POLITIET

Nyhetsbrev fra næringslivskontakten
Nordland politidistrikt

I denne utgaven:
- ✓ Polititets trusselvurdering for 2024.
- ✓ Trusler som næringslivet bør vie særlig oppmerksomhet

Foto politiet

Politiets trusselvurdering for 2024
Politiet utarbeider trusselvurderinger hvert år, og vi har et særlig ansvar for å kommunisere til sentrale samfunnsaktører hvilke trusler som kan true våre felles samfunnsverdier. Næringslivet er nettopp en sådan sentral aktør, og gjennom dette nyhetsbrevet ønsker jeg å kommunisere til næringslivet i Nordland hvilke trusler som i særlig grad truer næringslivet.

Gjennom denne informasjonen håper politiet på å bidra til å skape en felles forståelse for det trusselbildet vi står overfor, og danne grunnlag for forebyggende samhandling mellom private og offentlige aktører.

Tusler som næringslivet bør vie særlig oppmerksomhet

Cyberkriminalitet
Cyberkriminaliteten har stor geografisk spredning og rammer bredt. Kriminaliteten rammer virksomheter i form av eksempelvis datainnbrudd, datatyverier og løsepengevirus-angrep. Verdien på stjålet informasjon vurderes som økende. Små og mellomstore virksomheter er særlig utsatte.

Politiet erfarer en rekke endringer innen cyberkriminalitetsfeltet i 2023, særlig relatert til geopolitiske og teknologiske faktorer. De cyberkriminelle fortsetter å utvikle og tilpasse teknikker, metoder, verktøy og strategier, blant annet for å omgå mottiltak fra offentlige og private virksomheter. Samtidig er det observert flere likheter med foregående år. Majoriteten av de cyberrettede kriminelle lovbruddene i 2023 er fortsatt både opportunistiske og profittmotiverte. Ett lovbrudd kan imidlertid ha ulik motivasjon og verdi, eksempelvis profitt og samtidig etterretningsverdi for statlige aktører.

Politiets vurdering er at trusselen fra cyberkriminelle aktører er økende. Aktørene tilegner seg stadig mer kompetanse og kapasitet til å gjennomføre kriminalitet av økt kompleksitet og skadepotensial.

De siste årene har det skjedd en voldsom teknologisk utvikling, blant annet innen bruken av digitale verktøy. I dag er en stor del av både offentlige og private tjenester digitalisert, noe som gjør samfunnet sårbart for manipulasjon og utpressing. Teknologi og teknologisk utvikling er derfor en fundamental driver for cyberkriminalitet, og teknologien gir et økt handlingsrom for kriminelle aktører. Dette krever nye mottiltak fra lovgivere, offentlige aktører og private virksomheter.

Utviklingen innenfor både kunstig intelligens (KI) og anonymiseringsteknologi bidrar til å skape et utvidet handlingsrom for kriminelle. Kriminelle aktører benytter ulike digitale økonomiske tjenester som bidrar til anonymisering. Utviklingen innenfor kryptovalutamarkedet påvirker kriminelle aktørers mulighet til å gjennomføre ulovlige handlinger, som for eksempel hvitvasking og bedragerier, eller å skjule annen kriminell aktivitet.

Cyberkriminalitet krever ofte spesiell kompetanse, noe som har skapt et eget marked hvor tjenester og verktøy selges, kjøpes eller leies ut til kriminelle formål. Politiet observerer at dette markedet er stort og økende. Nyvinninger kommer raskt ut på det kriminelle markedet. Kriminelle har vist evnen til å ta lærdom av feil og er helt i front på å utvikle og bruke verktøy. Det mest prominente eksempelet på kriminalitet som handelsvare er *løsepengevirus*. Dette har utviklet seg til å bli en av de mest alvorlige sikkerhetsrisikoene for virksomheter i både offentlig og privat sektor.

Skillet mellom statlige og ikke-statlige cyberaktører blir stadig mer utvisket. Statlige aktører arbeider tett med private og offentlige cybersikkerhets- og teknologivirksomheter og hacktivist- grupper og cyberkriminelle. Hovedformålet med cyberoperasjoner fra statlige aktører er informasjonsinnhenting, herunder digital industrispionasje, samt å skape usikkerhet i samfunnet, men også for økonomisk vinning og transnasjonal undertrykkelse.

Nærmere om løsepengevirus
Løsepengevirus er skadevare som tradisjonelt sett blir benyttet til å kryptere fornærmedes data. Deretter kreves løsepenger for å låse opp datasystemene igjen. Angrepene skjer vanligvis ved at kriminelle som utvikler skadevaren, selger eller leier denne ut til andre kriminelle grupperinger, som bruker skadevaren til dataangrep mot en virksomhet. Målet er å få virksomheten som rammes, til å betale løsepenger.

I tillegg settes det ofte frem trusler om å selge data og sensitiv informasjon dersom løsepengene utbetales. Til slutt hvitvaskes utbyttet av andre kriminelle aktører gjennom flere ledd av vekslertjenester, noe som gjør det vanskelig å straffeforfølge. Det reelle omfanget av løsepengevirusangrep er usikkert. De siste to årene har det imidlertid vært noen færre anmeldte Løsepengevirus-angrep mot norske virksomheter. De fleste slike angrep er opportunistiske og motivert av vinning, men det er likevel observert angrep i 2022 og 2023 som tyder på større grad av kartlegging og målrettethet. Bedrifter som ikke har ressurser til – eller ikke har prioritert – å beskytte sine verdier tilstrekkelig, vil være spesielt sårbare for angrep. Ofte kan dette være små eller mellomstore bedrifter. Konsekvensene ved å bli utsatt for løsepengevirusangrep for den enkelte virksomhet kan derfor være betydelige. For noen kan det bety driftsstans og i verste fall konkurs.

Nærmere om datatyveri
Politiet har i 2023 observert en utvikling i utpressingsmodus blant enkelte kriminelle som har angrepet norske virksomheter. Som et ekstra ledd i utpressingen har gjerningspersoner utført datatyveri. I tillegg er det observert at gjerningspersoner har tatt kontakt med virksomheten via e-post og telefon for ytterligere utpressing. Samlet omtales dette som trippel utpressing. Det er også observert at kriminelle aktører publiserer stjålne data på det åpne nettet.

Dette kan utgjøre en økt risiko for gjentagende angrep, ved at den stjålne dataen er lett tilgjengelig for alle på internett og har kort nedlastingstid sammenlignet med data på det mørke nettet.
En annen type handelsvare er *påloggings-detaljer*. Disse er til salgs på markedsplasser på det mørke nettet, og kan brukes til datainnbrudd og annen kriminell aktivitet. Slike påloggingsdetaljer er mulig å stjele ved å bruke såkalt informasjonsstjelerskadevare, en type skadevare som det også handles med på det mørke nettet.

Nærmere om nulldagssårbarheter
En nulldagssårbarhet er et svakt punkt i en programvare som oppdages av angripere før forhandleren har blitt klar over det. Siden forhandleren ikke er kjent med svakheten, fins det ikke noe botemiddel mot dette, og angriperne vil ofte lykkes i sitt dataangrep.

En nulldagssårbarhet er også en handelsvare som kan kjøpes og selges på det mørke nettet, hvor en symbiose av hackere, kriminelle og etterretningstjenester opererer. Nulldagssårbarheter har begrenset levetid og har derfor svært høy verdi for kriminelle. Det kreves høy kompetanse og arbeid over tid for å utnytte nulldagssårbarheter, og derfor er dette også en ettertraktet handelsvare. Det siste året har politiet sett at kriminelle aktører har lyktes i å anskaffe programvare utviklet av statlige aktører, til bruk til kriminelle formål. På den måten blir avansert teknologi utbredt i kriminelle kretser, noe som også kan innebære en trussel mot kritisk infrastruktur.

Økonomisk kriminalitet
Digitaliseringen av samfunnet og integreringen av økonomier og arbeidsmarkeder øker mulighetene for grensekryssende økonomisk kriminalitet. Politiet ser at kriminelle organiserte nettverk har direkte eller indirekte kontroll over virksomheter og foretak, og det benyttes profesjonelle aktører og stråpersoner for å skjule kriminelle handlinger og eierskap. Samtidig trues deler av velferdsstatens finansieringsgrunnlag gjennom arbeidslivskriminalitet. Det er et vedvarende problem med svart avlønning og skjult omsetning på tvers av bransjer i arbeidslivet.

Både politiet og bankene registrerer en voldsom økning i antall bedragerier. Politiet forventer at bedrageri vil fortsette å øke i omfang. Bedrageri genererer stort utbytte til kriminelle aktører som benyttes til å finansiere ny kriminalitet. Flere siktede i norske bedragerisaker kan knyttes til organiserte kriminelle nettverk, som også er involvert i narkotika- og voldskriminalitet. Politiet forventer at bedrageri vil bli en enda viktigere inntektskilde for kriminelle miljøer i tiden som kommer.

Organisert kriminalitet
I Europa har trusselen fra organisert kriminalitet aldri vært høyere. Også i Norge er trusselen fra organiserte kriminelle betydelig. Flere sterkt profittmotiverte kriminelle nettverk opererer i Norge, og mange av disse er involvert i ulike former for bedrageri, samt i salg, distribusjon og innførsel av narkotika.

Organisert kriminell virksomhet kan resultere i både konflikter og samarbeid mellom kriminelle aktører. Politiet ser at flere av de organiserte kriminelle nettverkene i økende grad samarbeider med andre kriminelle. Slikt samarbeid blir spesielt tydelig der kriminelle kjøper og selger tjenester, oppdrag og spesialisert kompetanse. Slik kompetanse kan være alt fra transport og hvitvasking til vold og pengeinnkreving. Videre ser politiet at organiserte kriminelle aktører i økende grad søker å etablere legal næringsvirksomhet og/eller plassere utbytte fra kriminalitet inn i næringsvirksomhet for å hvitvaske dette. Ved å integrere den kriminelle virksomheten i den legale økonomien vil de kriminelle virksomhetene også kunne oppnå økt anerkjennelse og legitimitet.

Politiets vurdering er at trusselen fra organiserte kriminelle nettverk er betydelig og økende, blant annet på grunn av økt profesjonalisering, grensekryssende samarbeid og stadig mer komplekse forretningsmodeller.

Avslutning
Det er fortsatt lukrativt å rette kriminell aktivitet mot næringslivet. Privat næringsliv har også fått større betydning for nasjonal sikkerhet – sett i lys av den sikkerhetspolitiske og teknologiske utviklingen.

Man opplever en økt profesjonalisering fra de kriminelle. De behersker bruk av både sosial manipulering, moderne teknologi og komplekse verdikjeder for å gjennomføre bedrageriene.

For næringslivet blir det viktig å kartlegge virksomhetens verdier og relevante trusler, samt å iverksette adekvate tiltak for å redusere truslene.

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 trusselvurdering for 2024.
PSTs Nasjonale trusselvurdering for 2024.
NSM Risiko 2024.
DNB Trusler og trender fra et DNB-perspektiv.
Nordland politidistrikt. Kriminalitetsbildet og resultater for 2023.
Rostami & Mondani 2024. Kriminelle entreprenører – en studie av den organiserade brottslighetens kopplingar til næringslivet.