POLITIET

Nyhetsbrev fra næringslivskontakten

Nordland politidistrikt

I denne utgaven:

- ✓ Trusler mot næringslivet
- ✓ Datainnbrudd med løsepengevirus
- ✓ Bedrageri mot næringslivet
- ✓ Investeringsbedrageri
- ✓ Råd for å forebygge digital kriminalitet

INNLEDNING
I dette nyhetsbrevet har vi fokus på hva politiet i Nordland mener er de største kriminalitetstruslene mot næringslivet i 2021. På denne måten ønsker vi å gjøre næringslivet bedre kjent med truslene slik at næringslivet selv kan foreta en risikovurdering av truslene opp mot egen virksomhet, 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
Trusler mot næringslivet kan foregå gjennom ulike kanaler, men her skal man ha fokus på den kriminaliteten som foregår digitalt over internett. Datakriminalitet begås først og fremst for økonomisk vinning. Noen tilfeller av datakriminalitet begås imidlertid for å skade maskinvare, eller digitale tjenester, eller for å skaffe sensitiv informasjon. Denne type kriminalitet rammer både næringslivet, offentlige virksomheter, og kritiske samfunnsfunksjoner i tillegg til privatpersoner.

Nedenfor følger utvalgte særlig alvorlige kriminalitetstrusler innenfor denne hovedkategorien.

DATAINNBRUDD MED LØSPENGEVIRUS
Politiet vurderer det som meget sannsynlig at norske virksomheter vil bli utsatt for datainnbrudd med løsepengevirus. Dette ses i sammenheng med en jevn økning i antallet hendelser de siste årene, og mulighet for høy profitt. I tillegg er identifisering av gjerningspersoner og straffeforfølgelse meget komplekst.

Løsepengevirus er den største nåværende trusselen på datakriminalitetsfeltet, og har kostet næringslivet flere hundre millioner kroner de to siste årene. Dette er en type skadevare som brukes til å kryptere datafiler i offerets datasystem, før aktøren krever løsepenger mot å heve krypteringen. Metoden er komplisert og krever avansert teknisk kompetanse.

Antallet registrerte tilfeller av løsepengevirus, både forsøk og vellykkede tilfeller, har økt globalt og i Norge siden 2013. Globalt er det anslagsvis 5–15 Internasjonale aktører som er aktive til enhver tid. I Norge har vi informasjon om at én aktør alene har gjennomført over 30 vellykkede datainnbrudd mot norske bedrifter det siste året. Løsepengevirus og andre former for datakriminalitet starter ofte likt, ved at aktøren leter bredt etter innganger til potensielle ofres nettverk. Dette kan skje blant annet ved sosial manipulering i e-poster (phishing), utnyttelse av svakheter i programvare, eller gjetting av passord (brute forcing). Når aktøren først har fått informasjon som kan utnyttes, kan det ta flere måneder før løsepengeviruset aktiveres, noe som gjør det vanskelig både å håndtere hendelsen umiddelbart, og å spore relevant nettverksaktivitet. Selv om få datainnbrudd er vellykkede, er det stort potensial for profitt, og mulighetene for å identifisere og straffeforfølge gjerningspersonene er små.

Skadepotensialet for ofrene er betydelig. Et kjent eksempel er datainnbruddet mot Norsk Hydro i 2019, som kostet virksomheten ca. 600 millioner kroner. Koronapandemien har belyst sårbarheten til offentlige virksomheter med kritiske beredskapsfunksjoner. Internasjonalt er det meldt om flere hendelser med løsepengevirus mot nasjonale beredskapsfunksjoner. Et slikt angrep kan i ytterste konsekvens føre til tap av liv og helse, samt svekke tilliten til den rammede samfunnsfunksjonen.

BEDRAGERI MOT NÆRINGSLIVET
Politiet vurderer det som meget sannsynlig at kriminelle aktører vil øke sin aktivitet med faktura- og direktørbedrageri rettet mot norske virksomheter. Dette ses i sammenheng med potensialet for høy profitt, lav oppdagelsesrisiko og en økning de siste årene. Større virksomheter er mer utsatt for målrettede bedragerier, mens mindre virksomheter oftere er utsatt for massebedragerier.

Kriminelle aktører benytter særlig to fremgangsmåter:

1. Faktura- og direktørbedrageri.
Ved fakturabedrageri forledes mottakeren av fakturaen til å betale for en vare eller tjeneste vedkommende ikke har bestilt, eller aktøren endrer mottakers kontonummer på en reell faktura ved å sende en e-post med «oppdatert» betalingsinformasjon. Ved direktørbedrageri skaffer den kriminelle aktøren seg informasjon om nøkkelindivider i en organisasjon. Aktøren utgir seg så for å være leder og henvender seg ofte til en økonomimedarbeider i organisasjonen for å få overført en større sum penger til utlandet. Faktura- og direktørbedrageri har økt i omfang de siste årene. I 2019 utgjorde direktør og fakturabedrageri nærmere 60 prosent av det økonomiske tapet knyttet til svindel ved bruk av sosial manipulering i Norge. 13 prosent av norske virksomheter oppga i 2019 å ha blitt utsatt for direktørbedrageri i løpet av det siste året. Større virksomheter er særlig utsatt, men også frivillige organisasjoner er målgruppe for denne typen kriminalitet. Den betydelige gevinsten kriminelle tilegner seg, blir i mange tilfeller reinvestert i andre typer kriminalitet.

Faktura- og direktørbedrageri ved endring av mottakers kontonummer utføres av organiserte kriminelle grupperinger i utlandet. Aktørene fremstår som tilpasningsdyktige, de velger ofre bevisst, og utnytter menneskelige feil og/eller sårbarheter i datasystemer. Det økonomiske tapet som følge av faktura-bedrageri økte fra 8,7 millioner kroner i 2018 til rundt 138,5 millioner kroner i 2019.

Konsekvensene for enkeltbedrifter kan være store, og siden bedrageriet i ytterste konsekvens kan føre til konkurs, vil det også kunne påvirke enkeltindivider i stor grad. Økt bruk av hjemmekontor har gjort bedrifter særlig utsatt for faktura- og direktørbedrageri. I 2020 så Nordic Financial Cert en økning i faktura- og direktørbedrageri. Under koronapandemien har det også blitt avslørt mange fakturabedragerier knyttet til blant annet smitteforebygging.

2. Investeringsbedrageri
Under koronapandemien har det vært en økning i antallet tilfeller av investeringsbedrageri, spesielt aksje-bedragerier via falske handelsplattformer. Det er meget sannsynlig at investerings-bedragerier vil fortsette å øke både knyttet til kryptovaluta, og falske handelsplattformer.

Et investeringsbedrageri går ut på å forlede privatpersoner eller foretak til å investere i prosjekter eller produkter som er verdiløse eller ikke-eksisterende. Sosial manipulering er en sentral del av bedrageriprosessen. Det rapporteres at antallet forsøk på Investeringsbedrageri ble doblet i 2020, sammenlignet med 2019. Flere banker rapporterer om en økning i antallet svindelforsøk siden 2018, med en særlig økning i 2019, som har fortsatt i 2020. Under koronapandemien har mange, særlig eldre, blitt sittende mer hjemme alene. Dette har gjort dem mer sårbare for svindel.

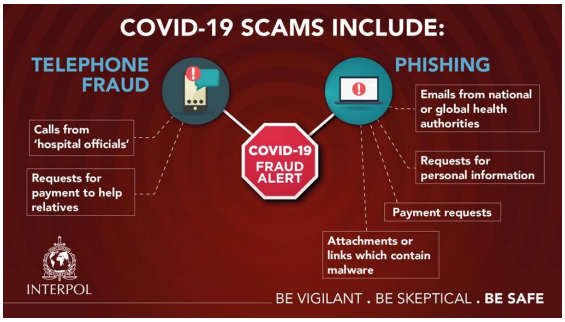
En fremtredende modus innen investerings-bedrageri er å tilby salg av aksjer eller kryptovaluta. Pyramidespill med salg av kryptovaluta tiltrekker seg privatpersoner gjennom løfter om høy avkastning. Verdiøkningen investorene forespeiles, er kun en illusjon, fordi kryptovalutaen ikke eksisterer.

Pyramidespillets forretningsmodell går ut på å verve nye investorer som sikrer ny kapital, som utbetales til bedragerne, mens investorene taper investeringen. Et eksempel på et slikt pyramidespill er OneCoin. Organiserte kriminelle grupperinger på Balkan antas å ha svindlet til seg rundt fire milliarder euro i perioden 2014–2018 gjennom dette spillet.

Eiendomsbedrageri har vist seg å være lukrativt i Norge. Bedragerne etablerer egne aksjeselskap som angivelig driver med eiendomsutvikling, og lurer småsparere til å investere. Aktørene selger overprisede eiendommer til aksjeselskapene og sitter igjen med overskuddet. Et eksempel er Indigo Finans-saken, hvor selskapet slo seg konkurs i 2017. Straffesaken har pågått siden. Kravet til konkursboet er på rundt 33 millioner kroner. Imidlertid antas investorer og småsparere å ha investert nærmere 300 millioner kroner i selskapet over flere år.

RÅD FOR Å FORBYGGE DIGITAL KRIMINALITET

God digital hygiene og nett-vett er viktig. Gjør forebyggende tiltak for å sikre virksomhetens verdier!



STOPP – TENK – TRYKK

Videre viser man til tidligere nyhetsbrev fra næringslivskontakten i Nordland politidistrikt som omhandler konkrete råd for å forbygge overnevnte kriminalitet.

NÆRINGSLIVSKONTAKTEN I NORDLAND

Næringslivskontakten i Nordland skal arbeide 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 2021.
Tidligere nyhetsbrev fra næringslivskontakten i Nordland politidistrikt.
The No More Ransom Project:
https://www.nomoreransom.org/no/index.html
Norsk senter for informasjonssikkerhet (NorSIS):
https://norsis.no
Nasjonal sikkerhetsmyndighet (NSM):
https://nsm.stat.no
https://nettvett/investeringsbedrageri
Nordic Financial CERT.