoner eller grupper.

Vi har ikke kjennskap til at DNB inngår i fiendebildet til enkeltpersoner eller grupper som tar i bruk voldelige virkemidler for å fremme sin sak. Det er imidlertid grunn til å forvente at enkeltpersoner eller grupper vil gjennomføre ikke-voldelige aksjoner eller markeringer i nærhet av DNBs lokaler for å skape medieoppmerksomhet rundt eget budskap.

Organiserte bedragere med DNB som mål

Kriminelle forsøker kontinuerlig å få tak i DNBs verdier ved å bedra konsernet. Rollen til kriminelle miljøer med en fysisk tilstedeværelse i Norge har den senere tiden blitt tydeligere og antall saker øker, blant annet som følge av automatisering.

I årsrapporten til DNBs Financial Cyber Crime Center for 2020 fremkommer det at kriminelle forsøkte å bedra DNB og våre kunder for 1,4 milliarder kroner. I tillegg til verdiene som kan gå tapt finnes koblinger til annen alvorlig kriminalitet som er vel så viktig å bekjempe som økonomisk tap.

Lånebedragerier er sentrale i bedragerier mot konsernet, og kan forekomme i alle låne-produkter konsernet tilbyr. Flertallet av sakene består av flere ledd hvor ID-tyveri, utnyttelse av svake grupper i samfunnet, nasjonale muldyr, falsk dokumentasjon og finansiering av biler alle spiller inn i større, organiserte bedragerier. Det finnes koblinger til organiserte kriminelle miljøer i Sverige, Litauen, Romania, Syria, og Albania. Trenden innenfor lånebedragerier vil trolig holde seg stabil fremover, men det er flere usikre faktorer som kan påvirke trusselen i begge retninger. Denne trusselen må sees i sammenheng med det som beskrives under temaet En ny arena for organisert kriminalitet i denne vurderingen.

Phishingangrep har lenge vært dagligdagse, men ofte av dårlig kvalitet. I 2020 opplevde man flere trender som økte trusselen på dette området. Den første utviklingen var automatisering, og phishing kjennetegnes nå av automatiserte oppringninger og beskjeder til mottaker. Ved kun å måtte forholde seg til de personene som allerede er i ferd med å gå på bedrageriet, evner mindre aktører å gjennomføre større angrep mens de store angrepene blir enda større.

Angrepssummen er ikke lenger på noen tusen kroner, men kan medføre tap på mange millioner. Som følge av erstatnings-reglene i Finansavtaleloven vil banken ofte, ved gjennomføring av transaksjoner, måtte erstatte tap som overskrider egenandelen på 12 000 kroner. Dette er grunnen til at phishing er plassert i trusselkategorien for bedrageri mot DNB.

Spear phishing har blitt mer vanlig og vi opplevde flere tilfeller av dette i 2020. Dette er en kjent modus innenfor cyberdomenet og bedragerier i utlandet, men norske bedragerier har ikke vært spesielt preget av dette hittil.

Flere aktører benytter også screen scraping for å samle informasjon om våre sider. Mange av disse bruker informasjonen de har innhentet til å opprette falske sider eller misbruke DNB sin logo.

Det er sannsynlig at nivåene av phishing vil være stabilt høye så lenge samfunnet preges av Covid-19, men sannsynligvis også lenger. Teknologi gjør det enklere å gjennomføre angrep som holder høy kvalitet uten at det krever høy teknisk kompetanse.

Målrettede, automatiserte angrep er allerede i gang, men etter hvert som kvalitet og volum på disse øker vil trusselen fra phishing-aktørene skjerpes. Det vil ta tid før denne trusselen materialiserer seg for fullt, men i tiden fremover vil vi se en kontinuerlig forbedring av slike angrep, samtidig som de kriminelle høster lavthengende frukter innen automatisering.

UTSIKTER MOT 2022

Organiserte miljøer med en tilstedeværelse i Norge vil prege lånebedrageriene mot konsernet, samtidig som phishing blir mer målrettet, automatisert og medfører stabilt høye tap.

DNB LIVSFORSIKRING

Bedragerier mot DNB Livsforsikring viste en økning i 2020 i forhold til tidligere år. Totalt 180 saker med mistanke om bedrageri ble utredet med en oppklaringsprosent på 64 %. For bedragerier mot pensjonsoppgjør i Bergen ble 31 saker avgjort med en kapitalisert besparelse på 97,5 millioner kroner. For bedragerier mot personalforsikring i Trondheim ble 25 saker avgjort med en kapitalisert besparelse på 40 millioner kroner.

Bedrageriene mot selskapet viste ingen nye metoder og de avslørte svindlerne er i all hovedsak alene om bedrageriet. Det har ikke fremkommet opplysninger i 2020 som tilsier at organiserte kriminelle utnytter DNB Livsforsikrings produkter for svindel.

Metodene for bedragerier mot pensjons-oppgjør har i 2020 fulgt de to tradisjonelle sporene som litt forenklet kan presenteres slik:

1. Late som om en er arbeidsufør mens en i realiteten er arbeidsfør for å få utbetalt en erstatning
2. Late som om en er frisk mens en i realiteten er syk for å få tegnet en uføreforsikring en ellers ikke ville fått.

For 2021 forventer vi en nedgang i bedragerier mot pensjonsoppgjør som følge av endringer i DNB Livs portefølje. Vi vurderer likevel at vi fra våren 2021 vil se økning i svindel knyttet til uføreprodukter. Dette har bakgrunn i NAVs statistikk og analyse av legemeldt sykefravær i Covid-19 perioden som har økt betydelig i grupper hardt rammet av oppsigelser og permitteringer.

Når det gjelder bedragerier mot personal-forsikring har metodene i hovedsak gått ut på å dikte opp eller overdrive yrkesskade-hendelser, samt holde tilbake informasjon om reelle hendelser som ville ha medført avkortning eller avslag.

For 2021 vil vi sannsynligvis se en økning i rapporterte bedragerier mot personalforsikring ettersom denne porteføljen har hatt en betydelig økning. Det er likevel ingen indikasjoner på at svindel generelt mot disse forsikrings-ordningene øker.

DNB Livsforsikring har i 2020 begynt utviklingen av et databasert system som skal forsøke å identifisere mulig svindel mot selskapets uføreforsikringer. Systemet vil etter all sannsynlighet bidra til bedrageribekjempelsen i 2021.

PHISHING

Phishing er en metode for å lure til seg sensitive opplysninger, som brukernavn og passord, koder og kredittkortnumre.

SPEAR PHISHING

Spear phishing er en skreddersydd og målrettet type phishing som bruker personlig informasjon om et individ for å virke mer troverdig.

Bedrageri – en høy trussel mot våre kunder

Bedragere angriper kundene våre betydelig oftere enn de angriper oss. DNBs Financial Cyber Crime Center skriver i sin årsrapport at de håndterte over 5000 saker i 2020. Dette utgjør en økning på 25 % fra 2019 og bedragerier i digitale kanaler har økt med 300 % siden 2018. De aller fleste av disse sakene var rettet mot våre kunder.

PÅVIRKNINGEN AV COVID-19

Covid-19 har påvirket måten kriminelle aktører angriper sine mål. Innenfor de fleste bedragerityper er det primært snakk om å endre metoder, snarere enn å introdusere nye former for bedrageri. Unntakene er Advance Fee Fraud og bedragerier som retter seg mot statsgaranterte lån.

Advance Fee Fraud har lenge vært mye brukt i utlandet og har, i sin enkleste form, også funnet sted i Norge. Økningen av denne typen bedrageri var betydelig i 2020 og rettet seg nesten utelukkende mot kunder som forsøkte å ta opp lån hos det de trodde var utenlandske finansinstitusjoner. DNB vurderer at det er to store drivere bak dette. Den første er Covid-19 som har satt mange mennesker i en prekær økonomisk situasjon. Den andre er det nye gjeldsregisteret som har ført til at mange av dem som tidligere ville fått lån i norske finansinstitusjoner nå får avslag. Dette fører til at flere forsøker å dekke kredittbehovet sitt ved å finne finansinstitusjoner som er villige til å låne ut penger på nett.

Statsgaranterte lån har også blitt utnyttet av både enkeltaktører og organiserte kriminelle miljøer ved at det er søkt om lån på uriktig grunnlag. Bedragere utnytter ikke bare at mange er i en vanskelig økonomisk situasjon, men også tiltakene som er på plass for å hjelpe folk under krisen. Denne situasjonen vil høyst sannsynlig fortsette så lenge pandemien definerer så mye av hverdagen som den gjør i dag.

UTSIKTER MOT 2022

Bedrageritrusselen mot våre kunder er høy, og vi mener dette nivået vil vedvare frem mot 2022. Det er svært sannsynlig at dette vil medføre høye tap. Videre er det sannsynlig at det vil dukke opp saker med ekstraordinære angrepssummer.

INVESTERINGSBEDRAGERIER OG KJÆRLIGHETSBEDRAGERI

Investeringsbedragerier på falske nettbaserte handelsplattformer har over flere år vært den største bedrageritrusselen mot våre privatkunder. Flere kunder enn noen gang har falt for denne bedrageriformen, og Europol advarte i 2020 om at de få landene i Europa som ikke var berørt av investeringsbedrageri kom til å bli det i løpet av året. Dette er et vekstområde for organiserte kriminelle miljøer, hvor de globale tapene måles i milliarder av kroner.

Pyramideselskap, eller såkalte Ponzi Schemes, er nært beslektet til investeringsbedragerier, men utbredelsen av slike går gjerne i bølger. Vi er nå inne i en periode hvor flere av disse bedrageriene er i vekst, men det kan til tider være krevende å skille legitime aktører fra kriminell virksomhet.

Antallet kjærlighetsbedragerier holder seg fremdeles relativt stabilt, men det er verdt å gjenta at disse bedrageriene bare til dels er ment som inntektskilde for mange av trusselaktørene. Bedrageriene spiller imidlertid en sentral rolle i å flytte og hvitvaske penger ved at ofrene manipuleres til å flytte utbyttet fra bedragerier via egne konti.

Frem mot 2022 kommer fremdeles investeringsbedragerier til å utgjøre den største bedrageritrusselen mot våre privatkunder. Aktørene som utgjør hoveddelen av denne trusselen er avanserte organiserte kriminelle grupperinger, ofte med koblinger til Øst-Europa og Israel. Disse grupperingene har tid, nettverk, kompetanse og økonomiske ressurser, og kommer til å fortsette å bruke ofre for kjærlighetsbedragerier til å flytte og hvitvaske penger.

BUSINESS EMAIL COMPROMISE

Bedrageritrusselen mot våre bedriftskunder er fremdeles størst innenfor Business Email Compromise (BEC). Her forsøker aktører å etterligne eller kompromittere en epost og få ansatte eller kunder til å overføre penger eller sende regninger med feil kontonummer. Globalt står BEC for de største tapene innen bedrageri og FBI rapporterer fire ganger høyere tap til BEC sammenlignet med kjærlighetsbedragerier, som utgjør andreplass på listen.

Angrepssummene har økt betraktelig de siste årene, og avanserte grupperinger er oftere involvert i bedragerier fra ti millioner og oppover. Dette kulminerte i 2020 med et tap på hundre millioner i én BEC sak, noe som kan betegnes som en ekstraordinær angrepssum. Saker med så høyt tap er vanskelig å forutse og det reflekterer på ingen måte at alle aktørene nå retter seg mot angrep i denne størrelsesordenen. Noen aktører går etter høyere beløp enn andre. Vi anser det likevel som svært sannsynlig at området i tiden fremover fortsatt vil domineres av avanserte aktører som vil gå etter høye beløp.

AUTOMATISERING

Flere av områdene som påvirker våre kunder vil preges av automatisering i tiden som kommer. I artikkelen om bedragerier mot DNB har vi belyst hvordan automatisering påvirker phishing, men så å si alle bedrageriområdene vil kunne spisses ved at de kriminelle bruker ressurser på automatisering.

Group IB meldte nylig at 40 russisktalende kriminelle grupperinger hadde automatisert deler av dialogen med sine ofre i bedragerier gjennomført i Russland i det som ble kjent som Classiscam saken. Mange av disse grupperingene endret fokuset sitt mot mål i Europa i januar 2021.

Det er grunn til å tro at vi vil se flere slike forbedringer i prosessene til de kriminelle i tiden som kommer.

ADVANCE FEE FRAUD

Advance Fee Fraud er når et offer for bedrageri betaler et forskudd for å få noe av større verdi tilbake, f.eks. i form av lån, avkastning på investering, gaver eller lignende. Offeret mottar imidlertid aldri det hun eller han i forkant har betalt for.

BUSINESS EMAIL COMPROMISE (BEC)

Bedragere forsøker å kompromittere epostkontoen til en bedrift for å få bedriften eller en tredjepart til å overføre penger.

CLASSISCAM

Russisktalende kriminelle grupperinger forsøker å bedra forbrukere gjennom annonser på nett. Kommunikasjonen med ofrene er til stor grad automatisert.

Den britiske tenketanken Rusi skrev i januar at bedragerier mot privatpersoner og næringslivet var blitt så alvorlig at det måtte sees på som en trussel mot nasjonal sikkerhet og mente det krevde en respons fra sikkerhets- og etterretningstjenestene.

Tema

Leveransekjedeangrep

Det finnes mange måter å hacke en virksomhet på for å få tilgang til informasjon eller utføre sabotasje. Noen av de mest vanlige og kjente metodene er ved hjelp av infiserte epost-vedlegg, lenker til nettsider som laster ned skadevare eller utnyttelse av sårbarheter i internetteksponerte tjenester eller digital infrastruktur.

De siste årene har en annen metode fått stor oppmerksomhet: Leveransekjedeangrep (supply chain attack). Dette er betegnelsen på angrep hvor en trusselaktør infiltrerer et datasystem eller nettverk via en partner eller leverandør som har rettmessig tilgang. Denne typen angrep fikk bred medieomtale i 2020, da det velrennomerte cybersikkerhets-selskapet FireEye gikk ut offentlig og fortalte at de var blitt utsatt for et slikt angrep. FireEye anses som et av de mest spesialiserte og anerkjente sikkerhetsselskapene innenfor håndtering av målrettede, skadelige cyberoperasjoner.

FireEye benyttet seg av programvare fra en leverandør som heter SolarWinds. Da de installerte en sikkerhetsoppdatering til programvaren hadde trusselaktøren endret denne slik at den inneholdt en bakdør som ga tilgang til systemene. Flere sikkerhetsselskaper knytter trusselaktøren bak angrepet til russisk etterretning. FireEye har selv uttalt at trussel-aktøren var interessert i informasjon om flere av deres mest profilerte kunder, i tillegg til angrepsverktøy som selskapet har utviklet for å utføre legitime penetrasjonstester for å avdekke sårbarheter mot firmaer som ønsker dette.

I etterkant har det også kommet frem at en rekke andre virksomheter har vært rammet av samme angrep. Sikkerhetsoppdateringen som inneholdt bakdøren ble lastet ned over 18 000 ganger – noe som betyr at det potensielt kan være like mange ofre i saken. I Norge har Oljefondet offentliggjort at de fikk bakdøren installert. På kundelisten til SolarWinds er en rekke prominente virksomheter, blant annet flere av de amerikanske departementene, sikkerhetstjenester, NASA, Microsoft, Visa, Mastercard, PwC, Lockheed Martin, New York Times og mange flere. Det betyr ikke at disse virksomhetene har vært kompromittert i kampanjen, men kan fortelle oss noe om hvem trusselaktøren egentlig forsøkte å få tilgang til.

I et leveransekjedeangrep utnytter trusselaktøren en etablert tillit mellom to selskaper. Trusselaktøren utnytter den allerede etablerte kanalen i selve infiltrasjonen av sitt sluttmål. Kundelisten til SolarWinds gjør det lett å forestille seg hvorfor akkurat dette selskapet ble brukt som et ledd i leveransekjedeangrepet. Det legges til grunn at flere av virksomhetene på kundelisten har god IT-sikkerhet med få eksterne og svake angrepspunkter på internett. Trusselaktørene kan enten forsøke å gjennomføre cyberoperasjoner mot hver enkelt av disse virksomhetene, eller de kan bruke alle sine ressurser på å kompromittere én som har legitim tilgang til alle gjennom å være underleverandør av en programvare alle benytter. Det kan se ut til at nettopp det sistnevnte har vært tilfelle i SolarWinds-saken.

Det finnes flere andre eksempler på leveransekjedeangrep. I perioden 2016–2019 pågikk en større kampanje populært kalt «Operation Cloud Hopper». Kampanjen ble knyttet til kinesiske myndigheter av flere store sikkerhetsselskaper. I en Reuters-artikkel kom det frem at flere store leverandører av IT-tjenester skal ha vært kompromittert i denne kampanjen, blant annet Hewlett Packard, IBM, Fujitsu, Tata Consultancy Services og NTT Data. Disse tjenesteleverandørene har en rekke kunder over hele verden, hvorav flere ble kompromittert via tilgangen tjenesteleverandørene hadde til deres nettverk. Målet til trusselaktøren var å drive industrispionasje mot flere selskaper innenfor blant annet industri, bioteknologi og telekom. Svenske Ericsson og sveitsiske Syngeta er to av virksomhetene som var sluttmål i kampanjen.

Installering av sikkerhetsoppdateringer er «best practice» innenfor IT-sikkerhet. At trusselaktører velger å utnytte dette som en angrepsvektor blir derfor et enormt paradoks når man skal beskytte virksomheten sin fra å bli kompromittert.

HVORDAN BESKYTTE SEG MOT LEVERANSEKJEDEANGREP?

For en virksomhet som DNB er det nødvendig å kjøpe programvare og tjenester for å kunne levere finansielle tjenester. Eksemplene over viser viktigheten av å ha et bevisst forhold til tredjepartsleverandører og god oppfølging av sikkerhet både under anskaffelse og så lenge programvaren eller tjenesten er i bruk. Grunnen til at digitale leveransekjedeangrep lykkes, er at det er vanlig å ha høy tillit til eksterne tjenester og leverandører. Programmer som installeres kan få rettigheter og tilgang til mer enn de behøver, og har denne tilgangen til enhver tid snarere enn basert på en kontinuerlig vurdering av behov. På den måten er det vanskelig å stanse et angrep – trusselaktøren som bruker en tjenesteleverandør eller programvare som angrepsvektor har fått bred tilgang til nettverket i det den er på innsiden. Det kan sammenlignes med å få tilgang til universalnøkkelen til et hus.

Man kan for eksempel sammenligne det med andre tjenester som DNB kjøper, enten ved at vi får det levert eller betaler andre for å gjøre jobben. Hvis DNB skal få levert avisen, har kanskje avisbudet behov for å få tilgang til resepsjonen for å legge ifra seg avisene der. Da får avisbudet tilgang til resepsjonen på sitt adgangskort – ikke til kontorlokaler, bankhvelv og møterom. Tjenesteleverandører og programvare bør ikke ha tilgang til mer enn nødvendig – da slipper man unødvendig høy risiko.

Å installere sikkerhetsoppdateringer for programvare, eller tillate tjenester tilgang til nettverket er en nødvendighet for å få gode IT-tjenester. Adekvate tiltak må imidlertid iverksettes for å redusere risikoen for at en trusselaktør kan utnytte dette for å utføre et angrep via en leverandør. Her er det viktig å ha gode prosesser på plass for å regelmessig evaluere sikkerheten. Samtidig bør gode sikkerhetsprinsipper slik som «least privilege» og «zero trust» etableres for å redusere sannsynligheten for at en hendelse kan inntreffe.

Når trusselen kommer fra innsiden

Innsidetrusselen er et krevende område å balansere. Dette er det mange grunner til, men det skyldes kanskje særlig at vi ønsker å bevare en gjensidig tillit mellom arbeidsgivere og ansatte. Når man slipper noen på innsiden, enten som ansatt, konsulent eller leverandør, ligger det en implisitt tillit i at personen må få nødvendige tilganger for å utføre sitt virke. Det er viktig å balansere tilgang og kontroll slik at arbeidet kan utføres på en hensiktsmessig og effektiv måte samtidig som risikoen for misbruk av tilgang og informasjon begrenses. Skulle en innsidehendelse oppstå vil dette kunne utgjøre en betydelig belastning for virksomheten, både gjennom tap av omdømme og fallende aksjekurser. Og ikke minst tapt tillit.

Skadepotensialet til en innsider strekker seg over et bredt spekter, og henger i stor grad sammen med hva slags informasjon personen har tilgang til. Dette kan tolkes både bokstavelig i form av fysisk tilgang til verdier, eller tilgang til informasjon og IT-systemer der de mest kritiske verdiene for en virksomhet ofte befinner seg. De fleste trusselscenarioer vil bli verre dersom trusselaktørene kommer «på innsiden».

De fleste tilsiktede innsidesakene dreier seg om selvmotiverte ansatte som på eget initiativ velger å begå handlinger for egen vinning eller for å skade virksomheten de arbeider for. I et slikt scenario er det riktig å beskrive den ansatte som en trusselaktør. Disse kan være motivert av økonomisk vinning, anerkjennelse, ideologi eller misnøye.

En rekke ulike aktører som utgjør en trussel mot DNB og finansnæringen ønsker å rekruttere innsidere. Innsideaktivitet kan arte seg på svært ulikt vis. På den ene siden står den «ubevisste innsideren» som helt uten intensjon kan volde betydelig skade gjennom å bli utnyttet av en trusselaktør på utsiden. På den andre står «den bevisste innsideren» som med intensjon begår handlinger som skader virksomheten. Om lag en tredjedel av kjente innside-saker inngår i denne kategorien.

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

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

I trusselvurderinger er det nettopp tilsiktede handlinger, der en aktør har intensjon om å utgjøre en trussel, som er tema.

I andre saker står trusselaktøren på utsiden og forsøker å rekruttere ansatte til å agere som innsidere. Omtrent 16 % av de bevisste innsiderne er rekruttert fra en stilling de har, mens 6 % infiltrerer et selskap i den hensikt å agere som innsidere. Noen saker der dette skjer får mye oppmerksomhet. Ett eksempel er saken fra sensommeren 2020 der PST pågrep en mann mistenkt for å ha overlevert sensitiv informasjon til russisk etterretning. Selv om dette var første gang en norsk statsborger er blitt pågrepet av PST på et slikt grunnlag siden 1984 er saken en tydelig påminnelse om at vi må ta innsidetrusselen på alvor.

I saker der enkeltpersoner utsettes for sosial manipulering spiller trusselaktørene på sårbarheter og muligheter. Aktørene som står bak slik tilnærming er eksperter på å «trykke på de rette knappene», og man kan havne i en situasjon man aldri så for seg å havne i. Rekruttering av innsidere er ikke bare aktuelt for etterretningstjenester som vil ha tilgang til sensitiv informasjon, men også for organiserte kriminelle grupperinger. Også informasjon vi ikke tenker på som spesielt sensitiv kan utgjøre puslespillbrikkene som mangler.

Organiserte kriminelle kan enten prøve å få noen som allerede er på innsiden til å bistå dem eller de kan forsøke å plassere noen på innsiden. Politiet har i flere år advart mot at «organiserte kriminelle grupper forsøker å infiltrere næringslivet og offentlige instanser» og at disse gruppene ønsker tilgang for å tilegne seg verdier direkte eller for å fremskaffe informasjon som kan videreselges eller benyttes til utpressing av næringslivsaktører.

Næringslivet er en kilde til både penger og informasjon, og har ofte også en sentral rolle i drift av samfunnets kontrollinstanser og å rapportere på avvik. For finansbransjen tar disse kontrollinstansene blant annet form som anti hvitvasking eller bedragerihåndtering. Informasjon som teledata, regnskap og over-våkningsbilder kan også være av betydelig interesse for organiserte kriminelle. Slik informasjon er tilgjengelig innen mange ulike bransjer som en konsekvens av de kontroll-mekanismene som er iverksatt. Næringslivet blir dermed både en kilde til penger, et sted å hvitvaske penger, men samtidig også stedet mange av de ulovlige midlene blir oppdaget og hentet tilbake.

Det er få kjente eksempler på innsidesaker med en tydelig kopling til organisert kriminalitet, men de eksemplene vi kjenner viser at slike forhold kan få alvorlige økonomiske konsekvenser og ha betydelig negativ innvirkning på omdømmet til en virksomhet.

For å være godt rustet til å håndtere innside-trusler må vi kunne ha en åpen og ærlig diskusjon om innsidetrusler. Vi må jobbe for å finne gode løsninger som motvirker innside-trusselen uten at dette går på bekostning av effektiviteten. Samtidig må vi sørge for å ivareta tillitsforholdet mellom arbeidsgiver og arbeids-takere, kunder og næringsliv. Vi snakker ofte om at god kontroll ikke er et resultat av mistillit, men et utrykk for god service. På samme måte bør fokus på innsideaktivitet oppfattes som at man er sitt ansvar og sin rolle bevisst, snarere enn et uttrykk for at arbeidsgivere mangler tillit til sine ansatte.

PSD2: Nye muligheter og nye utfordringer

Det nye PSD2-regelverket gjør det mulig å gi tillatelse til at betalinger initieres av andre enn den banken man har konto i. Dette innebærer at man vil kunne samle oversikten over konto-eene man har i ulike banker på ett sted, og derifra gjennomføre betalinger.

Intensjonen er at PSD2 skal føre til mer oversiktlige bankforhold, mer konkurranse og innovasjon innenfor betalingstjenester, samt bedre sikkerheten gjennom krav til økt beskyttelse mot bedragerier. En slik utvikling er svært positiv for både betalingstjenester og forbrukere. Likevel er det en risiko knyttet til at kriminelle utnytter smutthull i betalingskjeden. Denne artikkelen tar for seg de nye utfordringene PSD2 medfører innenfor bedragerifeltet.

DE NYE SIKKERHETSKRAVENE

PSD2 vil høyst sannsynlig forbedre sikkerhetsnivået i flere europeiske land. Dette vil få positive ringvirkninger også for Norge ettersom dårlig sikkerhet hos i enkeltland påvirker hele finansbransjen. Ettersom direktivet skal passe hele Europa tar det imidlertid ikke høyde for at Norge har vært langt fremme på dette området, spesielt med tanke på bruk av BankID og det direktivet kaller sterk kundeautentisering.

Med innføring av det nye regelverket vil mottakere kunne merkes som «sikre», slik at kravet til sterk kundeautorisering bortfaller i transaksjoner til disse. Dersom finansinstitusjoner gjør dette ligger risikoen hos dem. Forbrukere skal imidlertid også gis anledning til å merke mottakere på tilsvarende måte. Dette innebærer at kunder som utsettes for manipulering vil stå i fare for merke konti som tilhører bedragere som sikre. Det er viktig å balansere sikkerhet med smidige kundeløsninger for forbrukerne. Samtidig er det helt avgjørende å sørge for nye forbrukervennlige løsninger ikke medfører dårligere sikkerhet enn vi har i dag.

For å omgå eksisterende sikkerhetstiltak, stjele og hvitvaske penger må trusselaktørene kamuflere sine transaksjoner. En av hovedhensiktene med PSD2 er å gjøre

PSD2
Payment Services Directive nr. 2 (PSD2) er den nyeste versjonen av EU-direktivet som regulerer betalingstjenester i EUs indre marked.

PENGEMULDYR
Et pengemuldyr er en person som tar imot penger fra en person og overfører det videre til noen andre, ofte mot betaling. Pengemuldyr er sentrale i hvitvaskings-prosessen fordi de hjelper kriminelle å flytte og skjule penger.

EXIT SCHEME
Exit scheme er et bedrageri hvor et etablert selskap eller en tjeneste slutter å levere en tjeneste eller et produkt, men fortsetter å ta betalt for dette. Innen kundene forstår at de ikke mottar det de betaler for har de kriminelle stjålet pengene og forsvunnet.

transaksjoner mellom enkeltpersoner raskere og enklere. Vi ser allerede nå at de kriminelle manipulerer ofre for bedragerier til å opptre som pengemuldyr ved at de overfører utbytte fra straffbare handlinger. Deteksjon og utredning blir vanskeligere når PSD2-betalinger kan gjennomføres av en tredjepart. Hva slags informasjon som kan deles mellom ulike finansinstitusjoner er strengt regulert. En fragmentert utredning der hvert ledd får tilgang til mindre informasjon vil utgjøre en fordel for trusselaktørene.

APPER, NETTSIDER OG EXIT SCHEMES

I januar 2021 advarte Interpol samtlige medlemsland om at kriminelle i større grad enn før utvikler egne apper for å gjennomføre bedragerier. Kvaliteten på de falske appene varierer, men noen er troverdige. Falske nettsider og handelsplattformer på nett har allerede lurt europeere for milliarder av euro og har vist at det er vanskelig å skille de ekte aktørene fra de kriminelle. Dersom apper eller nettsider brukes for å få mulighet til å initiere betalinger, vil forbrukere kunne forledes til å gi tilgang til at betalinger initieres på deres vegne. Trusselaktørene kan så vente til de har et tilstrekkelig antall «kunder» og initiere mange betalinger til seg selv på en gang. En variant av dette er et kjent fenomen blant annet innen krypto-bransjen er såkalte «exit schemes».

AKTØRER OG UTVIKLING

Innenfor økonomisk kriminalitet deler vi organiserte miljøer i to grupper, mindre og mer avanserte. Begge gruppene vil søke å utnytte PSD2, men innledningsvis vil dette sannsynligvis gjøres på ulike måter.

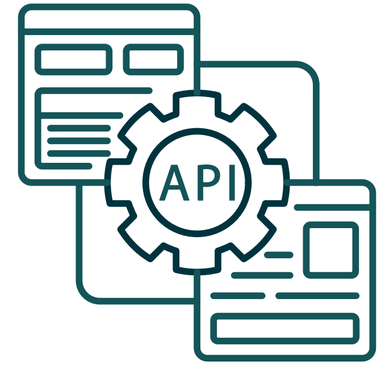
I 2019 ble eldre kvinner utsatt for bedrageri over telefonen, etter hvert kjent som Olga-svindel.

Her forsøkte organiserte bakmenn å skjule flere av transaksjonene som PSD2-transaksjoner. Investeringsbedrageri er et annet område hvor flere transaksjoner har utnyttet mulighetene PSD2 har åpnet for. Denne bedragerityPen utgjør den største bedrageritrusselen mot våre privatkunder og dekkes nærmere i kategorien Bedrageri mot våre kunder. Trusselaktørene har allerede begynt å utnytte potensialet som ligger i PSD2. Det er for tidlig å sammenfatte noen god statistikk på området. Vi forventer imidlertid at bildet av denne trusselen vil bli klarere i nær fremtid når nye kundeløsninger tas i bruk for fullt.

Når det gjelder exit schemes er det lite sannsynlig at dette vil utvikle seg til et stort problem over natten. Falske apper og nettsider for denne typen bedrageri vil høyst sannsynlig være forbeholdt et fåtall aktører innledningsvis. Det vil kreve tid, teknisk kompetanse, kjennskap til hvordan reelle tjenester fungerer, juridisk forståelse, markedsføring, økonomisk investering og mye annet som kan for mindre aktører er utenfor rekkevidde. Trusselaktørene må også forsere implementerte kontroller i de ulike plattformene. Dersom exit schemes, eller en variant av disse, blir et omfattende problem vil dette trolig domineres av de mer avanserte organiserte kriminelle miljøene, eller enkeltaktører med høy kompetanse og gode ressurser.

Slike avanserte bedragerier blir ofte mer tilgjengelig for de mindre avanserte aktørene over tid. Dette skjer som regel først når metodene og verktøyene til de avanserte aktørene blir mer kjent og det er tydelig at det er penger å hente. Når dette skjer faller ofte kvaliteten på bedragerie ne, samtidig som man ser en eksplosiv utvikling i antall saker.

Hverken finanssektoren, tredjeparter som ønsker å tjene penger på PSD2 eller forbrukere er tjent med at kriminelle miljøer utnytter nye systemer og øker sin kapasitet. Konsekvensene av sterke organiserte kriminelle miljøer er ikke et problem som begrenser seg til finansbransjen alene. Det er og blir et samfunnsproblem.



En ny arena for organisert kriminalitet

Den organiserte kriminaliteten i Norge øker. Kriminelle grupperinger som lenge har bedrevet det vi forbinder med klassisk organisert kriminalitet finner veien over til nye områder. Hva skjer når de tar med seg den gamle verktøykassen inn i domenet for økonomisk kriminalitet?

KNYTNINGER TIL INTERNASJONAL ORGANISERT KRIMINALITET

Vi har lenge kommunisert at mye av kriminaliteten vi ser på nett gjennomføres av kriminelle i utlandet. Kriminelle velger å angripe mål i andre land for å vanskeliggjøre politiets etterforskninger og andre utrednings-prosesser. Ettersom kriminelle som opererer på nett har en hel verden å plukke sine mål fra, er det helt unødvendig å lette politiets etter-forskninger ved å ramme mål i sitt eget politi-distrikt. Det skal likevel sies at kriminalitet på internett uansett er et område med generelt lav risiko for å bli tatt, lave strafferammer og høy profitt.

Allerede i 2009 mente Symantec at cyber-kriminalitet hadde forbigått narkotikakriminalitet som organiserte kriminelles foretrukne måte å tjene penger på. Når det gjelder bedrageri estimerer man globale tap på over 5 milliarder dollar årlig. Det er derfor helt naturlig at også organiserte kriminelle aktører i Norge er involvert i denne kriminalitetsformen.

Økokrim slapp i 2020 rapporten Kriminelle nettverk innen økonomisk-, arbeidslivs-, og miljøkriminalitet, hvor de er klare på at det ofte ikke er mulig å trekke et klart skille mellom de organiserte miljøene som driver med narkotika og de som driver med økonomisk kriminalitet. Dette stemmer med det politiet formidler om at de kriminelle nettverkene i Norge ofte er involvert i flere typer kriminalitet. Europol fastslår i rapporten The use of vio-lence by organised crime groups fra 2020 at internasjonale kriminelle grupperinger har en etablert tilstedeværelse i de landene de opererer. Dette dreier seg gjerne om lokale aktører som bistår med korrupsjon og trusler.

DNB har over tid sett en tydelig trend mot at organiserte kriminelle miljøer står bak hoveddelen av bedrageriene vi ser. Koblingene vi ser til grupperinger med en fysisk tilstedeværelse i Norge har aldri vært klarere enn i dag. Dette er gjerne grupperinger som er kjent for andre kriminalitetsformer enn økonomisk kriminalitet.

VOLD OG TRUSLER

Vold rettet mot personer utenfor de kriminelle miljøene fører til økt oppmerksomhet fra politi, som gjør det vanskeligere for de kriminelle å tjene penger og øker sjansen for at de blir tatt. De organiserte kriminelle miljøene har tidligere unngått dette fordi det ikke er lønnsomt.

Europol påpeker at de nå ser en endring i denne trenden og at voldsbruk og trusler mot personer utenfor de kriminelle miljøene øker. Europol ser denne trenden i sammenheng med mer tilgjengelige våpen og inntoget til en yngre generasjon uerfarne kriminelle som ikke er like opptatt av å holde sine handlinger skjult.

I Norge bekrefter Økokrim at det finnes koblinger mellom noen av grupperingene som er involvert i bedragerier og grupperinger med «kapasitet på vold og trusler». Både Danmark og Sverige rapporterer om en økt villighet blant kriminelle til å bruke dødelig vold for å oppnå sine mål.

Sammenlignet med noen av sine naboland har Norge hittil fremstått som relativt skjermet for en del av disse kriminelle metodene, særlig det som grenser opp mot næringslivet. En forklaring kan være at grupper med betydelig voldspotensiale i liten grad har vært involvert i bedragerier. En annen mulighet er at man har hatt mangelfullt innsyn i hvordan de kriminelle opererer.

Uavhengig av hvilken årsaksforklaring som best beskriver de faktiske forholdene ser DNB i dag en mye sterkere kobling til grupperinger med stort voldspotensiale. Vi har sett saker der aktører med tilknytning til ulike organiserte kriminelle grupperinger truer kundene våre, i noen tilfeller også med våpen. I de mest alvorlige tilfellene har kunder blitt utsatt for vold.

HVORDAN PÅVIRKER DEN GEOGRAFISKE PLASSERINGEN TRUSSELEN FRA ORGANISERTE KRIMINELLE?

Det er relevant å spørre om geografisk nærhet til organiserte kriminelle grupperinger har noen reelle konsekvenser når mye av kriminaliteten uansett skjer på nett. Det korte svaret er at geografisk nærhet gir mange fordeler for de kriminelle som er villige til å ta den ekstra risikoen. De kjenner språket, kulturen, menneskene og næringslivet. De vet hvordan politiet, rettsvesenet og bankene opererer. Ikke minst åpner geografisk nærhet for vold og trusler på en annen måte enn når man sitter mange tusen kilometer unna, så lenge man er villig til å ta i bruk slike virkemidler.

Organisert kriminalitet er en del av samfunnet og utvikler seg i takt med samfunnet. Bildet vi som samfunn har av organisert kriminalitet, hva de er involvert i og hvilke midler de bruker for å oppnå sine mål, er imidlertid overraskende utdatert. Gjennom egne kontrollmekanismer blir det tydelig at vi bør ta politiets advarsler om et økende voldspotensiale innenfor økonomisk kriminalitet på største alvor. For at vi skal kunne håndtere utfordringene det medfører er vi avhengig av en god forståelse av hvordan det fungerer og en god dialog på tvers av sektorer for å håndtere det på best mulig måte.

VOLD OG TRUSLER

Organiserte kriminelle miljøer eller multikriminelle nettverk bringer med seg vold og trusler til større grad enn det som tidligere har vært forbundet med økonomisk kriminalitet.

Overvåkning av data internasjonalt – trussel mot konfidensialitet i finansielle data?

Overvåkning, eller utnyttelse av store mengder datatrafikk, er noe som skjer hver dag og som vi hører om med ujevne mellomrom. Den vanligste formen er kontroll fra forskjellige lands myndigheter når data passerer landegrenser, men det er også andre aktører som på andre måter utnytter disse massive mengdene med data.

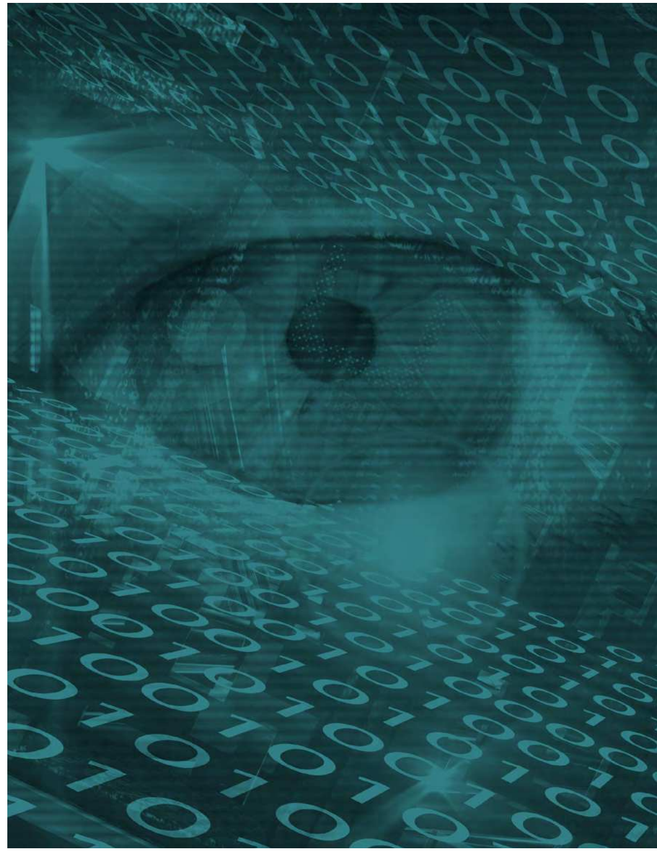
Mange tenker umiddelbart på personsensitive data som sier noe om hvem du er, hva du liker, hvor du er aktiv, hvem du kjenner, økonomien din og politisk ståsted. For våre kunder og ansatte er dette viktige data. Faren for at stater og private selskaper utnytter personsensitive data til overvåkning, danner ofte grunnlaget for diskusjoner om dataovervåkning. Det er imidlertid minst like interessant å se på forretningssensitive data, noe som i liten grad har vært i fokus i slike diskusjoner. Slike data utgjør en meget liten del av den datatrafikken en bank har, men kan være svært viktig. Brytes konfidensialitet til viktige forretningssensitive data, kan det i ytterste konsekvens føre til at forhold som er viktige for forretningskunder som f.eks. strategisk samarbeid, oppkjøp, sammenslåinger, konsesjonsrunder og andre lignende forhold feiler.

HVORDAN GJENNOMFØRES OVERVÅKNING AV INTERNASJONAL DATATRAFIKK OG HVEM GJØR DET?

Statlige aktører står for størstedelen av internasjonal dataovervåkning, selv om enkelte private aktører også samler store mengder data som kan utnyttes. Flertallet av land som gjennomfører kontroll med data i trafikk holder dette hemmelig. Det antas at mellom femti og hundre land i verden har overvåkning av datatrafikk i drift og at antallet er stigende.

Det er vanlig å plassere overvåkningssystemer i overgangene mellom nasjonale og internasjonale datalinjer og telekomleverandører pålegges ofte å hjelpe til med tilrettelegging. Systemene vil normalt dekke hele datastrømmen og trafikken speiles ut på egne servere. Herfra filtreres trafikken basert på spesielle attributter i dataene og hva det søkes etter. Både metadata og innhold i datatrafikken vil kunne brukes til filtreringen. Enkelte typer dekryptering vil ofte være en del av systemet.

Mange kommersielle aktører samler så mye data fra sosiale media, nettsøk, økonomiske tjenester, mailkommunikasjon o.l. at de fint kan brukes til overvåkning. Faren ved dette ligger ikke nødvendigvis i datainnsamlingen hos den første kommersielle aktøren. I 2018 ble det oppdaget at selskapet Cambridge Analytica før valget i USA i 2016 utnyttet data samlet fra 87 millioner Facebook-profiler til å etablere individuelle profiler for tilrettelagt politisk reklame. Et annet eksempel er da NRK i 2020 kjøpte en stor mengde app-posisjonsdata sammenstilt fra mange kilder. Gjennom videre sammenstilling, var de i stand til å identifisere personer i psykiatriske avdelinger, krisesentre og finne skjermet militært personell.



HVILKEN TRUSSEL REPRESENTERER DATA-OVERVÅKNING MOT KONFIDENSIALITET I FINANSIELLE DATA?

I de fleste demokratiske land er statlig overvåkning av datatrafikk regulert og begrenset til å avdekke trusler mot nasjonal sikkerhet. Personvernet havner under press ved dataovervåkning, men samtidig bidrar dataovervåkning til å beskytte samfunnet. Dataangrep identifiseres og terrorplaner stanses. Faren i vestlige demokratier er at man langsomt utvider overvåkningen og lar «nasjonale sikkerhetsinteresser» dekke industrielle og økonomiske interesser. Dette kan over tid representere en trussel mot viktige konfidensielle data i finansbransjen.

Mange ikke-demokratier er godt rustet til å overvåke datatrafikk, men mangler demokratienes kontrollmekanismer for å hindre uinnskrenket bruk. Trusselen mot konfidensialitet her er mer direkte i form av:

- Manglende skiller mellom «nasjonale sikkerhetsinteresser» og nasjonale eller private industrielle, teknologiske eller økonomiske interesser
- Svak eller ikke -eksisterende domstols- eller parlamentarisk kontroll over overvåkning
- Korrupsjon innen etterretnings- og sikkerhetstjenester, samt store IT-selskaper
- Få eller ingen begrensninger på registrering, lagring og deling av data for både offentlige og private aktører

Det er ikke bare mottakerlandet som bør vurderes, men også hvilke land dataene beveger seg gjennom langs internasjonale datalinjer. Brytes konfidensialitet i større mengder forretningssensitive data, kan det på sikt lede til en langsom umerkelig degradering av konkurransekraft for kunder og oss som bank.

KRYPTERING BESKYTTER?

Når datatrafikk speiles ut og behandles i systemer for overvåkning, er det mulig for tjenestene som driver overvåkningssystemene å kjøre dataene igjennom forskjellige systemer for dekryptering. Kryptering kan brytes ved å utnytte kjente svakheter i eksisterende standarder. Flere eldre krypteringsalgoritmer har svakheter som kan gjøre dekryptering mulig uten veldig høy ressursbruk. Det er nødvendig at krypteringsnøkler holdes konfidensielle for å sikre integriteten til et krypteringssystem. Nøklene kan bli kompromittert under overføring, for så å utnyttes til dekryptering. Avhengig av kompetanse er det også mulig for tjenestene å bryte kryptering gjennom massiv utregning. Dette er ressurskrevende, og det må prioriteres strengt i bruken av dette. Mange av disse tjenestene lagrer også data som kan dekryptere på et senere tidspunkt. I en rekke land slik som eksempelvis USA, England, India og Sverige så er tjenesten som utfører dataovervåkning også nasjonens kryptomyndighet, med sterk kompetanse på å kunne dekryptere informasjon.

USIKKERHET – VI KAN IKKE HA FULL OVERSIKT OVER TRUSSELEN

Hoveddelen av dataovervåkning holdes hemmelig. Vi er først og fremst avhengig av tillit til kontrollmekanismene. I vestlige demokratiske land med etablert legal- og/eller parlamentarisk kontroll er trusselen fra kompromittering og utnyttelse av våre data sannsynlig lav til meget lav. Utenfor denne sfæren vil trusselen mot konfidensialitet være høyere. For personsensitive data må vi leve med at det kun i noen meget sjeldne glimt kommer til overflaten hva som blir samlet inn og lagret. Under visse forhold kan forretningssensitive data ha betydelig interesse for dataovervåkere. Kompromittering kan lede til en langsom umerkelig degradering av konkurransekraft for kunder og oss som bank. På grunn av hemmeligholdet rundt dataovervåkning, blir det også en høy grad av usikkerhet om det reelle trusselnivået. Usikkerheten er spesielt høy når dataflyten går utenfor vestlige demokratiske land. Oversikt over hvilke land data utveksles med eller rutes gjennom, blir en viktig del av å vurdere trusselen.

DOMSTOLSKONTROLL

En domstol/særlovsdomstol godkjenner hvilke attributter det kan søkes etter i et system for dataovervåkning. Ikke en del av en etterforskning og krever ikke mistankegrunnlag mot et rettssubjekt.

PARLAMENTARISK KONTROLL

Et kontrollutvalg under parlamentet kontrollerer at regjeringens hemmelige tjenester holder seg innenfor mandat.

FORRETNINGSSENSITIVE DATA

Data som i seg selv, eller satt sammen med andre data, er strategisk viktig informasjon for forretningskunder og DNB.

Kryptering under angrep – kan vi stole på at våre data er sikre?

For å sikre at våre data holdes konfidensielle benytter vi oss av kryptering. Kryptering er å matematisk låse ned data med en nøkkel, som gjør dataene uleselig frem til nøkkelen brukes for å låse opp igjen.

KRYPTERING – EN FORUTSETNING FOR TILLIT

Bank- og finansinstitusjoners forretning er grunnleggende basert på tillit bygget opp over mange år. En av de viktigste komponentene i tilliten, er at vi kan behandle kundenes data på en trygg og sikker måte. I den senere tid har det vært stort fokus på etterlevelse, og spesielt GDPR har tatt mye tid og ressurser. Etterlevelse er viktig, og bøtene for å ikke overholde lover og regler kan være store. Samtidig er disse bøtene småpenger sammenliknet med tapene som følger dersom vi mister kundenes tillit. Blant de verste scenarioene er at lister av kredittkortdata, personnummer eller annen sensitiv informasjon blir lagt ut til salgs på Darkweb, eller at dokumenter fra en viktig handel fanges opp av konkurrenter, media eller andre uvedkommende. Svært mange trusselaktører kan ha betydelig interesse av data om bankens kunder.

Begrepet «Privacy by Design» oppsto på 70-tallet og tolkes oftest som å sikre data gjennom teknologisk design. To viktige begreper når man gjør et sikkert design, er data i bevegelse og data i ro. Det vil si at man setter søkelys på at data ikke skal være lesbart av uvedkommende når den er i bevegelse (overføres) eller i ro (lagret). For å sikre dette benytter man kryptering.

Moderne løsninger utvikles ofte under visjonen «zero-trust» (ikke stol på noen). Eldre løsninger er normalt ikke bygget for zero-trust. Dette innebærer at man ofte må bygge relativt komplekse sikkerhetsmekanismer og driftsrutiner som isolerer dem. Eldre interne nettverk er ofte designet i en tidsperiode med større tillit og utgjør en sekundær sårbarhetsdimensjon.

DARKWEB

Darkweb er en liten del av internet som bare kan nåes gjennom spesielle nettlesere. Opprinnelig ble det bygget for legitim sikker og anonym kommunikasjon, men er også tatt i bruk av kriminelle for anonymt salg og kjøp av illegale varer og tjenester.

ZERO-TRUST

Zero-Trust er et sikkerhetskonsept som går på at man ikke automatisk skal stole på noe eller noen som er på innsiden (eller utsiden) av våre grenser. Som eksempler på innsiden kan være på internt lokalt nettverk eller innenfor adgangssperrer på kontoret.

NØKKELLENGDE

Nøkkelen eller passordet til krypterte data kan være av forskjellige lengder. Jo lengre nøkkelen er, jo vanskeligere er det å bryte krypteringen. Nøkkellengden oppgis i bits.

DES

Tidlig på 1970 tallet etablerte IBM en gruppe som designet en krypteringsalgoritme «for å beskytte sine kunders data». I 1973 ble «the Data Encryption Standard» (DES) en standard i USA. DES har en nøkkellengde på 56 bits.

AES

Den nye krypteringsalgoritmen Advanced Encryption Standard (AES) ble foreslått av National Institute of Standards and Technologi i 2001 og etablert som en standard i USA i 2002. Algoritmen er en erstatning og forbedring av DES og støtter flere nøkkel-lengder. Normal nøkkellengde er 128 bits.

HVORDAN FUNGERER KRYPTERING?

Det finnes to hovedgrupper av kryptering, symmetrisk og asymmetrisk. I symmetrisk kryptering bruker man samme nøkkel for å låse og åpne data, i asymmetrisk benyttes et nøkkelpar som består av en privat og en offentlig nøkkel.

Begge gruppene har sine fordeler og ulemper. Symmetrisk kryptering er raskere og mer effektiv, men krever en felles nøkkel som må holdes hemmelig. Dette benyttes ofte for kryptering av store datamengder, for eksempel databaser. Asymmetrisk kryptering benyttes som oftest for dokumenter, men også for BankID (der banken passer på nøkkelparet) eller for etablering av sikker overføring i nettleser (HTTPS).

Kryptert trafikk mellom tjenesten og nett-leseren er nå normalen hvor over 85 % av alle nettsteder på internett er kryptert. Dette gir en økt sikkerhet for brukeren, og det forhindrer at en trusselaktør kan avlytte trafikk, plante falsk trafikk eller skadevare som en del av trafikken til nettleseren.

KAN KRYPTERING KNEKKES?

Kryptering er basert på matematikk, og baserer sin sikkerhet på at det tar svært lang tid å bryte algoritmen. Jo lengre nøkkel som benyttes i kryptering, jo lengre tid tar det å bryte den. I prinsippet finnes det ingen ubrekkelige algoritmer, bare man har nok tid. Etter hvert som datamaskiner har blitt kraftigere, har man sett at krypteringsalgoritmene blir utdaterte. Den første offisielle krypteringsalgoritmen DES ble etablert som standard i 1973. I 1997 ble det arrangert en konkurranse hvis mål var å vise at DES ikke burde benyttes lengre. Resultatene er representativ for utviklingen: Første gjennom-føring i 1997 brukte 140 dager å knekke en melding kryptert med DES, i 1998 brukte man 56 timer og i 1999 22 timer. DES ble trukket tilbake som standard i 2005 og er erstattet med AES.

Datamaskiner blir stadig kraftigere, og ny teknologi gjør at de eksisterende krypterings-algoritmene er under stadig angrep. Mens normale datamaskiner estimert vil bruke 13,7 milliarder år på å knekke en 128 bits lang AES nøkkel vil en kvantedatamaskin bruke 6 måneder.

Det pågår flere initiativer for å forbedre dagens algoritmer, blant annet i regi av organisasjonen NIST. I løpet av 3–5 år vil likevel krypterings-algoritmer som vi anser som trygge i dag sannsynligvis være knekket, enten på grunn av kvantemaskiner, tradisjonelle hurtigere maskiner eller forbedrede dataalgoritmer. Alle dagens krypteringsmekanismer kan bli lett å knekke med fremtidens teknologi, og det er utfordrende at eldre systemer ikke nødvendigvis støtter nyere krypteringsmekanismer. Derfor har en noen finansinstitusjoner etablert post-kvantum programmer, ikke nødvendigvis bare for å beskytte seg mot kvantemaskiner, men for å få etablert en aktiv forvaltning av bruk av kryptering. Det er ikke mulig å stoppe utviklingen. Vi må imidlertid posisjonere oss slik at vi har oversikt over og enkelt kan erstatte våre krypteringsalgoritmer når det er behov for det.

DATA UNDER BEHANDLING

Når et menneske eller en maskin skal lese eller behandle data kan de ikke være kryptert. I datasammenheng opererer vi med «Privacy by design», mens når mennesker skal behandle sensitiv informasjon må vi stole på sikkerhetsbevissthet, rutiner og verktøy som sikrer at data i form av skjermbilder, eposter, datafiler og utskrifter blir behandlet på en god måte.

KVANTEDATAMASKINER – KRYPTERINGENS DØD?

Mens dagens normale datamaskiner benytter det binære tallsystemet til sine kalkulasjoner og logiske operasjoner, benytter kvantedatamaskiner en kvantebit (qubit). En kvantebit kan være i en blandingstilstand av 0 og 1. Når så flere kvantebiter sammenfiltres (entanglement), er det mulig å utføre enkelte typer beregninger svært mye raskere enn hva tradisjonelle datamaskiner kan. Kvante-maskiner er spesielt flinke på faktorisering av store tall (som er basis for kryptering), noe som kan gi store sikkerhetsutfordringer i fremtiden. Den eksperimentelle kinesiske kvantedatamaskinen Jiuzhang løste i 2020 en kompleks beregning på 200 sekunder som dagens superdatamaskiner ville estimert bruke 2,5 milliarder år på å løse. Det er fremdeles usikkert når kvantedatamaskiner blir stabile nok til praktisk bruk, men forskningen pågår for fullt og det oppnås nye resultater fra måned til måned.

DNB