POLITIET

Nordland politidistrikt

Nyhetsbrev fra næringslivskontakten

Nordland politidistrikt

Utgitt: Juli, 2025

Foto politiet

Politiets trusselvurdering for 2025
Kriminalitetsbildet er i stadig endring. Kriminelle opererer sømløst på tvers av politidistriktsgrenser og landegrenser og utnytter både teknologi og strukturer i et samfunn preget av høy grad av tillit og digitalisering. Dette skaper sårbarheter som kriminelle nettverk og aktører drar nytte av, og det stiller høye krav til politiets og næringslivets evne til å tilpasse seg, utvikle nye metoder og ta i bruk ny teknologi.

Dette nyhetsbrevet retter seg i særlig grad mot næringslivet i Nordland, og bygger i all hovedsak på Politiets trusselvurdering for 2025 og på Nordland politidistrikts trusselvurdering for samme periode.

Dette nyhetsbrevet har som mål å bidra til å øke kunnskapen om utviklingen og de utfordringene næringslivet står ovenfor når det gjelder kriminalitet. Denne kunnskapsdelingen vil således bidra til å styrke vår felles evne til å forebygge kriminalitet rettet mot næringslivet i Nordland.

Økonomisk kriminalitet
Økonomisk kriminalitet omfatter eksempelvis bedrageri, skattesvik, korrupsjon, hvitvasking og arbeidslivskriminalitet. Både statens finanser, privatpersoner og næringsliv rammes av denne formen for kriminalitet, der formålet er økonomisk gevinst. Antall anmeldelser økte med 12 prosent fra 2023 til 2024, og dermed står økonomilovbrudd for den høyeste økningen fra 2023 til 2024.

Bedragerier utgjorde 85 prosent av økonomilovbruddene i 2024, opp fra 77 prosent i 2020. Til tross for denne stigningen antas det fortsatt å være mørketall på området. Rundt tre av fire anmeldte bedragerier var digitale.

Et titall av sakene omfatter korrupsjon, i all hovedsak begått av kommunalt ansatte som misbruker sine stillinger ved salg eller kjøp av varer og tjenester fra bedrifter mot betaling. Korrupsjon skjer både i privat og offentlig sektor, og har skadevirkninger utover det økonomiske. Det kan undergrave tilliten som borgerne har til statlige institusjoner, tjenestepersoner og prosesser. Personer i sentrale roller som lar seg bestikke, kan risikere å bli involvert i ytterligere kriminalitet.

Arbeidslivskriminalitet er brudd på et bredt spekter lover som gjelder norsk arbeidsliv. Kriminaliteten er gjerne organisert, virker konkurransevridende og undergraver viktige deler av samfunnet. Gjengangere innen arbeidslivskriminalitet begår ofte skatte- og avgiftskriminalitet i tillegg til konkurskriminalitet. Antall anmeldelser av hvitvasking har økt jevnt de siste årene. Utbytte må hvitvaskes for å kunne brukes og integreres i den legale økonomien, og man har registrert en økt bruk av pengemuldyr – dvs. at kriminelle truer eller betaler personer til å la dem disponere bankkontoene deres til hvitvasking.


Foto: Politiet.

Cyberkriminalitet
Cyberkriminalitet gjelder et bredt spekter av kriminalitet som strekker seg fra cyberrettet til cyberstøttet kriminalitet, og innebærer ethvert lovbrudd som begås med eller suppleres av informasjons- og kommunikasjonsteknologi, inkludert datasystemer, nettverk, enheter og programvare. Typiske lovbrudd innen cyberkriminalitet er datainnbrudd, tyveri av sensitiv informasjon, ulovlig deling eller salg av stjålne data, bruk av løsepengevirus for å presse ofre for penger, samt tjenestenektangrep for å forstyrre eller lamme digitale tjenester. Cyberrettet kriminalitet rammer datasystemer direkte, mens cyberstøttet kriminalitet er lovbrudd begått med støtte av datasystemer, eksempelvis

bedragerier, seksuallovbrudd mot barn eller distribusjon av narkotika.

Politiet er av den oppfatning at det kan være attraktivt å begå cyberkriminalitet i Nordland. Dette skyldes dels geografien og bosettingsmønsteret, dels regionens strategiske betydning for kritisk infrastruktur når det gjelder forsvar, romfart og transport.

Tyveri av sensitiv informasjon
I en globalisert og digitalisert verden er kunnskap ofte det største konkurransefortrinnet i næringslivet. Dette forsøker de kriminelle å utnytte, fordi urettmessig tilgang til andres sensitive informasjon kan gi dem stor økonomisk gevinst. De kan enten selge informasjonen til andre som har interesse av den, eller presse eieren av informasjonen for penger for ikke å selge den videre. Bedrifter som opererer i markeder med sterk konkurranse, samt bedrifter som sitter på kunders personopplysninger, vil være spesielt sårbare for denne formen for cyberkriminalitet.

Cyberkriminalitet har lenge vært en trussel mot næringslivet. Det har ført til at flere virksomheter har satset stort på ulike løsninger for cybersikkerhet, inkludert sikkerhetskopiering av sensitiv informasjon. Dette har hatt en positiv effekt, men flere kriminelle aktører har nå endret sin modus. Tidligere oppnådde de kriminelle stor effekt ved å kryptere ulike virksomheters informasjon, låse de ansatte ute fra sine egne data og kreve løsepenger for å oppheve krypteringen. Bedrifter omgår nå i noen grad denne trusselen ved at de lagrer informasjonen flere steder, med ulik sikkerhet. Enkelte cyberkriminelle har derfor gått over til å heller presse offeret for penger uten å låse ned og kryptere virksomhetens datasystemer. Dette foregår ved at de begår datainnbrudd og stjeler sensitiv informasjon som de så truer med å selge videre eller offentliggjøre med mindre offeret betaler løsepenger.

Kombinasjonen av stjålne data og offentlig tilgjengelig informasjon kan true både individer og nasjonale sikkerhetsinteresser.

Dette bildet er også i ferd med å forverres som følge av at kriminelle tar i bruk ny teknologi, som kunstig intelligens, som muliggjør enda mer presis og målrettet cyberkriminalitet.

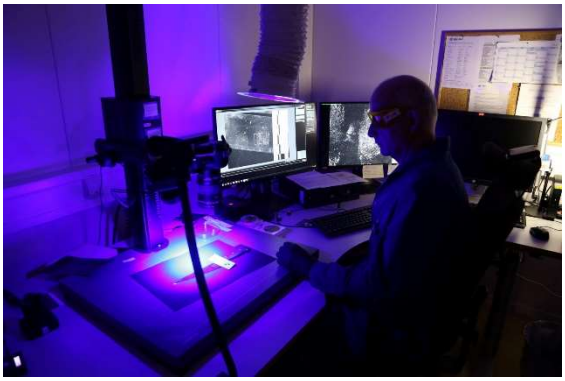
Foto: Politiet.

Cyberangrep mot virksomheter
Profittmotiverte kriminelle er fremdeles blant de største aktørene innenfor cyberkriminalitet, og er ofte forbundet med løsepengevirus. Sammen med datatyverier utgjør løsepengevirus en vesentlig og økende cyberkriminell trussel mot norske virksomheter og deres leverandørkjeder. Politiet er kjent med ofre over hele landet og i alle politidistrikt det siste året, og mørketallene er trolig store. Microsoft rapporterer om en nær tredobling i antall angrepsforsøk med løsepengevirus globalt i 2024. Landegrenser er ingen hindring i denne sammenhengen. Små og mellomstore bedrifter er særlig utsatt, da de ofte er mer sårbare og minst rustet til å håndtere konsekvensene av et slikt virusangrep. Disse bedriftene kan være viktige leverandører og underleverandører til virksomheter som råder over kritisk infrastruktur og understøtter grunnleggende nasjonale funksjoner.

Politiet har det siste året observert angrep både mot ulike deler av virksomheters verdikjeder og mot samarbeidende tredjeparter. Cyberrettede verdikjedeangrep skjer når noen uten tillatelse tilfører egenskaper til eller endrer deler av et produkt for å utnytte dette senere. Slike endringer kan skje i alle ledd av verdikjeden, enten via programvare, maskinvare eller systemdokumentasjon. Verdikjedeangrep

retter seg mot produkter under utvikling, mens tredjepartsangrep går via leverandører eller underleverandører for å ramme flere virksomheter.

Lange og uoversiktlige leverandørkjeder utgjør en sårbarhet som trusselaktører utnytter. Alvorlig svikt i IKT-systemer kan i verste fall true den finansielle stabiliteten og påvirke samfunnssikkerheten. Cyberkriminelles trusler mot leverandørkjeder samt små og mellomstore bedrifter i Norge, forventes å bli mer målrettede. Skadeomfanget forventes også å bli større, i likhet med utfordringene med å få sikret kritiske verdier og tjenester. Angrep via tredjepart forventes å fortsette å øke da mange virksomheter har integrerte systemer med underleverandører eller andre samarbeidspartnere som kan angripes og utnyttes av trusselaktørene.

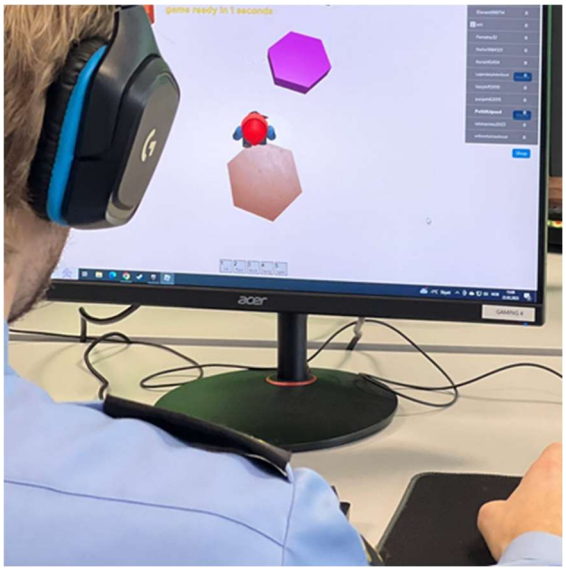

Foto: Politiet.

Forventet utvikling

Norske virksomheter står overfor en stadig mer sammensatt og krevende trussel i det digitale rom. Virksomheter utsettes for alt fra løsepengevirus og bedragerier til tap av sensitiv data som også kan føre til juridiske og forretningsmessige implikasjoner. Kravet til egensikring er høyt, og ofte er utfordringene de samme for små, mellomstore og store virksomheter. Selv om det ikke er praktisk mulig å sikre virksomheter fullstendig, er grunnleggende forebygging, bevissthet og god sikkerhetshygiene ofte effektivt i å forhindre kriminell utnyttelse.

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 2025
Nordland politidistrikts trusselvurdering for 2025. .
PSTs Nasjonale trusselvurdering for 2025.
NSM: Risiko 2025.
Kripos: Cyberkriminalitet 2025.