POLITIET

Nyhetsbrev fra næringslivskontakten
Nordland politidistrikt

I denne utgaven:

- ✓ Trusler mot næringslivet i 2022

INNLEDNING
I dette nyhetsbrevet fokuserer vi på hva politiet mener er de mest alvorlige kriminalitetstruslene mot næringslivet i 2022. Gjennom dette ønsker vi å gjøre næringslivet bedre kjent med truslene slik at næringslivet selv kan foreta risikovurderinger, og eventuelt treffe nødvendige tiltak som kan bidra til å forebygge kriminalitet.

Dersom enkelte virksomheter i Nordland ønsker bistand fra politiet i dette arbeidet kan man ta kontakt med næringslivskontakten i Nordland. Se kontaktinformasjon til næringslivskontakten i Nordland i siste avsnitt i dette nyhetsbrevet.

TRUSLER MOT NÆRINGSLIVET
Man vil løfte frem trusler mot næringslivet som er vurdert som spesielt alvorlige, og hvor det forventes en negativ utvikling. Vurderinger av hva som vil skje frem i tid vil imidlertid alltid inneholde en viss grad av usikkerhet. Mange av kriminalitetstruslene muliggjøres og understøttes av teknologi, og dette har for så vidt også utvidet handlingsrommet til de kriminelle.

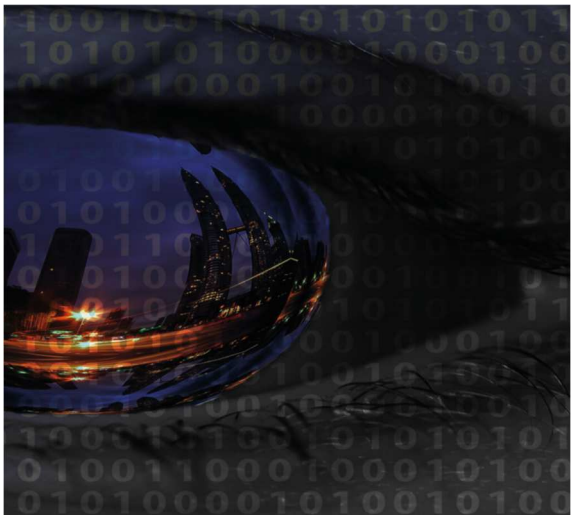
DIGITAL VINNINGSKRIMINALITET
I 2021 ble det anmeldt nærmere 19 000 bedragerisaker i Norge. Felles for de fleste bedrageri er at de i økende grad foregår i det digitale domenet. Digitale bedrageri er den nye vinningskriminaliteten som rammer næringslivet og folk flest. I årene fremover forventes det at bedrageriforsøk vil automatiseres og i større grad tilpasses den enkelte som usettes for dette. Digital vinningskriminalitet er i mange tilfeller massebedragerier som distribueres til mange potensielle ofre. Aktørene som står bak er ofte kriminelle nettverk, både norske og utenlandske.

Det er *meget sannsynlig* at omfanget av digital vinningskriminalitet vil øke.

INVESTERINGSBEDRAGERI
Investeringsbedrageri innebærer at man blir forledet til å investere i prosjekter eller produkter som er verdiløse eller ikke-eksisterende. Dette kan være investeringer i kryptovaluta, aksjer eller andre finansielle instrumenter, eiendom, råvarer og verdifulle gjenstander som kunst og antikviteter. Sosial manipulering er ofte en sentral del av bedrageriprosessen.

De siste årene har investeringsbedrageri ved salg av kryptovaluta økt. Metodene er mange. Enkelte modus er de samme som for bedrageri ved aksjeinvesteringer. Andre modus inkluderer opprettelse av falske handelsplattformer på nett, gjerne kombinert med en aggressiv markedsføring i sosiale medier som også misbruker kjente personer for å skaffe legitimitet. Fornærmede kan også motta fiktive kvitteringer og dokumentasjon på investering og gevinst, som igjen brukes for å manipulere fornærmede til å gjøre ytterligere investeringer. Økokrim estimerer at norske bedrageriofre har sendt omlag 75 millioner kroner ut av landet i forbindelse med kryptobedrageri i 2021. Globalt økte tapene ved bedrageri via kryptovaluta med omlag 81 prosent i 2021 sammenlignet med året før.

Politiet mener at det er *meget sannsynlig* at omfanget av investeringsbedrageri med kryptovaluta og falske handelsplattformer vil øke.



DIREKTØRBEDRAGERI
Ved direktørbedrageri utgir bedragere seg for å være en leder, og kontakter medarbeidere i

en virksomhet eller forening for å manipulere de til å overføre en større sum penger eller godkjenne utbetalinger. Henvendelsen kan komme via e-post eller telefon. Sistnevnte er gjerne mer målrettede og benyttes ved større og mer kompliserte forsøk på direktørbedrageri. I følge Næringslivets Sikkerhetsråd har ni prosent av norske virksomheter i løpet av en ettårsperiode blitt utsatt for direktørbedrageri, eller blitt forsøkt utsatt for denne typen bedrageri. Det er like vanlig i offentlig som privat sektor, men det er mer sannsynlig at større enn små foretak blir utsatt for direktørbedrageri.

Direktørbedrageri er en type bedrageri som i enkelttilfeller, særlig når det rettes mot store internasjonale foretak, kan generere stort utbytte. Ved flere tilfeller er norske foretak bedratt for beløp over hundre millioner kroner. Samme modus benyttes også i saker med lavere bedrageribeløp.

Det er *meget sannsynlig* at ny tilgjengelig teknologi, som deepfake, vil bli benyttet i økt omfang ved forsøk på direktørbedrageri mot større foretak.

DATAINNBRUDD
Datainnbrudd uten påfølgende bruk av løsepengevirus utgjør en alvorlig trussel mot norske virksomheter, særlig ved tyveri av data. Økonomisk vinning oppnås gjerne ved å selge stjålet informasjon eller illegitime systemtilganger til andre kriminelle eller statlige aktører.

Det er *meget sannsynlig* at norske virksomheter vil bli utsatt for datainnbrudd og datatyveri.

LØSEPENGEVIRUS
Løsepengevirus rettet mot bedrifter og virksomheter anses som den største trusselen i det digitale rom. Bakgrunnen for denne vurderingen er en jevn økning i antall hendelser, samt liten fare for identifisering og straffeforfølgning.

Aktørene oppnår tilgang ved bruk av phishing, utnyttelse av lekkede eller svake passord og ved å utnytte sårbarheter i programvaren eller nettverket til offeret. Virksomheter med tidskritiske prosesser er sårbare mål. Politiet har registrert det siste året at aktørene i økende grad har benyttet dobbel utpressing – dvs. at de i tillegg til å kryptere stjeler data om de truer med å offentliggjøre.

Det er *meget sannsynlig* at norske virksomheter vil bli utsatt for løsepengevirus.

HVITVASKING VIA VIRTUELLE EIENDELER
Virtuelle eiendeler vil trolig bli mer utbredt i nettbaserte spill, innen kunst og i finans. Dette medfører nye muligheter, men også nye utfordringer. Det er *sannsynlig* at virtuelle eiendeler i økende grad vil bli brukt til hvitvasking.

Det er estimert at det ble hvitvasket 8,6 milliarder dollar (USD) via kryptovaluta i 2021, noe som er en økning fra tidligere år. Dette utgjør bare en liten andel (0,15 prosent) av det totale transaksjonsvolumet av kryptovaluta i 2021, men baserer seg kun på de transaksjonene som har blitt fanget opp som hvitvasking.
Hvitvasking av utbytte fra tradisjonell narkotika- og annen organisert kriminalitet fanges antakelig opp i liten grad, da slike transaksjoner hovedsakelig vil fremstå som lovlige transaksjoner fra en person til en annen. Det er et relativt lite antall utenlandske vekslingstjenester som mottar mesteparten av det kjente utbyttet som hvitvaskes via kryptovaluta. Disse bruker ofte infrastrukturen og likviditeten til en større vekslingstjeneste, men har selv ansvaret for å kontrollere

opplysninger om kunder og opphavet til pengene. Dette er ofte svært mangelfullt utført. Det er også utfordrende at mange av de store internasjonale kryptovekslingstjenestene holder til i jurisdiksjoner kjent for manglende åpenhet og tilsynsvirksomhet. En del vekslingstjenester har hatt tilhold i samme kontorbygg i Moskva og hvitvasket enorme summer knyttet til russiske kriminelle.

NFT-er er en annen virtuell eiendel som kan benyttes til hvitvasking. NFT står for "non-fungible token", og er et unikt bevis på eierskap over noe som ikke er fysisk, som digitale filer som kunst, lyd, gjenstander i videospill og andre former for kreativt arbeid. NFT er en unik kode, lagret og beskyttet på en offentlig tilgjengelig blokkjede. Bruksområdet for NFT-er kan bli betraktelig større enn i dag. Eksempelvis kan artister bevise eierskap til musikk eller video, noe som vil gjøre det mulig for kunstnere, artister og andre å selge sine produkter og tjenester direkte til fans. NFT-er utnyttes også av kriminelle aktører. Det finnes flere eksempler på at personer har kjøpt «falske» NFT-er. I praksis betyr dette at man kjøper en kopi fra en annen utgiver. Dette kan sammenlignes med å kjøpe falske merkeklær. I denne sammenheng gjennomfører ofte bedragerne falske handler, såkalt «wash trading», noe som medfører at NFT-er fremstår som hyppig omsatt og populær når dette i realiteten ikke er tilfellet. Det er indikasjoner på at «wash trading» har økt betydelig i 2021.

BRUKEN AV PENGEMULDYR ØKER

Med pengemuldyr menes de personer som mottar penger digitalt eller i kontanter fra én person og overfører dem videre til en annen mot betaling.

Ofte overfører pengemuldyrene pengene for bedragerne til utenlandske bankkonti. Bruk av pengemuldyr er et økende problem i mange land. Pengemuldyr benyttes særlig i tilknytning til digital vinningskriminalitet, det er derfor *sannsynlig* at vi vil se en økning også i bruken av pengemuldyr i Norge de neste årene.

Danmark registrerte en økning i antall oppdagede pengemuldyrkontoer på 400 prosent i perioden 2018 til 2020. I Norge rapporterte en av de største bankene at de avviklet nærmere 1500 kundeforhold i 2021 grunnet mistanke om hvitvasking, bedrageri, svindel og pengemuldyraktivitet. Dette er økning fra 2020, og en fortsettelse av en trend man har sett over flere år. Økokrim opplever også at antall rapporteringer om pengemuldyr har økt de siste fem årene.

NÆRINGSLIVSKONTAKTEN I NORDLAND

Næringslivskontakten i Nordland arbeider med å forebygge og redusere arbeidsmarkeds-kriminalitet og kriminalitet rettet mot næringslivet.

Næringslivskontakten er politidistriktets hovedkontakt med næringslivet utenom straffesakssporet, og skal gi råd og videreformidle henvendelser til rett instans.
Funksjonen skal sørge for et godt lokalt samarbeid mellom politiet, næringslivet, sikkerhetsmyndigheter og andre aktører i det sivile samfunn. Dette vil bidra til både proaktive og treffsikre tiltak i næringslivet og hos andre private aktører, og til en helhetlig og kunnskapsbasert kriminalitetsbekjempelse i politiet.

Håvard Fjærli er Næringslivskontakten i Nordland politidistrikt. Han kan kontaktes på:
Tlf. 918 83 382
E-mail: havard.fjarli@politiet.no

Kilder:

Politiets åpne trusselvurdering for 2022.
Politiets trusselvurdering 2022, Kripos.
Trusslevudering2022, Økokrim.