



POLITIET

Nyhetsbrev fra næringslivskontakten **Nordland politidistrikt**

I denne utgaven:

- ✓ Politimesterens signaler til næringslivet.
- ✓ Den seneste utviklingen innen cyberkriminalitet.
- ✓ Julen er høysesong for cyberangrep.
- ✓ Arbeidslivskriminalitet.
- ✓ Kontanter i den kriminelle økonomien.



Politimesterens signaler til næringslivet

«Trusselnivået mot oss har økt, og vi må være årvåkne» var hovedbudskapet til politimester Heidi Kløkstad om påvirkning fra fremmede makter - og da Russland i særdeleshet - på en konferanse i Bodø tidligere i høst. Nordland er en viktig del av nordområdene, med tett konsentrasjon av militære anlegg og installasjoner.



Politimester Heidi Kløkstad. Foto: politiet.

Politimesteren ba næringslivet være ekstra oppmerksomme fordi de både representerer store verdier og sitter på avansert teknologi. Hun nevnte flere eksempler på hvordan fremmede makter forsøker å påvirke oss gjennom hybride trusler:

- Digitale angrep.
- Styrt migrasjon.
- Skadeverk og sabotasje på infrastruktur.
- Fake news.
- Eiendomsoppkjøp.

Politimesteren ba videre næringslivet om å kontakte PST Nordland og/eller lokalt politi dersom de sitter inne med informasjon som bør undersøkes nærmere.

Den seneste utvikling innen cyberkriminalitet

Utviklingen innen cyberkriminalitet er preget av en generell teknologisk utvikling. Små tekniske forbedringer i skadevare, nye teknikker som automatiserer og forenkler

prosesser eller nye metoder for å unngå deteksjon vil – dersom utviklingen fortsetter – kreve nye metoder og tiltak fra lovgivere, politiet, og private og offentlige virksomheter. Flere av disse forholdene vil kunne få betydning for grunnleggende nasjonale funksjoner og norske interesser.

Politiet har erfart at cyberkriminelle går lengre i sin virkemiddelbruk, spesielt når det gjelder løsepengevirusangrep. Det er meget sannsynlig at cyberkriminelle vil fortsette å ta i bruk nye kreative virkemidler for å legge ytterligere press på norske virksomheter.

Politiet har registrert en utvikling hvor flere løsepengevirusaktører gjennomfører datatyveri uten kryptering. Dette er sannsynligvis et resultat av økt sikkerhetskultur- og bevissthet i virksomheter, herunder bedre rutiner for sikkerhetskopiering, samt en økt forståelse for verdien av informasjon blant de kriminelle. Denne utviklingen bidrar meget sannsynlig til å endre behovet for verktøy og kompetansekrav for løsepengevirusaktører, fra kryptering og dekryptering til aksessetablering.

Et gjennomgående trekk ved trusselbildet i det digitale rom er at skillet mellom statlig og kriminell aktør er uklart. Finansielt motiverte cyberkriminelle, ideologisk motiverte hacktivist, og statlige aktører har alle direkte eller indirekte interesse av å ramme norske virksomheter.



Foto: politiet

Flere hendelser har vist at cyberkriminelle har evne til å utnytte både gamle teknologiske sårbarheter som ikke er utbedret, og nye

sårbarheter etter hvert som de blir kjent eller oppstår. Hendelsene viser videre at cyberkriminelle evner å utnytte nulldagssårbarheter - dvs. sårbarheter som er ukjente for produsenten og brukeren. Å finne og utnytte nulldagssårbarheter krever høy kompetanse og arbeid over tid, selv om dette kan dempes gjennom å kjøpe seg tilgang til relevante sårbarheter. Nulldagssårbarheter kan ofte kun benyttes én gang og har derfor svært høy verdi for cyberkriminelle.

Julen er høysesong for cyberangrep

Politiet har tidligere år registrert en økning av cyberangrep rettet mot norske virksomheter i desember og inn mot jul. God beredskap og tydelige planer for ferien tar imidlertid ned risikoen for cyberangrep med alvorlige konsekvenser.

Beredskap er billigere enn å rydde opp etter cyberangrep. Ofte er det ikke mye som skal til for å bedre sikkerheten for virksomheter flest. Svake passord og teknisk gjeld er og forblir norske virksomheters mest sårbare punkter. Det er det mulig å gjøre noe med, sier Albert-Hoff, leder av Nasjonalt cybersikkerhetssenter i Nasjonal sikkerhetsmyndighet (NSM).

NSM gir tre konkrete råd for digital beredskap gjennom julen:

- Sjekk at kriseplanene dine er oppdatert. Lag en oversikt over ansatte som er eller kan være tilgjengelige om det skulle oppstå en hendelse. I tilfelle en digital krise er ansatte med teknisk kompetanse, kommunikasjonsmedarbeidere og ledelse sentrale.

- Gå gjennom grunnleggende sikkerhetstiltak i virksomheten. Dobbeltsjekk at flertrinnslogging og sterke passord er på plass.

- Minn alle ansatte om at julen er høysesong for forsøk på digital utpressing, phishing og andre dataangrep.

Virksomheter som opplever uregelmessigheter oppfordres til å varsle Nasjonalt cybersikkerhetssenter. Alle varsler

bidrar til at NSM kan bygge et godt situasjonsbilde av betydning for nasjonal sikkerhet.

Arbeidslivskriminalitet

Nordland statsadvokatembeters rapport av 30. august 2023 viser at utenlandske arbeidstakere har høyere risiko for å utsettes for arbeids- og dødsulykker på jobb i Norge.

I undersøkelsen har statsadvokatene sett nærmere på 24 arbeidsulykker i fylket. I 3 av 24 saker er fornærmede død. Her kommer det fram tydelige funn som gir grunn til bekymring:

- 37 % av de fornærmede i arbeidsulykkene er utlendinger.
- 3 av 24 arbeidsulykker endte med dødsfall og alle de omkomne var utlendinger.
- 37 % av de fornærmede var ikke ansatt i bedriften der ulykken fant sted – de var på jobb for en underentreprenør, leverandør eller samarbeidspartner. Av disse var 23 % enten i opplæringsstilling eller på en form for tiltak.

Statsadvokatene i Nordland, Arbeidstilsynet og senterleder for a-krimssenteret i Nordland oppfordrer næringen til å ta nødvendig grep for å forebygge at ulykker skjer.

Førstestatsadvokat Hilde Stoltenberg opplyser at den viktigste forbyggende faktoren er at arbeidsgivere sørger for trygge arbeidsplasser for alle.

Det er arbeidsgivers klare og lovpålagte plikt å sørge for et fullt ut trygt og forsvarlig arbeidsmiljø for sine ansatte.

– Vi har sett over år at utenlandske arbeidstakere er overrepresentert når det gjelder arbeidsrelaterte skader og dødsfall, både nasjonalt og internasjonalt. Dette skyldes blant annet risikofylte jobber, språkproblemer, dårlig opplæring og mangel på barrierer eller verneutstyr, sier seksjonsleder Trond Henry Skjønfsjell i Arbeidstilsynet.

Det er viktig at arbeidsgivere tar dette ansvaret på alvor og jobber systematisk med å

forebygge at arbeidstakere skader seg eller dør på jobb.

Leder for A-krimssenteret i Nordland, Kurt Kolvereid Jacobsen bekrefter at de ser det samme gjennom sin kontrollvirksomhet. – Vi ser dessverre ofte at det slurves med HMS på bekostning av arbeidstakernes sikkerhet. Mangelfull eller ingen opplæring i bruk av arbeidsverktøy eller at arbeidstakere utfører arbeidsoppgaver som medfører fare for liv og helse er slett ikke uvanlig, sier Jacobsen, som leder Skatteetaten, NAV, Arbeidstilsynet og Politiet sin felles innsats mot arbeidslivskriminalitet i Nordland.

Rapporten peker på at mange av de fornærmede er sårbare - enten fordi de er utenlandske, står i opplæringsstilling eller er på jobb for en underleverandør. Det kan således være grunn for arbeidsgiverne/ virksomhetene til å rette forebyggende tiltak inn mot disse gruppene.

Kontanter i den kriminelle økonomien

En ny rapport fra Økokrim viser at den kriminelle økonomien fortsatt er kontantbasert. Rapporten peker på at store summer norsk valuta har blitt transportert ut av landet for å hvitvaskes. I snitt har 27 millioner norske kroner blitt transportert ut av landet hver dag. Dette til tross for at norske kroner ikke er spesielt anvendelig i utlandet. Bare en brøkdel deklarerer, resten smugles ut.



Foto: politiet

Selv om den registrerte bruken av kontanter i samfunnet har gått ned og de fleste nå velger digitale betalingsløsninger, er den nominelle verdien av den norske kontantbeholdningen i

dag om lag den samme som i 1996, på rundt 40 milliarder kroner.

Det er grunn til å tro at en stor andel av kontantbeholdningen i dag benyttes i den kriminelle økonomien. Bare i 2022 ble det transportert ut av landet rundt 8 milliarder kroner.

Politiet arbeider for å styrke samarbeidet med finansnæringen, offentlige etater og internasjonale partnere med det formål å styrke kontrollen over den kriminelle økonomien, forhindre hvitvasking og finansiering av terror.

NÆRINGS LIVSKONTAKTEN 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:

Nå er det NOK. Kontanter i den kriminelle økonomien. Økokrim, 2023.

Cybersum – 002 september 2023, Kripas.

Kilden, 29. september 2023.

En gjennomgang av arbeidsulykkesaker i 2022 for Nordland.

Nordland statsadvokatembeter. Rapport av 30. august 2023.

NSM, Cyberangrep i høytiden, publisert 7.12.2023.