Trusselvurdering 2020

DNB

Årlig trusselvurdering 2020 er utarbeidet av Threat Intelligence Group (TIG).

Gruppen består av representanter fra Cyber Defense Center/IT SQR, Financial Cyber Crime Center/ Group Security og Security Governance/Group Security.

Trusselvurderingen behandler fem mer generelle tema, to korte innlegg og ni kategorier av mer spesifikke trusler mot DNB.

Rapporten tar sikte på å gi en bredest mulig vurdering av relevante trusler mot DNB ett til tre år frem i tid.

Ingrid Oskarsen (Cyber Defense Center) er ansvarlig for temaene innenfor digitale trusler. Sebastian Claydon Takle (Financial Cyber Crime Center) er ansvarlig for temaene innenfor økonomisk kriminalitet.

Thomas Grieg Sætren (Security Governance) er ansvarlig for geopolitiske forhold og fysiske trusler.

Layout ved Design Team.

Group Security koordinerer arbeidet og ansvarlig for utgivelsen er Lars Eirik Berg, Divisjonsdirektør.

Redaksjonen avsluttet 12. mars 2020

Trusselvurderingen er utarbeidet for internt bruk i DNB, men deles også utenfor DNB. Dokumentet kan inneholde enkelte faguttrykk og vendinger som er interne for DNB

Sikkerhet i et lederperspektiv

Daglig mottar vi et vell av informasjon som påvirker vår evne til å ta kloke valg og beslutninger. For å lykkes i omgivelser preget av hurtig teknologisk utvikling, komplekse trusler og omfattende krav fra samfunn og aktører, bør vi gjennomføre helhetlige operasjonsanalyser. Disse må forankres i ledelsen og i styret.

Vi må skaffe oss overblikk, på tvers av sektor, bransje og geografi. Vi må se bedriftens rolle fra ulike perspektiv, og vi må ivareta både bedrifts- og samfunnsansvaret. Ulike bedrifts-funksjoner må bringes sammen slik at alle opererer ut ifra ett felles situasjonsbilde.

«The purpose of business» eller «the business of purpose»? Hva er viktigst? Vi er alle en del av et samfunn og en samfunnskontrakt, både som enkeltmennesker og som organisasjoner. En virksomhet som ikke fyller sin del av samfunnskontrakten, vil neppe overleve i lengden. Det standpunktet uttales stadig mer kraftfullt av investorer, i styrerom og blant folk flest. Et ansvarlig næringsliv bidrar positivt til mennesker, samfunn og miljø som påvirkes av virksomheten. Verdiskapningen sikres ved å ha kunnskap om egne verdier, aktuelle trusler og egne sårbarheter, samt ved aktivt å forholde oss til risiko, og treffe risikoreduserende tiltak når det ansees nødvendig. Formelt er dette lederens ansvar, men skal man lykkes må alle utøve ansvaret.

Denne trusselvurderingen er et godt grunnlag for dem som vil sikre forbedret effekt ved å inkludere kunnskapsbaserte sikkerhetsvurderinger i sine analyser. Kompetansen finnes i banken eller hos bankens samarbeidspartnere. Den bør utnyttes til det beste for samfunnet, bankens kunder og eiere.

Odin Johannessen
Direktør, Næringslivets Sikkerhetsråd

Om årlig trusselvurdering

Hvilken sammenheng har egentlig disse gamle visdomsordene med moderne risikobaserte sikkerhet, og ikke minst våre Races 4 The Future?

For å planlegge for fremtiden så må man iblant se bakover, og det er nettopp over 2500 år tilbake i tid vi ser her, hvor den kinesiske militærstrategen og filosofen Sun Tzu viser oss at selv i gamle Kina hadde de god forståelse for risikobaserte tilnærminger.

Disse tre enkle setningene oppsummerer godt hvor viktig virksomhetstilpasset trusseletter-retning egentlig er. «Kjenner du din fiende», eller i vår sammenheng; kjenner vi til de kriminelles vilje og ikke minst evne til å kunne påføre DNB eller våre kunder skade eller tap, er det et veldig godt steg på veien for å kunne iverksette effektive sikkerhetstiltak der det gjelder mest.

Ser vi trusselbildet i kombinasjon med å «kjenne oss selv» – ved å ha god kontroll på våre verdier, samt sårbarhetene i sikkerheten rundt verdiene, så har vi klarlagt de tre viktigste faktorene «verdi, trussel og sårbarhet» for å fastsette vår reelle sikkerhetsrisiko. Godt sikkerhetsarbeid handler ikke nødvendigvis kun om å ha mest og best mulig sikkerhet, men det handler også vel så mye om å bruke de nødvendige ressurser på de riktige og mest kostnadseffektive tiltakene.

For å kunne vinne våre nåværende og kommende race så må også sikkerhetsarbeidet ikke bare fokuseres på å forhindre at vi kjører i grøfta, men i minst like stor grad skal god og naturlig integrert sikkerhet gjøre at vi kan kjøre raskest mulig, innenfor det som er akseptable risiko- og lovmessige rammer. Åpenhet og positivitet rundt sikkerhet vil også styrke vårt omdømme og tillitt i samfunnet, og dermed være med på å skaffe flere sponsorer til våre race, både i form av gode samarbeidspartnere og ikke minst flere kunder. M.a.o, sikkerhet skal være et av våre konkurransefortrinn.

Det å «kjenne vår fiende» er derfor like viktig som det å «kjenne oss selv», så vi håper denne rapporten kan være et av mange bidrag fra sikkerhetsmiljøene som skal støtte oppunder at vi vinner våre Race 4 The Future!

Lars Eirik Berg
Divisjonsdirektør Group Security, DNB

Sun Tzu, en av de første strategiske tenkere, levde i Kina (544–496 f.kr).

If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle.

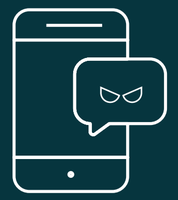
– Sun Tzu

Nøkkelfakta

Med lekkasjene
som rapporteres rundt oss, er det bare et spørsmål om tid før hver enkelt av oss blir berørt

Fra «on prem» til **hybrid løsning**

Bank under **geopolitisk** konkurranse



Halvparten av truslene
mot ansatte kommer pr. telefon

Løsepengevirus
gir kostbare erfaringer

Sosiale media, telefon
– alt kan benyttes for å komme til informasjon

1,2 mrd
forsøkt bedratt fra våre kunder og DNB

Når bankranerene
later som de er Finanstilsynet

Terrorisme og politisk vold

Over 4000 bedragerisaker

Begrenset antall ran
i Norge

Avansert **dataangrep**

AI

– Trussel eller gimmick?

Trusselaktører samarbeider
for å utnytte hverandres kompetanse

Biometridata
– mer verdt enn penger?

Investeringsbedrageri og kjærlighets-bedrageri

En middelsstor bank i en verden av geopolitisk konkurranse

Fra siste års beskrivelse av fremvekst av autoritært lederskap og en uforutsigbar, delvis dysfunksjonell verdensorden, hvordan ser den globale strukturen ut mer konkret? Ut av dette, kan vi trekke av konklusjoner for DNBs virksomhet?

Geopolitisk er det aller tydeligste trekket at verdens to største makter, USA og Kina, er inne i en gigantisk kamp om det økonomiske herredømmet. Motsetningsforholdet har tydelige ideologiske og sikkerhetspolitiske undertoner, med viktige innenrikspolitiske forhold bak. Med en metafor ser det nå ut som de to statene er låst fast i en langdryg global brytekamp.

Det Kinesiske kommunistpartiet, som eneherskende i Kina, bygger sitt grep om makten på den suksessen det har hatt i å bringe økonomisk utvikling. Sammenhengen mellom økonomisk utvikling og makt medfører at behovet for økonomisk utvikling trumfer de aller fleste andre utviklingsmål. Naturressurser, energi, handelsveier og teknologisk kunnskap blir avgjørende tilganger for videre utvikling.

Kina er også et stort rike og alt som truer Kinas enhet eller Kommunistpartiets enhetlige kontroll blir sett på som truende. Beskyttelse mot separatisme rettferdiggjør sterke virkemidler internt og eksternt. Det er i dette Kinas sterke reaksjon, tidligere mot Norge, og nå mot Sverige ligger.

I USA var det stort sett enighet om hovedtrekk i utenrikspolitikken, mens uenighet i stor grad ble reservert til innenrikspolitikken. Nå er dette endret. I Washington er all utenrikspolitikk først og fremst blitt til et innenrikspolitisk spørsmål. Trump er president for USA og hva som skjer med verden utover USAs interesser har lav prioritet. Kun et skifte av administrasjon vil endre dette. Ved siden av fokuset mot Kina, så endrer også tvekampen prioriteringer i forholdet mellom sikkerhetspolitikk og handelspolitikk. Tidligere fikk sikkerhetspolitikk være sikkerhetspolitikk og handelen fikk gå mest mulig fritt. Nå er dette forholdet endret. Gjeldende nå er at hvem du handler med internasjonalt de facto også er sikkerhetspolitikk.

EU er nå preget av nettopp alt annet enn å være en sammenføyning, en union. EU preges av avskalling, indre uenighet og en stans i integrasjonen. Håpet fra 10–15 år tilbake om EU som en leverandør av overnasjonal sikkerhet har aldri materialisert seg. Det er stor usikkerhet om EUs videre kurs.

Samtidig er det tidligere transatlantiske sikkerhetssamarbeid i transformasjon. ▶

Tidligere Østblokkland ivrer for samarbeidet med USA, mens Tyskland holder tilbake. USA kritiserer sine allierte for ikke å gjøre nok og et Frankrike, som etter lenge å ha marsjert sammen med de andre, på ny har inngitt seg på marsj i egen retning. Den franske presidenten Macron uttrykte nylig i frustrasjon over tilstanden til det transatlantiske sikkerhets-samarbeidet at det var «hjernedødt». For de mindre europeiske landene er summen en økt grad av usikkerhet. I søken etter sikkerhets-løsninger i et turbulent geopolitisk landskap lener de seg på det transatlantiske samarbeidet fremfor det intra-europeiske. Det er ingen umiddelbare utsikter til at dette vil endre seg.

Det russisk-europeiske forholdet ligger igjen på et bunnivå. Russland, hvis maktbase ikke ligger i landets økonomi, men i landets geografiske størrelse og sterke militærmakt, har gjennom de siste årene hatt suksess med å bruke makt der de ser det formålstjenlig. De europeiske landene har forsøkt å stå imot, men i liten grad lykkes. EUs taushet i et viktig spørsmål som Ukraina eksemplifiserer unionens manglende evne. Initiativet i de russisk-europeiske relasjonen har ligget hos Russland som har kunnet hjelpe til å skape splid, skremme og skape usikkerhet innad i Europa. Foreløpig ser Russland ut til å beholde et ganske stort spillerom overfor Europa.

I Washington forstås Russland som en av de store globale spillerne. Med fokus på Kina sees det ikke som strategisk hensiktsmessig å konfrontere Russland i Øst-Europa, i hvert fall ikke nå. Problemet med Russlands bruk av trusler og makt mot Europa sees primært som noe de europeiske medlemmene i det transatlantiske samarbeidet bør kontre.

I den europeisk-russiske relasjonen ser vi også forskjeller i forståelsen mellom handels-politikk vs. sikkerhetspolitikk. I tysk perspektiv så er disse adskilt og det legges til rette for økte leveranser av energi fra Russland, noe Washington har tydelig kritisert. Fra Russisk side er det ingen tvil, Putins regjeringsapparat er helt avhengig av inntektene fra olje og gass. Utviklingen i globale og regionale markeder for olje og gass er tett koblet sammen med sikkerhetsinteresser.

Relasjonen Kina-India, mellom verdens to mest folkerike stater, begge atommakter, er ofte oversett fra Nord-Europa. Relasjonen handler om kontroll over naturressurser og handelsveier nødvendige for videre økonomisk utvikling og politisk dominans over Sørøst-Asia. Strategisk usikkerhet overfor motparten og frykt for indre uro preger også relasjonen.

India har under statsminister Modi hatt betydelig økonomisk vekst. Medaljens bakside har vært Modis hindu-nasjonalistiske politikk, med økt spenning internt mellom folke- og religiøse grupper. Nå i 2020 har det vært voldelige demonstrasjoner en lang rekke steder mot ny lovgiving som berører rett til statsborgerskap. Hindi-dominansen over indisk politikk er så stor at selve det politiske systemet neppe vil rokkes, men begrensede uroligheter omkring borgerrettigheter, religiøs- og kulturell identitet må ventes å pågå i hvert fall gjennom 2020.

Utenrikspolitisk har India løst sine sikkerhets-utfordringer, først og fremst overfor Kina, med en tydelig tilnærming til USA. Senest tydeliggjort under Modis strålende mottakelse under President Trump statsbesøk til India. Når India må forholde seg til konfrontasjonen mellom USA og Kina må India ventes å lene seg ytterligere mot USA. Indisk-Kinesiske relasjoner må forventes å bli anstrengt, preget av både konkurranse, mistenksomhet og usikkerhet.

Hva som skjer i det som tegner til å bli et jevnt amerikansk presidentvalg er en av jokerne i kortstokken. Demokratene samles om Jo Biden, og han kan ha en mulighet til å vinne over den sittende presidenten. Skjer det, så vil Washington sannsynlig styrke de transatlantiske forbindelsene og Russland holdes sterkere tilbake. Likevel, kampen overfor Kina om økonomisk innflytelse har så streke drivere at virkemidlene kan endres, men motsetningen vil bestå. ▶

Konkurransen om tilgangen til informasjon på tvers av de geopolitiske skillelinjene vil medføre at digitalt baserte operasjoner for å skaffe informasjon vil fortsette med minst samme intensitet.

Det digitale rom vil også være den viktigeste arenaen for å påvirke. Kina har kommet meget langt med sine digitale systemer for skjerming av befolkningen mot påvirkning utenfra. Russland har hatt en viss suksess med sine operasjoner for å påvirke og skape splid. De demokratiske landene med sine åpne tilganger vil fortsette å forbli mer sårbare for påvirkning. Iran og Nord-Korea som to isolerte stater satt utenfor den globale verdensarenaen, kan utnytte den digitale sfæren for å øve press imot og skaffe seg oppmerksomhet til sin sak. Særlig hvilken vei et sanksjonstynget Iran nå går er usikkert.

HVA BETYR DETTE FOR DNB

Som en norsk bank vil vi oppfattes internasjonalt å komme fra et land som er godt etablert innenfor det transatlantiske sikkerhetssamarbeidet.

Beskyttelsen vi finner internasjonalt, ved at vi kommer fra et lite nordeuropeisk land, vil mulig bli svakere. Sikkerhetssamarbeidet i Europa f.eks. innenfor det digitale området vil gå videre, men uten sterke politiske drivere bak. I Norge vektlegges handel i stor grad som separert fra sikkerhetspolitikk. Med en kundeportefølje innenfor olje og gas, maritim næring og råvareeksport, så vil vi og våre kunder, spesielt fra kinesiske og russisk side, forstås som nærmere knyttet til sikkerhetsinteresser enn hva vi selv er vant med.

Washington har ikke lenger frihandel som mantra. Fortsetter handelskrigen med Kina å trekke i langdrag, vil hvem man handler med komme under økt oppmerksomhet. Imidlertid hvis dette skjer, forventes USA å begrense seg til diplomatiske press overfor Norge. Dette kan dermed få virkning for norske selskaper.

Ved Covid-19s plutselige inntreden har avbrudd i produksjon, leveranselinjer og reising ført til en rask og kraftig økonomisk oppbremsing. Saudi Arabias nylige prisdumping i kampen om hegemoniet i oljemarkedet har samtidig sendt oljeprisen til bunns. Gitt behovet for økonomisk utvikling i Kina og Russlands avhengighet av en høy oljepris, så vil ledelsesapparatet i disse landene ha ytterligere behov for å skaffe seg informasjon. DNB operer med og har relasjoner til kunder som for disse stormaktene er av interesse. Det mest nærliggende middelet for å skaffe denne informasjonen er gjennom videreføring og mulig forsterkning av de cyberoperasjonen de fører. Andre virkemidler for å nå denne typen informasjon kan også bli tatt i bruk.

Nord-Korea kan som følge av fortsatt økonomisk press gjennomføre digitalt baserte operasjoner med hensikt å skade. Dette i tillegg til de operasjonen de allerede har for å tilegne seg penger. Det foreligger en viss mulighet for at et presset Iran vil bruke det digitale rom for skadelige kampanjer. ■

Fra «on prem» til hybrid løsning

Tiden hvor DNB eide og driftet hele den digitale infrastrukturen selv er over. De siste årene har vi beveget oss fra IT «on premise» (altså systemer som vi eier og drifter selv) til en hybrid løsning med bruk av nye skytjenester som en del av våre verdikjeder. Fordelene er mange: Det blir enklere for DNB å skalere infrastrukturen, vi kvitter oss med gammel teknisk gjeld, kostnader vil gå ned på sikt og man får også andre, moderne muligheter når det kommer til sikkerhet. Samtidig er mye av den nye teknologien ung og uprøvd, og det er vanskelig å få tak i nok personell med kompetanse på de nye løsningene.

Det tradisjonelle infrastrukturkonseptet med en sterk ytre mur eller perimeter utfordres av at flere tjenester tas ut av våre egne datahaller og legges i skyene. Sikkerhetsprinsippene som ligger til grunn i den gamle løsningen er ikke nødvendigvis kompatible med de nye.

For våre «on premise»-systemer har vi benyttet et sikkerhetsprinsipp populært kalt dybde-forsvar eller «løkmodell» (se for deg lagene i en løk). Tanken er at man har flere lag med sikkerhetsmekanismer som hver for seg bidrar til den totale sikkerheten, og dersom et av lagene feiler så vil neste lag likevel kunne hindre sikkerhetsbrudd. Ved overgang til sky-tjenester så reduseres dette perimeteret og tidligere kjente forsvarssystemer erstattes med nye og mer uprøvde forsvarsmekanismer. En enkelt konfigurasjonsendring kan dermed få alvorlige konsekvenser.

Ved å sette bort tjenester til eksterne leverandører gir man også bort kontroll. I vår egen infrastruktur kan vi plassere ut og kontrollere egne sikkerhetsmekanismer, men dette tilbys ikke nødvendigvis fra våre leverandører. Det vil si at vi potensielt kan miste innsyn i våre egne data, og må stole på at leverandørene gjør en like god jobb som DNB selv ville gjort. I tillegg blir vi «en av mange» for våre leverandører, mens vi tidligere hadde ansvar for oss selv. ▶

Tradisjonelt dybdeforsvar til venstre, blandet sammen med skybaserte tjenester utgjør en Hybrid løsning

På den positive siden finnes det flere eksempler på at bedrifter som har blitt utsatt for dataangrep rett og slett blitt reddet fra en fullstendig kompromittering ved at de har benyttet en hybrid modell. Det har hindret trusselaktørene å bevege seg fra det ene nettverket til det andre. Men vi vet at IT-sikkerhet er en katt- og mus-lek, og at kriminelle vil bevege seg i takt med utviklingen. Et av verdens største IT-sikkerhetsselskaper, FireEye, skriver følgende i sin årlige trendrapport: «Samlet sett fortsetter vi å se at flere kunder tar i bruk en hybrid løsning for sin digitale infrastruktur ved å blande «on prem»-løsninger med sky-arkitektur eller -tjenester. Samtidig observerer vi at angripere blir mer komfortable med å jobbe i slike hybridmiljøer for å nå sine mål.»

For oss i DNB betyr dette at vi fortsatt må tenke sikkerhet selv om vi plasserer infrastrukturen vår hos leverandører, bare på en annen måte enn tidligere. ■

Slik gjennomføres et avansert dataangrep

Trusselaktøren velger seg ut mål basert på hva de ønsker å oppnå. Dette kan være spionasje eller informasjonstyveri for å oppnå en fordel i forhandlinger eller bruke denne informasjonen som beslutningsgrunnlag.

Så starter trusselaktøren å kartlegge sitt mål. Hvordan ser deres digitale infrastruktur ut? Hvem jobber med hva, og hvilken e-postadresse bruker de? Hvordan ser organisasjons-strukturen ut? Noe av denne kartleggingen foregår på et teknisk nivå, mens annen informasjon er lett tilgjengelig på internett.

Basert på denne kartleggingen velger trusselaktøren verktøy for å trenge inn i nettverket. Dette er en teknisk krevende oppgave. Det er ikke usannsynlig at en trusselaktør må bruke så mye som 6 måneder for å utvikle verktøy som fungerer. Hvis aktøren ikke har denne kompetansen selv, kan det være et alternativ å kjøpe verktøy av andre hackergrupper, for eksempel på det mørke nettet.

Når aktøren har valgt verktøy, starter selve inntrengningen i nettverket. Her må trusselaktøren utnytte en sårbarhet for å komme seg inn. Denne sårbarheten kan bestå av tekniske løsninger, eller trusselaktøren kan bruke sosial manipulasjon, eller en kombinasjon av begge. For eksempel ved å tilpasse en e-post med tematikk som er relevant for mottaker, og legge ved et vedlegg eller lenke til en side som inneholder skadelig kode. En annen metode er å utnytte sårbar, internetteksponert infrastruktur som ikke har de nyeste sikkerhetsoppdateringene. Hensikten er å få plassert ut en bakdør som gjør at trusselaktøren kan logge seg inn i nettverket og oppnå samme typen tilgang som en som har fått det tildelt på legitim måte. De aller fleste dataangrep blir oppdaget i denne fasen. Enten ved hjelp av automatiske sikkerhetsmekanismer eller ved skreddersydd sikkerhetsmonitorering. I DNB er det Cyber Defense Center (CDC) som har ansvaret for sikkerhetsmonitorering.

Neste fase kalles gjerne «kommando og kontroll»-fasen. Det er her trusselaktøren har fått tilgang inn i nettverket, og arbeidet med å plassere ut verktøy, skaffe seg riktige tilganger osv. Hvis trusselaktøren fortsatt får jobbe uhindret, starter arbeidet med å oppnå sluttmålet. Det kan være å hente ut dokumenter, logge tastetrykkene til ansatte, se på skjermene deres, legge inn falske SWIFT-betalinger eller plassere ut løsepengevirus.

Det er ikke alltid at en trusselaktør lykkes med sitt angrep, og da starter gjerne prosessen med å forbedre seg og utvikle seg for å oppnå sine mål. Derfor har de mest avanserte aktørene lang tidshorisont for sine operasjoner.

Det globale internetts utvikling inn i 2020
I årlig trusselvurdering for 2019 skrev vi om at det globale internett var i ferd med å deles opp i flere større segmenter. Hvert av segmentene blir skilt ved at de større statene setter inn tekniske kontroller for å kontrollere trafikk inn/ut av landet og etablere egne regler for forvaltning av informasjon innenfor sitt område.

Kina har lenge operert et system for kontroll med kinesiske borgeres digitale kommunikasjon inn/ ut av Kina. Populært har dette systemet vært kalt «The Great Firewall of China», selv om formålet har ligget langt fra å sperre ute skadevare fra det kinesiske segmentet av internett. Kina har også fulgt opp med lovgiving som effektivt forbyr krypteringsløsninger inn/ut av landet, nettopp for at det ikke skal være mulig å omgå «The Great Firewall of China» og andre overvåkningsløsninger som eventuelt måtte ligge i den kinesiske delen av internett.

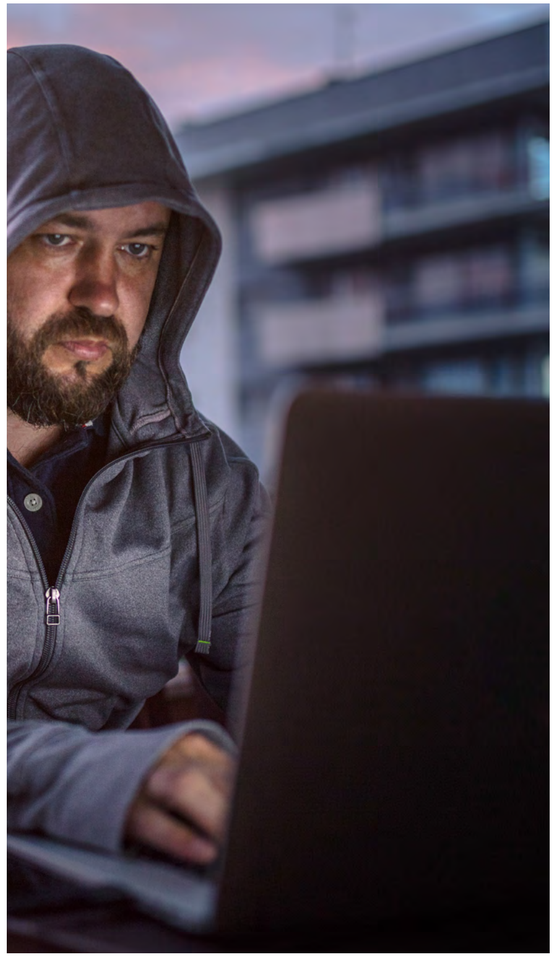
Ved siden av utviklingen i Kina så pekte vi på en utvikling hvor Russland tidlig i 2019 innførte lovkrav om at det russiske internett segmentet (RUNET) i tilfelle krise skulle kunne kobles fra det globale internett og kunne driftes som en separat enhet. Forutsetninger for å få til dette er at det er et begrenset antall linjer som går internasjonalt, og at det ligger et system som effektivt kan styre trafikk i disse linjene på/av.

1. november 2019 trådde den nye loven om separat drift av RUNET i kraft. 24. desember 2019 meldte det russiske kommunikasjonsdepartementet at det hadde gjennomførte en vellykket test med frakopling av RUNET fra resten av det globale internett.

Loven hadde også en del med pålegg til internettleverandører om å legge til rette for «Deep packet Inspection», dvs. undersøkelse av innholdet i meldingstrafikken. Dette er imidlertid bare bekreftelse på etablert praksis. Russland rullet ut sitt første system for internett trafikkovervåkning, SORM generasjon 1, i 1998 og har nå etablert tredje generasjonen av SORM.

Store databasetyveri

Med lekkasjene som rapporteres rundt oss, er det bare et spørsmål om tid før hver enkelt av oss blir berørt.



I løpet av det siste året ble DNB kjent med at flere store dumper med lekkede opplysninger ble lagt ut på internett. I november 2019 ble en samling av 1,2 milliarder linjer med personlig informasjon funnet på en usikret server på internett. Blant disse opplysningene var det 5673 DNB-e-poster. Dette er den nye normalen og viser hvor viktig det er å ikke bruke samme passord på flere tjenester. Det er ikke lenger «hvis» passordet ditt blir lekket, det er «når».

Om passordet ditt er lekket fra en tjeneste vil en trusselaktør ofte forsøke dette passordet på andre tjenester. For eksempel hvis du bruker samme passord på nettsidene til det lokale idrettslaget og på Facebook, bør du håpe at idrettslaget har god IT-sikkerhet. Hva hvis passordet ditt lekkes derfra, og noen kan forsøke det samme på Facebook?

Noe vi har sett mye av det siste året hos DNB er at svindlere sender ut e-poster hvor de påstår at de har hacket mottakerens webkamera og tatt opp at de har sett på porno. For å tillegge legitimitet til trusselen, legger de ofte ved et passord som du har benyttet. Og dette kommer gjerne fra store database-tyverier.

Avhengig av hvor informasjon blir lekket fra, kan ulik type informasjon komme på avveie. Personnummer, kortdetaljer, brukernavn og passord er informasjon som åpenbart kan brukes av kriminelle for å gjennomføre målrettede bedragerier. Noen av disse bedrageriene er lite annet enn bakgrunnsstøy for store finans-institusjoner eller privatpersoner. Ingen merker noe spesielt til at noen belaster kortet ditt på et annet kontinent. Beløpet blir refundert, kortet erstattet, saken avsluttet. Det store maskineriet som går i bakgrunnen for å håndtere disse sakene er stillegående og lite forstyrrende.

Andre bedragerier har konsekvenser som kan følge enkeltpersoner i flere år. ID-tyveri kan føre til at noen forsøker å tømme en bankkonto. Dette er ganske konkret, oppdages som regel raskt og blir tatt hånd om. Men kriminelle kan også ta opp utallige forbrukslån i andres navn. De kan bruke stjålne identiteter til å opprette selskaper i utlandet. Ofte brukes de selskapene videre til å hvitvaske penger eller bedra andre.

I tillegg til informasjonen som kan brukes direkte er det masse informasjon om oss som kan brukes til å bygge tillitt. Hvilket spill du spiller, hva du har sett på Netflix i det siste eller hvilket resepter som snart skal fornyes: alt dette er informasjon som misbrukes i et forsøk på å manipulere oss, og det fungerer overraskende bra. Vi responderer på at den vi kommuniserer med faktisk vet noe om oss.

Med lekkasjene som rapporteres rundt oss, er det bare et spørsmål om tid før hver enkelt av oss blir berørt. På grunn av måten de fleste av oss opererer med samme passord flere steder og tillit til korrespondanser som virker å kjenne oss, eller personlig informasjon om oss, er dette dømt til å få alvorlige konsekvenser for enkeltpersoner. Det er ikke et realistisk alternativ å hindre alle disse lekkasjene. Vi må endre våre vaner, både når det gjelder hvordan vi sikrer oss, og når det gjelder hva som skal til for at vi har tillit til den vi kommuniserer med.

Artificial Intelligence (AI)-generert innhold – trussel eller gimmick?

AI-generert innhold har revolusjonert skreddersydd reklame, det kan være alt fra tekst og bilder til lydfiler eller videoer. Fellesnevneren er at innholdet produseres fra start til slutt av maskiner, ikke mennesker. Diskusjonene rundt temaet handler som regel om hvor vanskelig det har blitt å se forskjell på menneskeskapt og maskinskapt innhold. Realiteten er at det ofte ikke er sannsynlig at man vil se forskjell.

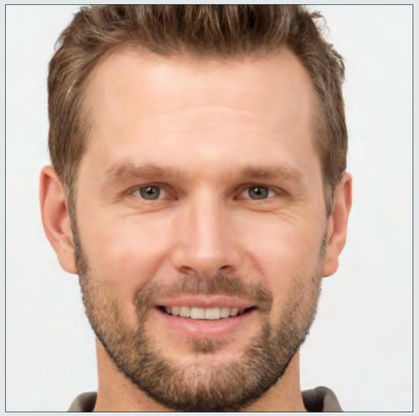
Noen ganger er dette spennende, morsomt og underholdende – som da vi fikk en personlig hilsen fra vår nye Konsernsjef Kjerstin Braathen. Andre ganger kan det by på utfordringer, nettopp fordi du ikke fikk en personlig hilsen fra Kjerstin, men fra noen som vil ha deg til å tro det for å lure deg for informasjon eller penger.

Det er to hovedmomenter som skaper sikkerhetsutfordringer. Det første går på evnen til å «skape» helt nye identiteter og dermed virke åpen samtidig som man skjuler sin egen identitet. Det andre er AI sin evne til å utgi seg for å være en konkret person. Videoklipp, bilder eller lydopptak kan nå brukes på en helt annen måte enn tidligere.

AI-GENERERT TEKST

AI-generert tekst har kommet langt. På nettsider som for eksempel «talktotransformer.com» kan man starte å skrive og maskinen tar over og begynner å generere tekst. Den kopierer ikke tekst den finner på internett, den «skaper» ny tekst med originale meninger og falske sitater fra mennesker som ikke finnes.

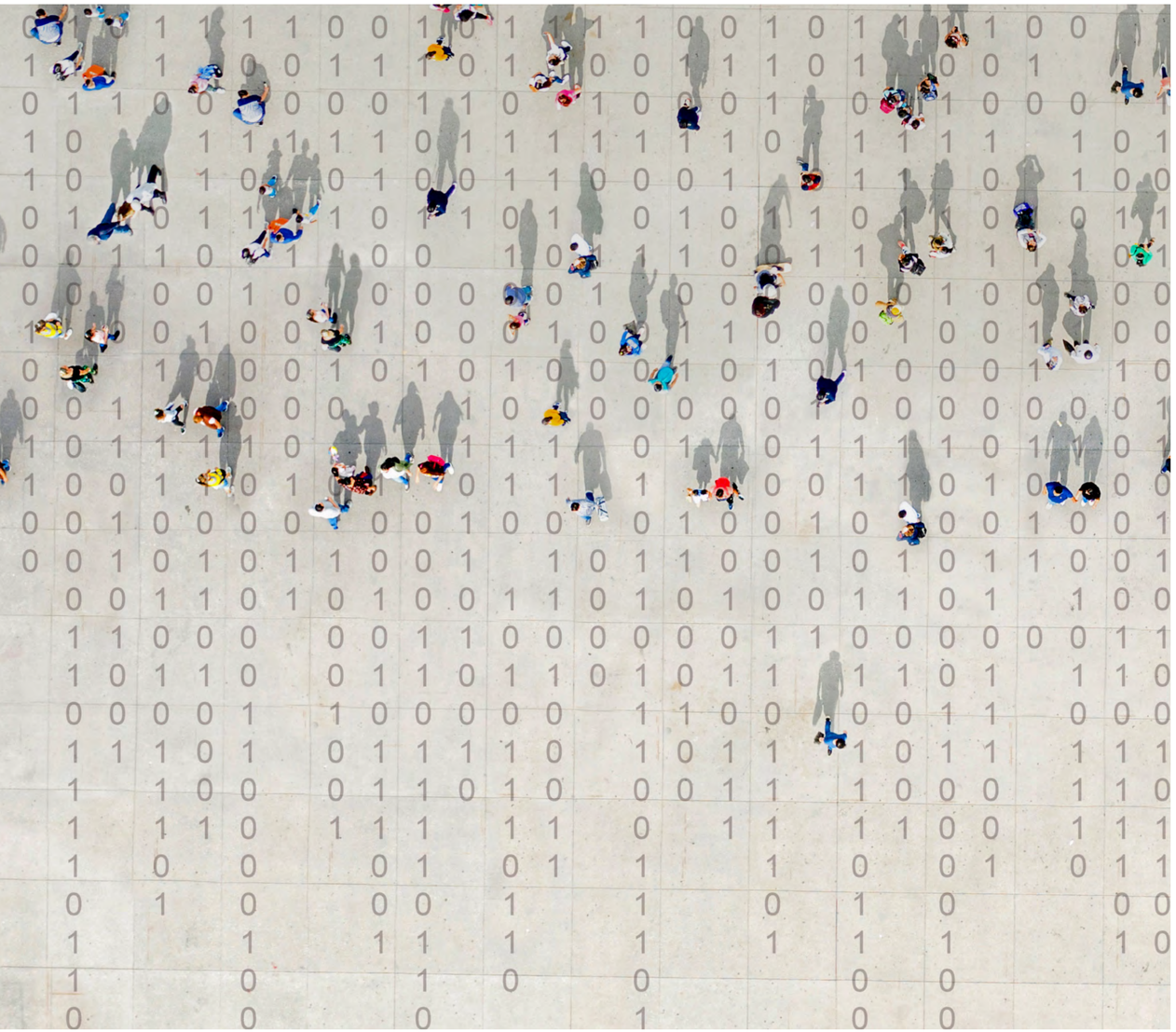
«Evnen menneskeskapt AI har til å bedra mennesker er ikke begrenset til urettmessige finansielle transaksjoner eller trusler mot vårt privatliv. Et AI-program kan generere falsk medisinsk dokumentasjon og kredittvurderinger, utgi seg for å være en lege eller jurist og brukes for å gjennomføre bedragerier[1].»



[1] Talk to transformer

Sitatet til venstre tar opp noen gode poenger og har egentlig funnet essensen i spørsmålet om AI generert tekst. Problemet er bare at det ikke er et sitat. Det er resultatet av talktotransformer ble stilt følgende spørsmål: «Kan AI-generert innhold brukes til bedragerier?». Referansen viser til en person som ikke finnes.

AI-generert tekst brukes i dag til å gjennomføre sosial manipulasjon. I saker hvor noen tidligere måtte dedikere menneskelige ressurser for å manipulere noen kan dette nå gjøres ved hjelp av AI-generert tekst. Dette betyr at man kan gjennomføre skreddersydd manipulasjon mot tusenvis av mennesker samtidig. ▶



AI-GENERERT LYD

Programmer som «Lyrebird» kan kopiere en stemme og AI kan bruke stemmen til å si hva som helst. Det finnes allerede eksempler på at mennesker har gjennomført transaksjoner på bakgrunn av telefonsamtaler med «sjefen», hvor det slett ikke har vært sjefen de har snakket med.

AI-GENERERT BILDE OG VIDEO

Bildet som følger med sitatet på forrige side er ikke ekte. Personen finnes ikke. Den ble generert av AI på nettsiden www.generated.photos etter at alder, kjønn osv. ble definert. Det har blitt lett å skjule sin egen identitet ved å generere en falsk identitet. Det samme kan gjøres med video, men det som skaper mer oppmerksomhet er evnen til å ta et bilde eller en video av en ekte person og bruke den informasjonen til å generere helt nye bilder og videoer av den personen, såkalte «Deep Fakes». Frem til nå har det største bruksområde til denne teknologien vært innenfor pornografi hvor kjendiser «klippes inn» i scener de ikke har deltatt i, men det finnes ingen grense for hvilke situasjoner man kan «klippe inn» mennesker i. Potensialet for misbruk er stort.

SOSIAL MANIPULASJON ELLER AI-GENERERT INNHOLD

Teknologi som kan brukes for å skjule ens egen identitet, eller i verste fall på en troverdig måte utgi seg for å være noen andre, kan utgjøre en trussel. Bedragere kan benytte dette for å manipulere tusenvis av kunder samtidig. Skadepotensialet internt i konsernet er åpenbart tilstede når den du snakker med på telefonen kanskje ikke er den du tror det er.

Det er likevel viktig å huske på at muligheten til å generere innhold er et verktøy. Et verktøy som kan tas i bruk av aktører som allerede i dag utgjør en trussel mot konsernet og våre kunder. Det er ikke noe nytt at trusselaktører skjuler sin identitet for å skaffe tilgang til vår informasjon eller våre systemer eller for å bedra banken og våre kunder. Dette skjer daglig. Når de tar i bruk nye verktøy for å gjennomføre disse angrepene blir det mer sannsynlig at de vil lykkes. Det mest allsidige verktøyet de har er den grunnleggende sosiale manipulasjonen de gjennomfører hver eneste dag. Den har de perfeksjonert og den virker å være tidløs. Den handler som regel mer om våre personlige sårbarheter enn ny og spennende teknologi.

Faren er at de kriminelles utnyttelse av nye verktøy og ny teknologi vil føre til mer troverdig manipulasjon slik at flere ansatte og kunder, også de som normalt er aktsomme, kan bli lurt. ■

Biometriske data

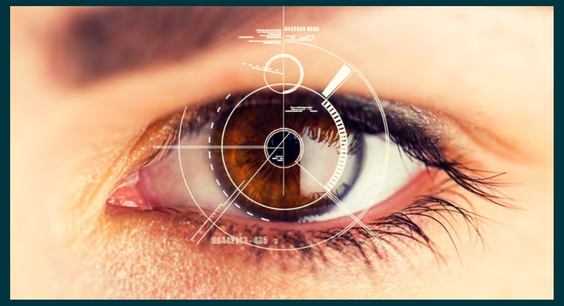
Biometriske data har stor verdi for finans-institusjoner, deg og meg – og trusselaktører.

Biometriske data har blitt brukt for å identifisere mennesker i mange, mange år; høyde, hårfarge, øyenfarge, kroppsfasong, og i mer moderne tid, systematiske bruk av fingeravtrykk, dette er så velkjent for oss at vi sjelden tenker over det.

Moderne teknologi gir muligheter for å registrere og lagre mye mer detaljerte biometriske data, helt ned på individ nivå, samt å analysere enorme datasett for å identifisere en spesifikk person. I dag er det mulig å registrere detaljerte biometriske data som er unike for individet og dermed svært vanskelig å manipulere. Eksempler på dette er fingeravtrykksmønster, tanndata, stemmemønster, irismønster, data om ansikts-struktur/hodeform, data om skjelettstruktur, DNA m.m. Dette kalles ofte for «enhanced biometrics», avanserte biometriske data.

Enkelte typer avanserte biometriske data er også mulig å samle inn på avstand. Et eksempel på dette er ansiktsstruktur fanget opp med kamera. Teknisk er det mulig å samle inn enkelte typer biometriske data om deg uten at du merker det.

For deg og meg representerer manglende kontroll med våre biometriske data et stort potensial for tap. Taper du dine kredittkortdata så lider du og/eller banken et økonomisk tap. Du kan likevel ganske raskt få deg et nytt kort og dermed gjøre de tapte kortdataene verdiløse for andre. Hvis dine avanserte biometriske



data går tapt og du f.eks. taper kontrollen med datasett med din spesifikke ansiktsstruktur eller irismønster så er dette ikke like lett å endre som å sperre/bytte et kredittkort. Avanserte biometriske date er direkte knytte til deg og din identitet.

For forskjellige trusselaktører har avanserte biometriske data en verdi. Det gjør det mulig å gjennomføre bedragerier, mot deg, eller ved å bruke din identitet overfor andre. En annen aspekt er at biometriske data kan brukes for å holde deg under oppsikt. Så langt så er det undertrykte befolkninger i diktaturer som har fått merke dette mest.

Teknologisk utvikling gjør det nå mulig å samle avanserte biometriske data i store registre. Det er høyest sannsynlig at forskjellige finans-institusjoner, som f.eks. DNB, i årene fremover kommer til å forvalte datasett med avanserte biometriske data. Datalagre av denne typen vil kunne ha stor verdi for trusselaktører, sannsynlig minst like høy eller høyere verdi enn dagens lagre med kredittkortinformasjon.

Moderne bankran

Det begås svært få fysiske bankran i dag, men i det digitale domenet ser vi forsøk hver eneste dag.

Penger forsøkes hentet ut fra banken ved hjelp av eksempelvis SWIFT, betalingsløsninger og minibanker. Det er først og fremst organiserte kriminelle grupper som bedriver digitale bankran, men også den påståtte statlige nordkoreanske hackergruppen Lazarus blir ofte nevnt i denne sammenhengen.

De fysiske filialene blir færre, samtidig som den digitale banken har blitt hverdagen. Digitale bankran er nærmest risikofritt for en potensiell angriper. Det kan utføres fra andre siden av verden, fra trusselaktørens eget hjem eller i trygge kontorlokaler. De trenger ikke utsette seg selv for risikoen det utgjør å anskaffe våpen, fysisk sette seg selv og andre i fare inne i et lokale, komme seg derfra – og sannsynligheten for å bli dømt er lav.

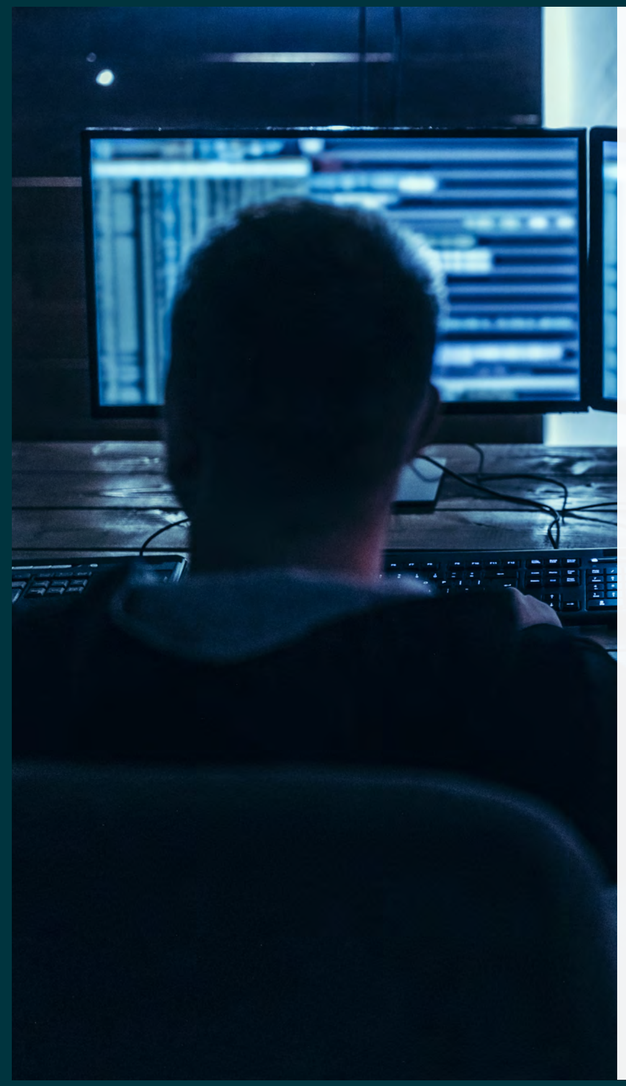
I februar ble Bank of Valletta (BOV) utsatt for et digitalt bankran. Banken måtte stenge alle sine operasjoner i ett døgn da det ble oppdaget at hackere hadde tatt seg inn i deres nettverk og lagt inn falske internasjonale betalinger. I februar i år meldte flere aviser at tre personer var arrestert i forbindelse med hvitvasking av pengene som ble stjålet fra BOV. Dette digitale bankranet ble utført av en gruppe som populært kalles EMPIRE MONKEY i sikkerhetsmiljøet, men det er ikke kjent hvilken nasjonalitet denne grupperingen har.

Den samme aktøren forsøkte i mars å trenge inn i banker i Norden ved å utgi seg for å være det norske og danske Finanstilsynet. Trussel-aktøren registrerte falske domener som:

- Finanstilsy.net
- Finanstilsynet-no.org

Trusselaktøren sendte deretter ut e-poster til nordiske banker, som så ut til å komme fra Finanstilsynet, som inneholdt lenker til disse falske sidene. Sidene var kopier av Finanstilsynets legitime sider. Gjennom et besøk på en av de falske sidene ble skadevare installert på datamaskinen til den som besøkte siden, for deretter å omdirigere brukeren til de legitime sidene til Finanstilsynet. Denne omdirigeringsteknikken minimerer angripers risiko for at brukeren selv oppdager noe mistenkelig.

I fjorårets trusselvurdering skrev vi om gruppen COBALT GANG som helt siden 2017 jevnlig har forsøkte å trenge inn i banken. Denne aktiviteten har de også fortsatt i 2019. Dette viser hvor lang tidshorisont noen av trusselaktørene har. Mot slutten av året så vi likevel få forsøk på å trenge inn i vestlige finansinstitusjoner, og gruppen har antagelig endret fokuset sitt mot Øst-Europa.



Utsikter mot 2021

Digitale bankran vil fortsette så lenge man kan bedrive det relativt risikofritt og så lenge den potensielle gevinsten ved vellykkede angrep er høy. Vi forventer likevel at flere aktører vil bevege seg over på utnyttelse av løsepengevirus, siden slike operasjoner er mindre teknisk krevende å gjennomføre, samt at «return on investment» vil være høyere. De kriminelle vil fortsette å utvikle sine verktøy og metoder.

Fem grupperinger

I DNB følger vi spesielt med på fem grupperinger som vi vet har kapabiliteten til å gjennomføre digitale bankran. En overvekt av disse er organiserte kriminelle som har tilhold i russisk språkområde. Flere av disse har forsøkt å trenge inn i DNBs IT-systemer det siste året.

DESTRUKTIVE ANGREP

Trusselnivå: Høy | Trend: Økende

Digital trussel

Kriminelle bruker krypteringsvirus for å presse bedrifter for penger, ved at de krypterer alle dataene til offeret og krever betaling for å gi bedriften tilgang til dekrypteringsnøkkelen.

For denne typen angrep peker pilen en vei: oppover. Både Europol og flere sikkerhetsselskaper peker på dette som den største digitale trusselen for virksomheter. Angrepene blir mer og mer målrettet.

For de kriminelle, så fungerer denne forretningsmodellen så lenge noen av ofrene velger å betale. Virksomheter som mangler sikkerhetskopi av filer, eller ikke har tilstrekkelig «backup», har kanskje ikke noe valg når det kommer til å betale løsepenger.

Norsk Hydro-hendelsen står igjen som en av de store hendelsene i 2019. Da et løsepengevirus krypterte deres IT-systemer, fikk hendelsen store konsekvenser for Hydro. Det resulterte i tapt produksjon, og store ressurser gikk med til krisehåndtering og gjenoppretting. De led et økonomisk tap på over 650 millioner kroner, og de brukte over et halvt år på å håndtere hendelsen ferdig.

Også i DNB har vi sett forsøk på at aktører har forsøkt å plante krypteringsvirus i vårt nettverk. Blant annet har en trusselaktør som assosieres med løsepengevirus forsøkt å trenge inn i vår digitale infrastruktur ved flere anledninger i 2019. Dette har blitt gjort ved bruk av e-poster som inneholder skadelige vedlegg. Hvis en mottaker av e-posten åpner vedlegget, kjøres skadelig kode i bakgrunnen som gir angriper kontroll over datamaskinen. Angriper har da mulighet til å utføre de samme handlingene på datamaskinen som den ansatte har. Med dette som en inngangsvektor har trusselaktøren forsert det første hinderet inn i nettverket og kan forsøke å bevege seg videre inn i nettverket til DNB. Omtrent halvparten av disse stanses av våre automatiske sikkerhetsmekanismer, mens de resterende stanses manuelt.

DISTRIBUERTE TJENESTENEKTANGREP

Distribuerte tjenestenektangrep (Distributed Denial of Service DDoS) er fortsatt en trussel. Siden DNB, i samarbeid med våre tjenesteleverandører, klarer å stanse angrepsforsøkene på en effektiv og god måte er dette likevel noe som sjeldent påvirker datasystemene til DNB.

Utsikter mot 2021

Målrettede destruktive angrep, og da spesielt løsepengevirus, vil svært sannsynlig øke i kommende år.

SPIONASJE OG TYVERI AV INFORMASJON

Trusselnivå: Moderat | Trend: Stabil

Informasjonstyveri

En trend som har blitt mer tydelig det siste året, er at trusselaktører samarbeider for å utnytte hverandres kompetanse. Aktører kan dermed spesialisere seg på spesifikke oppgaver eller teknologier, og bytte tjenester.

DNB besitter store mengder informasjon om vår egen og kunders virksomhet. Vi observerer mange forsøk på å komme inn i DNBs IT-systemer hvert år, men det er vanskelig å vurdere hva hensikten til aktørene er fordi de ofte blir stanset tidlig i hendelsesforløpet. Informasjonstyverier er en del av kartleggingsaktiviteten som en aktør må gjennom for å gjennomføre bedragerier og digitale bankran.

En trend som har blitt mer tydelig det siste året, er at trusselaktører samarbeider for å utnytte hverandres kompetanse. Aktører kan dermed spesialisere seg på spesifikke oppgaver eller teknologier, og bytte tjenester. For eksempel kan en trusselaktør som er ute etter informasjon hente det de trenger, for så å selge tilgangen til nettverket til noen som er eksperter på digitale bankran.

Et annet eksempel er at noen som er flinke teknisk kan samarbeide med noen som har kompetanse på pengeoverføringer eller hvit-vasking. Det at trusselaktørene samarbeider på denne måten, gjør at de hever kvaliteten i hvert ledd av sine operasjoner. Vi står altså ovenfor trusselaktører som har spesialområder de er eksperter innenfor, på lik linje som man ser i legitime og profesjonelle virksomheter.

Utsikter mot 2021

Det er forventet at spionasje og informasjonstyveri fortsetter på samme nivå.

Lokal, fysisk spionasje

Telefon, sosial manipulasjon, planting av avlyttingsutstyr. Gamle kjente metoder, kanskje justert inn i ny drakt, kan fortsatt brukes.

SYSTEMATISK TELEFONKARTLEGGING

En del av DNB internasjonalt var fra desember 2018 til mars 2019 mål for systematisk kartlegging over telefon. Totalt var det tre bølger av tilsammen 36 telefonsamtaler til syv DNB-kontorer internasjonalt og en lokasjon i Norge. Personer som ringte inn til DNBs internasjonale kontorer, utga seg for å være DNB-ansatte på reise, og ba om hjelp til å finne frem til personer eller kontaktdetaljer ved det aktuelle kontoret.

Undersøkelser rundt disse telefonsamtalene peker på at det var minst to personer som utga seg for å være ansatt i DNB. De brukte falske navn, navn til ansatte som har sluttet, eller utga seg for å være genuine ansatte. Telefonnumrene de ringte fra var fra USA, Kina, Italia, Sveits og Singapore, og var sannsynlig forfalsket. Kartleggingen var tydelig systematisk og lot seg kun identifisere ved at ansatte og lokale sikkerhetsansvarlige var årvåkne, og rapporterte disse til DNBs sikkerhetsorganisasjon sentralt. Det var nødvendig å sammenligne informasjon fra flere DNB enheter samtidig for å avsløre telefonkartleggingen.

FALSKE SOSIALE MEDIEPROFILER

Totalt har DNBs Cyber Defence Center (CDC) fått fjernet mer enn 200 falske sosiale media profiler, primært LinkedIn-profiler, hvor personer utgir seg for å være ansatt i DNB. Oftest brukes slike profiler i forbindelse med bedragerier utenfor DNB (se mer om bedrageri i egne kapitler). Det er også eksempler på at falske profiler brukes til å etablere nettverk inn mot DNB som kan brukes til å kartlegge personer og funksjoner i DNB, men også støtte videre sosial manipulasjon mot ansatte.

RUSSISK ETTERRETNING MOT WORLD ECONOMIC FORUM

I august 2019 ble to russiske statsborgere, hvorav en utga seg for å være rørlegger, stanset og holdt av Sveitsisk politi nær stedet hvor World Economic Forum (WEF) arrangeres i Davos. De to var ikke offisielt akkreditert til Sveits, men hadde russiske diplomatpass, og ble derfor sluppet fri. Sveitsisk politi mistenker at de to var russiske etterretningsagenter som forberedte videre handlinger mot mål under WEFs årlige konferanse. Hendelsen viser at russisk etterretning ønsker å samle inn informasjon fra den økonomisk-politiske sfæren. ■

Keylogger: ett eksempel
Keylogger er en liten fysisk enhet som kobles til en PC og registrer hvilke tastetrykk brukeren gjør. Enheten lagrer denne informasjonen og/ eller sender den ut ved hjelp av en type trådløs overføring. Alternativt kan den sende dataene den registrer skjult på nett.
Keyloggere kan også være i form av programvare, dvs. at de installeres som skadevare på datamaskiner. Keylogger brukes illegalt til å registrere hva brukeren skriver inn. Eksempler kan være pålogging eller der hvor brukeren skriver inn sensitiv informasjon.

Utsikter mot 2021
DNB må forvente nye forsøk på å kartlegge enkelt miljøer i konsernet ved hjelp av forskjellige former for informasjonsinnsamling. DNB kan også bli utsatt for at en på innsiden (ansatt, vikar, innleid, ol) samler informasjon som er tiltenkt benyttet for ulovlige formål, særlig vil strategisk viktig informasjon for DNB eller våre kunder, eller informasjon av betydning for ulike sektorer/markeder være mest relevant.

Avanserte kriminelle grupper og enkelte lands utenriksetterretning behersker et bredt spekter av metoder og arbeider også mot økonomiske mål. DNB med vår kundeportefølje kan være av interesse for disse.

Begrenset antall ran i Norge

Banker, postkontor og verditransporter ranes sjeldent i Norge.
I vårt naboland er ransaktiviteten høyere.

Antallet ran av bankfilialer og postkontor i Norge ligger stabilt på en til to i året. Flertallet av disse ranene er dårlig planlagt. Som regel er det en raner, noen få ganger to. I de fleste tilfellene blir raneren pågrepet i løpet av kort tid. I en del av tilfellene er det tegn på at raneren har handlet på impuls, eller med et ønske om å bli tatt.

Det siste forsøket på å rane en bankfilial i Norge skjedde 4. mars 2019. Ransforsøket ble utført av en tidligere ransdømt person, og var rettet mot en Sparebank1-filial på Majorstuen i Oslo. Det var tydelig at dette ranet foregikk uten at raner hadde utført noen god kartlegging på forhånd, da filialen var kontantløs. Til tross for at raneren truet med våpen inne i banklokalet, kom ingen fysisk til skade. Raneren ble pågrepet i nærheten av åstedet i løpet av relativt kort tid.

Selv om slike ran fremstår som amatørmessige, så kan de likevel være farlige for kunder og ansatte. Ran og ransforsøk medfører også stor psykisk belastning for de som blir truet, eller er i umiddelbar nærhet.

I Norge har i de senere år organiserte ran vært rette mot andre mål en kontanthåndterings-kjeden til banker. Kriminelle har sett gullsmeder og virksomheter som omsetter luksusvarer som mere egnede mål for ran.

Ved en anledning det siste året har østeuropeiske kriminelle utvist interesse for en ikke nærmere spesifisert kontanthåndteringskjede i Norge.

I Sverige fortsetter en ransaktivitet, som justert for folketallet, ligger på et nivå som er fem-seks ganger så høyt som i Norge. Mange av ranene er godt organisert, og har et høyt potensial for vold – for eksempel ved at ranere bruker automatvåpen. I Sverige har det vært et skifte fra ran av verditransporter og noen bankfilialer, til ran av vekslingsbyråer.

Gisseltakinger av nærstående til ansatte, med videre utpressing, forekommer meget sjelden. Vi har opplysninger om et tilfelle i Sentral-Europa i 2019 hvor en nær slektning til en pengetransportsjåfør ble tatt som gissel. Sjåføren ble tvunget av gisseltakerne til å kjøre til en parkeringsplass langs en større vei, hvorpå raneren tok pengene fra verditransporten. Gisselet ble løslatt på et annet sted senere samme dag. Det er fortsatt noen uavklarte omstendigheter rundt denne gisseltakingen og ranet. Det gjelder blant annet hva om skjedde med enkelte sikkerhets-funksjoner. ■

Utsikter mot 2021

Antall ran mot bank- og postfilialer i Norge vurderes til fortsatt å ville ligge på et til to per år. Et slikt ran vil sannsynlig bli utført av en enkelt person. 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.

Trusselaktører

Kriminelle enkeltpersoner, men det er også en meget liten mulighet for at en organisert gruppe ranere vil står bak.

Enkelte kunder truer og utagerer

Ansatte i DNBs kundefront blir utsatt for til dels grove trusler

I 2019 registrert vi et antall tilfeller hvor ansatte ble truet eller personer opptrådte utagerende overfor DNBs ansatte i Norge. Antall hendelser i 2019 er noe lavere enn i 2018, men dette skyldes sannsynlig variasjoner i rapportering og ren statistisk variasjon.

Fordelingen mellom tilfeller hvor truende eller utagerende personer var fysisk tilstede, versus tilfeller hvor truslene ble fremsatt per telefon, e-post eller chat er ca. femti-femti. Hendelser hvor den truende/utagerende personen er i umiddelbar nærhet av kunder, ansatte og/eller vektere vurderes som mest alvorlig. Det er i disse hendelsene potensialet for personskade er størst.

Per telefon, e-post og chat har det vært fremmet trusler med til dels meget alvorlig ordlyd. Eksempel på dette er trussel om drap overfor DNBs ansatte. Selv om den fysiske avstanden medfører at det ved hendelsene sjelden foreligger umiddelbar fare, så kan slike hendelser oppfattes som meget skremmende. For enkelte ansatte utgjør det en betydelig psykisk belastning, og det kan foreligge fare for psykiske ettervirkninger.

Kundene som fremmer trusler er nesten utelukkende privatkunder. Ved to av tilfellene har personen(e) som truet vært tilknytte organisert kriminalitet uten at selve truslene kan knyttes til slik virksomhet. I ett tilfelle kan trusler som ble fremmet mot en ansatt i arbeidtiden ha sin årsak i private forhold. Den faktoren som er mest fremtredende, er likevel at personene som truer og/eller utagerer har tegn på psykiske problemer og/eller er ruset.

Trusselsituasjonene oppstår oftest i forbindelse med at kunde ikke har midler, nektes adgang til konto eller nektes tilgang til midler på annen måte. I noen få tilfeller har det blitt fremmet trusler i forbindelse med eiendomssalg under skilsmisseoppgjør.

Med den markerte økonomiske nedgangen som kan observeres nå i starten av 2020, så er det betydelig usikkerhet om den økonomisk utviklingen i Norge videre i 2020. Hvis deler av befolkningen opplever å få vesentlig forverret økonomi med, tap av midler, inntektssvikt eller arbeidsledighet, kan antallet hendelser med truende/utagerende atferd forventes å øke noe. Det er spesielt i fasen hvor personer får forverret økonomien sin at potensialet for truende og/eller utagerende atferd kan utløses. Graden av økning i truende og utagerende atferd kan derfor ventes å ha en delvis sammenheng med i hvilken grad store grupper av befolkningen rammes av økonomisk nedgang. ■

Utsikter mot 2021
Omfanget og alvorlighetsgraden av trusler mot ansatte drives delvis av ytre samfunnsforhold og antakelig i noen grad av DNBs handlinger overfor kundene. Det ligger en betydelig usikkerhet i utviklingen i nordmenns privatøkonomi videre inn i 2020. Det vurderes at antallet hendelser hvor ansatte blir truet med fysisk skade, eller står overfor fysisk utagerende personer kan øke en del i 2020 og ligge i et område med 35–60 hendelser i inneværende år. I halvparten av tilfellene vil personen som truer og/eller utagerer være på samme sted som våre kunder og ansatte. Den andre halvparten av hendelsen vil bestå av trusler som fremmes overfor ansatte per telefon, e-post eller chat.

Trusselaktører
Primært kunder i privatmarkedet

*

Like truet som samfunnet omkring

I Europa regnes nå trusselen om høyreekstrem terrorisme som like stor som truselen fra ekstrem islamistisk terrorisme.

DNB I NORGE

I september 2019 endret Politiets Sikkerhetstjeneste (PST) trusselnivået for høyreekstremistisk terrorisme i Norge til «Mulig». Dette skjedde i etterkant av terrorangrepet ved Al Noor-moskeen i Bærum i august i fjor. Endringen i PSTs vurdering medfører at høyreekstremistisk terrorisme og ekstrem islamistisk terrorisme ble vurdert å være like høy. PST har videreført disse trusselnivåene i sin vurdering for 2020. Trusselen fra ekstrem venstreradikal terrorisme ble vurdert som «svært lite sannsynlig».

PST har begrunnet hevingen av trusselnivået for høyreekstrem terrorisme med økende radikalisering i diskusjonsfora på nett, og hvordan høyreekstreme terrorister som står bak rasistiske og islamofobe angrep i utlandet har motivert andre til å foreta nye angrep. PST peker generelt på de forsøkene som motivere personer til selv å foreta såkalte «motiverte angrep» som foregår både i høyreekstreme og ekstreme islamistiske miljøer. Dersom det skulle komme til en terrorhandling er det derfor mest sannsynlig at handlingen utføres av en enkeltperson.

Det foreligger ikke informasjon som tilsier at noen terrorister har finanssektoren eller DNB som mål.

DNB I UTLANDET

Den globale terrortrusselen kommer først og fremst fra jihadistiske terrorgrupper. Høyreekstrem terror er også relevant for Europa og USA. Det er en økt polarisering mellom høyre- og venstreside i både amerikansk og europeisk politikk. I Europa har politi- og sikkerhetsmyndigheter varslet om økt høyreekstrem terror, og da spesielt rettet mot innvandrere og islamske mål.

Internasjonalt er DNB representert i flere byer som har vært utsatt for terrorangrep. Storbyer som London, Paris, Berlin, Stockholm og New York har alle vært utsatt for alvorlige terrorangrep de siste årene. Det er ingen informasjon om at finanssektoren eller DNB spesielt er pekt ut som mål.

I løpet av en lengre periode i oktober–november 2019 var det store til dels voldelige demonstrasjoner i Santiago, Chile. Demonstrantene protesterte mot politisk undertrykking og ressursfordeling i samfunnet. Ved flere anledninger beveget demonstrasjoner seg i nærheten av DNBs lokaler og i nærhet til hvor DNB ansatte bor. Det er ingen indikasjoner på at DNB var mål for demonstrantene. ■

Utsikter mot 2021

Det er ingenting som tilsier at finanssektoren er spesielt utsatt for terrorangrep. Det er heller ingen terrorgrupper eller terrorister som har DNB som sitt uttalte fiendebilde, hverken nasjonalt eller internasjonalt. Det betyr at DNB er eksponert for den samme generelle trusselen som er i landene vi har kontorer, og kan på den måten bli rammet av et terrorangrep.

Trusselaktører

Radikaliserte enkeltpersoner med både ekstrem islamistisk og høyreekstrem motivasjon. Ekstreme islamistiske grupper, høyreekstreme grupper, venstreekstreme grupper.

Rekordhøye bedrageritall

I 2019 forsøkte kriminelle å bedra DNB og våre kunder for i overkant av 1,2 milliarder kroner.

For å tilegne seg penger fra konsernet utnytter organiserte kriminelle prosesser, systemer og mennesker. De sikter seg inn på sårbare grupper og skyr ingen midler for å nå sine mål. Mange av bedrageriene ble stanset, men både kunder, konsernet og samfunnet lider av tapene påført gjennom økonomisk kriminalitet.

Kriminelle forsøker å bedra DNB på mange måter. I 2019 så vi blant annet eksempel på store korttestingssaker hvor kriminelle forsøker å gjette på og konstruere reell kortinformasjon til bruk ved netthandel. Angrepene mot DNB var også preget av lånebedragerier og organiserte kriminelle miljøer som utnytter flyktninger for å gjennomføre utspekulerte bedragerier i stor skala. Det finnes flere organiserte miljøer i Norge og i utlandet som har hatt DNB som mål over lang tid og vi samarbeider med politiet og andre finansinstitusjoner for å opprettholde kontroll på dette området.

Flere saker har innslag av ID-tyverier. Media har den siste tiden fokusert mye på saker knyttet til misbruk av BankID spesielt i nære relasjoner. Disse sakene får ofte store konsekvenser for de som er involvert, og kan dermed også påvirke DNB sitt omdømme negativt.

Fjorårets trusselvurdering fokuserte på at trusselen mot konsernet kom til å holde seg stabil frem mot 2020. Dette har stemt med utviklingen vi har sett i løpet av året. Frem mot 2021 regner vi med en fortsatt stabil utvikling. Gruppene som gjennomfører målrettede bedragerier mot konsernet vil fortsette å utvikle sine metoder og sine verktøy, men det er ingen grunn til å tro at dette vil føre til en merkbar endring. Fremover kan vi forvente variasjoner av bedragerier vi har sett tidligere, både fra kjente aktører og fra nye aktører som kopierer andre som har hatt kriminell suksess.

Trusselaktørene som utgjør en trussel mot DNB har ofte tilknytninger til Sentral- og Øst-Europa, men med en fysisk tilstedeværelse og velfungerende nettverk i Norge. ■

Utsikter mot 2021
Det forventes en stabil utvikling når det gjelder angrep mot konsernet, til tross for at de kriminelle vil ta i bruk nye verktøy og metoder.

Kunder under angrep

I løpet av 2019 håndterte DNBs Financial Cyber Crime Center over 4000 saker.
De fleste av disse har vært forsøk på bedrageri mot våre kunder.

I likhet med bedrageriene i 2018 fokuserer de organiserte kriminelle miljøene mye av sine krefter på det svakeste leddet i kjeden. I dette tilfellet er det mennesket, ikke systemet, og kunder er enklere mål enn ansatte.

Vi opplevde i 2019 en massiv økning i bedragerier mot våre kunder. Mange av de tidligere omtalte modusene har dominert trusselbildet også i 2019, blant annet registrerte vi en 125 % økning i investeringsbedragerier. Samtidig har det dukket opp nye aktører som har brakt med seg nye modus. Det mest omtalte av disse er vishing (voice phishing), eller phishing over telefonen. Disse ble i media omtalt som «Olga-saker».

Koblingen mellom de organiserte kriminelle miljøene som driver med disse bedrageriene og andre former for alvorlig kriminalitet er sterkere enn noensinne. I tillegg til at de kriminelle gruppene driver med våpen-, narkotika- og menneskesmugling har man også fått satt fokus på den potensielt store faren for terrorfinansiering gjennom andre former for økonomisk kriminalitet.

Det er ikke alltid snakk om en direkte terrorfinansiering hvor terrorgrupper bruker økonomisk kriminalitet for å få midler til å gjennomføre terrorangrep. Det finnes også sterke bånd og samarbeidsallianser mellom mange organiserte kriminelle grupper og terrorgrupper. Disse samarbeider som regel ikke av ideologiske grunner, men heller fordi de er gjensidig avhengig av hverandre. Organiserte kriminelle miljøer trenger våpen, narkotika og ønsker å ta sin del av de store gevinstene som finnes i menneskesmugling. Dette krever samarbeid med terrorgrupper, eller grupper med sterke bånd til terrorgrupperinger, da disse ofte kontrollerer de ønskede ressursene eller nødvendige landområder.

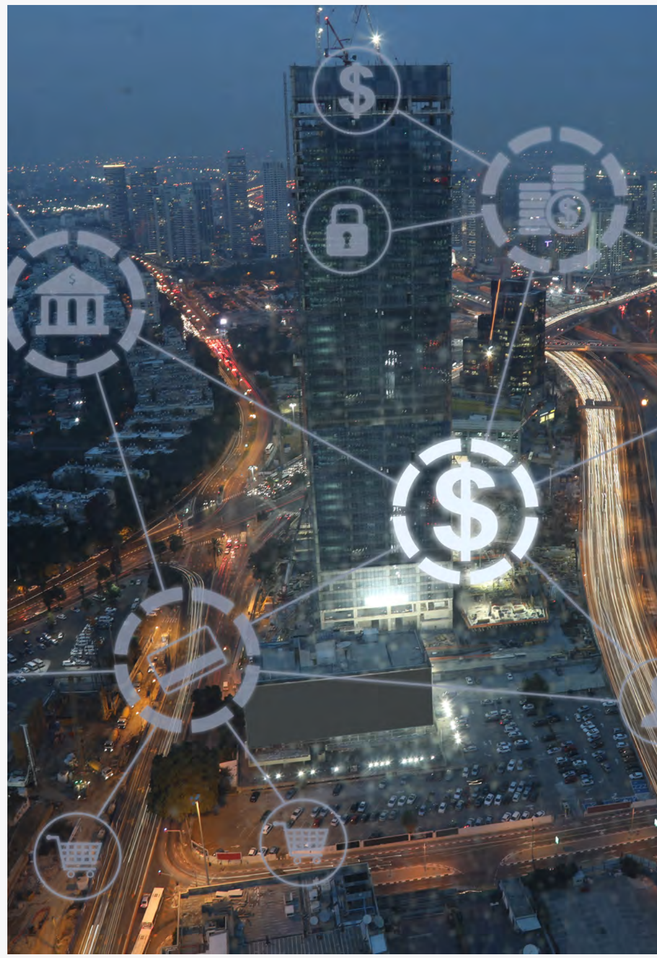
Terrorgruppene på sin side er ofte ikke godt nok kjent med det finansielle systemet og hvordan man skal flytte ulovlig midler. Ikke minst trenger de hjelp til å realisere disse midlene til verdier der de befinner seg. Et slikt gjensidig avhengighetsforhold sannsynliggjør at penger fra bedragerier og annen økonomisk kriminalitet senere forsvinner inn i finansieringen av terror.

VISHING

Vishing går ut på at bedragere tar kontakt med offeret på telefonen og forsøker å få dem til å opplyse enten betalingsdetaljer, som regel i form av kortdetaljer, eller påloggingsinformasjonen nødvendig for å kunne logge på nettbanken og gjennomføre en transaksjon. Både falsk IT-support og noen former for investeringsbedrageri har benyttet denne metoden tidligere, men vishing-kampanjene kundene våre opplevde høsten 2019 er noe nytt i Norge. I tillegg til at vishing var nytt var sakene spesielt alvorlig da de kriminelle nærmest utelukkende siket seg inn på eldre mennesker. Videre tømte de ofrenes bankkonto så langt det lot seg gjøre.

Det er nå snakk om konkrete kampanjer som gjennomføres av organiserte grupperinger som har en fysisk tilstedeværelse i Norge.

Vishing er ikke nytt i Sverige og Danmark hvor problemet har eskalert over tid. I Danmark har det tidligere vært innenfor disse bedrageriene man har sett størst tap nasjonalt. Et tett samarbeid med politiet og andre finansinstitusjoner førte til at disse miljøene raskt ble slått relativt hardt ▶



ned på i Norge. Det er mye som tyder på at vi her snakker om svenske organiserte kriminelle miljøer som har valgt å angripe personer i Norge og har brukt nordmenn for å gjennomføre bedrageriene.

Til tross for at deler av dette miljøet raskt ble tatt hånd om er det naturlig å tro at disse sakene ikke vil gå over. I løpet av året er det sannsynlig at man vil se flere slike kampanjer komme i bølger. Det kan ta noe lenger tid før vi i Norge havner i samme situasjon som Danmark og Sverige hvor disse sakene pågår kontinuerlig.

INVESTERINGSBEDRAGERI OG KJÆRLIGHETSBEDRAGERI

Mens investeringsbedrageri har sett en dramatisk økning det siste året har kjærlighets-bedragerier holdt seg relativt stabilt, med en liten registrert nedgang. Vi vet nå at kjærlighetsbedragerier ikke bare brukes av bedragere som en inntektskilde, men også som en måte å skaffe kontoer de kan benytte seg av i en hvitvaskingsprosess (muldyrkontoer). Det er ingen grunn til å tro at behovet for muldyrkontoer skal gå ned. Kjærlighetsbedragerier er relativt enkle å gjennomføre og vi tror de vil utgjøre en tilsvarende trussel i 2020 som i 2019.

Når det gjelder investeringsbedragerier er det vanskelig å vite når den eksplosive økningen vil ta slutt. Aktørene er store organiserte kriminelle grupperinger med en tilstedeværelse i blant annet, Øst-Europa og Israel. Det har vært flere avsløringer av disse gruppene og deres «callsentre» den siste tiden, men slike avsløringer og aksjoner er ikke i seg selv nok til å redusere trusselen. Det er mye penger å tjene for de kriminelle miljøene involvert i disse bedrageriene og det er ikke sannsynlig at trusselen fra disse gruppene vil reduseres i 2020.

Et område hvor vi kan forvente å se endringer fremover er det som drives frem av PSD2/ Open Banking. Når mange eksterne aktører blir gitt mulighet til å gjennomføre transaksjoner på vegne av våre kunder i deres nettbank vil det åpnes opp noen store muligheter for kriminelle grupperinger. Trusselaktørene er flinke til å utnytte tidsrommet hvor et produkt er nytt og det er noe usikkerhet blant brukere. Vi vil se flere aktører som utnytter denne usikkerheten i året som kommer. I starten av 2020 ser vi at de kriminelle overtaler kundene til å bruke betalingstjenester som ligger utenfor banken infrastruktur og dermed kontroll.

BUSINESS EMAIL COMPROMISE (BEC)

Kompromittert epost (BEC) er fremdeles den dimensjonerende trusselen mot våre bedrifts-kunder når det gjelder bedrageri. Innenfor denne kategorien finner man direktørbedrageri og falske fakturaer, spoofing og faktisk kompromitterte e-postkontoer.

Den store utviklingen her går på hvor mye de kriminelle forsøker å bedra kundene våre for og hvilket aktører som er involvert. De siste årene har dette feltet vært dominert av Vestafrikanske grupperinger, med varierende kompetanse, som forsøker å bedra små til mellomstore bedrifter for 50.000 NOK – 3.000.000 NOK. Målene deres varierte men gikk ofte i bølger og hadde fokus på kunder som sportsbutikker, kirker eller lag og foreninger.

Andre halvdel av 2019 så vi en dramatisk økning i angrep mot store bedrifter hvor angrepssummen ofte var over 10.000.000 NOK. Et av de største bedrageriene i norsk historie ble også gjennomført i 2019, da et selskap (ikke DNB-kunde) tapte 150.000.000 NOK på et slikt bedrageri. Det er sannsynlig at disse angrepene med betydelig høyere angrepssum gjennomføres av langt mer sofistikerte grupperinger med tilknytning til og tilstedeværelse i Israel.

Disse grupperingene er kjent for å ha gjennomført store angrep i Norge tidligere. Blant annet Operasjon Jackpot (2016) hvor politiet i Norge og Israel aksjonerte mot organiserte kriminelle miljøer i Israel etter at de hadde bedratt et norsk selskap for en halv milliard kroner.

Det er grunn til å tro at disse angrepene vil fortsette utover 2020 og at angrepene fra disse mer sofistikerte grupperingene vil øke. Trusselen mot våre kunder er høy og øker videre. ■

Utsikter mot 2021
Det er høyst sannsynlig at angrep mot våre bedrifts og privat kunder vil profesjonaliseres og øke i tiden frem mot 2021.

DNB