POLITIET

Norwegian Police

Informasjon fra Oslo politidistrikt Distribusjonskode: Kan deles med egen virksomhet

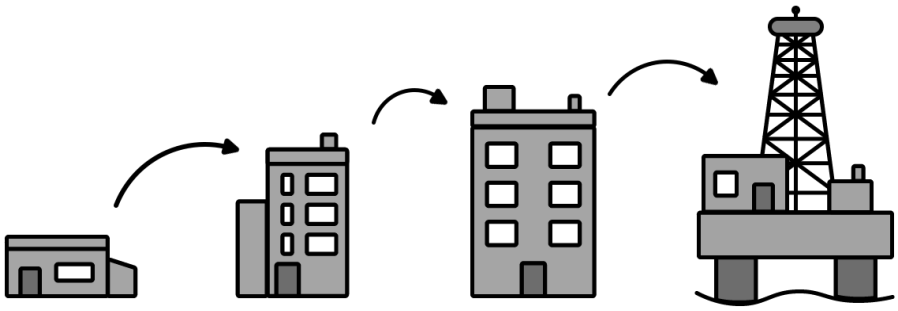
Fra: Næringslivskontakt/politiinspektør Christina T. Rooth, Oslo politidistrikt Dato: 18.1.23

Orientering til næringslivet om sikkerhetssituasjonen

Krigen i Ukraina har ført til en stadig mer spent sikkerhetssituasjon i Europa. Norske myndigheter har ikke grunn til å tro at Russland vil ønske å involvere Norge, eller noe annet land, direkte i krigføringen. Det er ingen konkrete fysiske trusler mot Norge. Politiet oppfordrer likevel alle til å tenke nøye gjennom hvordan sikkerhetssituasjonen påvirker deres virksomhet.

Et grunnleggende råd er å få oversikt over virksomhetens verdier og sårbarheter, og hvilke trusler som eventuelt er aktuelle for din virksomhet. Det er også viktig å tenke gjennom hvilken rolle din virksomhet spiller i et større samfunnsperspektiv.

Er dere et ledd i en leverandørkjede, som igjen kan få påvirkning for virksomheter som er kritisk viktige eller spesielt utsatt i dagens trusselbilde?



En sårbarhet et sted kan få store konsekvenser et helt annet sted

Trusselbildet

De åpne trusselvurderingene fra Etterretningstjenesten (ETJ), Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM) gir et godt bilde av trusselsituasjonen mot næringslivet i Norge. PST vurderer at etterretningstrusselen fra Russland er høyere nå enn den var før invasjonen, blant annet på bakgrunn av omfattende sanksjoner og dermed et forsterket behov for varer, teknologi og tjenester for Russland. Dette kan gi seg utslag i forsøk på ulovlig informasjonsinnhenting mot ulike sektorer, både gjennom menneskelig innhenting og nettverksoperasjoner.

Aktører innenfor forsvar og beredskap, norsk petroleumssektor og understøttende infrastruktur vurderes av PST til å være særlige utsatte mål for russisk etterretning. Teknologiselskaper med produkter som vil bli mangelvare i Russland på grunn av sanksjonene vurderes også som utsatte etterretningsmål. For øvrig vil alle virksomheter som utfører noe av betydning for Ukraina og Russland kunne være aktuelle mål for russisk etterretning.

OSLO POLITIDISTRIKT
Post: Postboks 2093 Vika, 0125 Oslo / (+47) 22 66 90 50
post.oslo@politiet.no / www.politiet.no / 961 398 142

Aktuelle fremgangsmåter for fremmed etterretning

I PSTs åpne trusselvurdering trekkes det spesielt frem fire fremgangsmåter fremmed etterretning typisk vil benytte i sin virksomhet - rekruttering, digitale angrep, kartleggingsvirksomhet og fordekte anskaffelser.
Nedenfor følger punkter virksomheter bør være oppmerksomme på innenfor disse fremgangsmåtene, samt forslag til tiltak.

1. Rekruttering og manipulering

Rekruttering av kilder på innsiden av norske virksomheter er en prioritert oppgave for russisk etterretning. Spesielt i virksomheter av interesse for Russland.

Hva bør en være oppmerksom på:

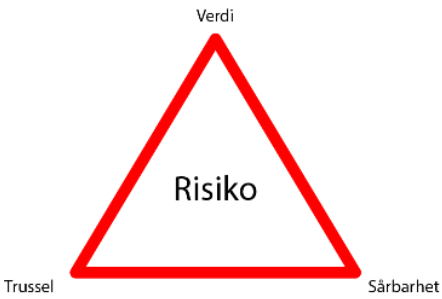
- Både nordmenn og ansatte fra andre land kan bli utsatt for rekrutteringsforsøk.
- Personer med nære relasjoner til Russland kan bli forsøkt presset eller truet til å samarbeide med hjemlandets sikkerhets- og etterretningstjenester.
- Åpne konferanser er en vanlig arena som etterretningstjenester benytter for å identifisere kilder de ønsker å rekruttere.
- Delegasjoner fra land Norge ikke har sikkerhetspolitisk samarbeid med kan bli brukt til å utføre etterretningsoppdrag.

Tiltak:

- Sørg for at dine ansatte er kjent med virksomhetens verdier og potensielle trusler mot disse.
- Ha klare varslingsrutiner.
- Snakk med ansatte som kan være særlig trusselutsatte og bygg tillit.

2. Digitale angrep

NSMs nasjonale oversikt over hendelser og forsøk på digitale angrep viser en betydelig økning i aktivitet mot norske virksomheter det siste året. Ifølge NSM har de fleste virksomhetene som har samfunnsviktige funksjoner, gode interne krav til forsvarlig sikkerhet. Men sikkerheten er ikke alltid like god bakover i verdikjedene, for eksempel hos leverandører og konsulenter. Det er flere eksempler på at underleverandører rammes av digitale angrep, og at dette igjen kan få konsekvenser for samfunnsviktige funksjoner. Det er derfor viktig å ha en helhetlig oversikt over verdiene sine, sårbarhetene og trusselen – også mot verdikjedene.



Hva bør en være oppmerksom på:

- Innsidetrussel og forsøk på sosial manipulasjon der ansatte blir en inngang til virksomhetens systemer.
- Virksomhetens digitale systemer vil alltid ha sårbarheter som kan utnyttes.
- Virksomheter som er en del av verdikjeden innenfor teknologi, forskning og utvikling og offentlig forvaltning og departementer vurderes å være spesielt utsatt fremover.

Tiltak:

- Vit hva du har – skaff deg oversikt. Hvilke verdier har du, hvilken avtale har du med dine leverandører, vit også hva du ikke vet.
- Bygg god sikkerhetskultur og ha sikkerhet fast på agendaen. Implementer den digitale sikkerheten inn i det generelle sikkerhetsarbeidet, slik at dette ikke er adskilt og gi god opplæring og informasjon til ansatte.
- Benytt totrinnsbekreftelse på alle digitale innlogginger, og sørg for at alle brukere har sterke unike passord.
- Sørg for å holde maskiner og programmer oppdatert og installer sikkerhetsoppdateringer så raskt som mulig. Slå av eller koble fra maskiner som ikke er i bruk.
- Administratorrettigheter bør begrenses, og fjern brukere og tilganger dere har som ikke er nødvendige.
- Ta sikkerhetskopi av data bedriften er avhengig av for å kunne fungere.

3. Kartleggingsvirksomhet

Russisk etterretning har tradisjon for å innhente informasjon om, og kartlegge norske forsvarsinstallasjoner og kritisk infrastruktur. Informasjon som i verste fall kan benyttes til å tilrettelegge for sabotasje, men også være ledd i å villede eller skape utrygghet rundt norsk leveranseevne.

Hva bør en være oppmerksom på:

- Tilreisende «turister» som fotograferer eller filmer sensitive forsvarsinstallasjoner eller samfunnskritisk infrastruktur ved hjelp av håndholdte kamera eller ved bruk av droner, kan være på oppdrag for hjemlandets etterretningstjeneste.
- Andre mistenkelige observasjoner.
- Vær spesielt oppmerksomme på russiske kjøretøy.

Tiltak:

- Ved observasjon av mistenkelig kjøretøy, noter registreringsnummer og eventuelle særtegn som for eksempel antenner og annet synlig elektronisk utstyr.
- Om mulig forsøk å få ID på mistenkelige personer.

4. Fordekte anskaffelser

En rekke stater er villig til å gå langt, inkludert bruke ulovlige virkemidler for å skaffe teknologi og kunnskap. De vil benytte seg av lovlige virkemidler som oppkjøp og investeringer, og andre ulovlige virkemidler som innbrudd i datanettverk og fordekte anskaffelser for å omgå eksportkontrollregelverket.

Hva bør en være oppmerksom på:

- Bestillinger som er uvanlige med hensyn til antall eller mengde, eller der du mottar lignende bestillinger fra flere aktører.

Tiltak:

- Bruk av stråselskaper kan gjøre det vanskelig å se hvem som egentlig handler. Vær oppmerksom der du får begrenset informasjon om kjøper eller sluttbruker. Be om sluttbrukererklæring.
- Aktører knyttet til Russland, Kina, Iran og Pakistan vil representere en særskilt utfordring.

Annet

Hva bør en være oppmerksom på:

- Oppkjøp av strategisk plasserte eiendommer, for eksempel i nærheten av kritisk infrastruktur.

Varsling til politiet

Det er viktig at politiet varsles umiddelbart om hendelser som pågår

- Dersom det er mulig, og politiet har kapasitet, vil vi følge opp henvendelser operativt ved å sende en patrulje til stedet.
- Dersom det er mulig, og ved kapasitet, vil vi også følge opp henvendelser om digitale angrep ved å sende en patrulje/team til stedet (om den rammede virksomheten ønsker dette).

1. Nød: 1 1 2 (fare for liv, helse og miljø)
2. Oslo politidistrikt: 02800/22 66 90 50, døgnbemannet
3. Politiets nasjonale cyberkrimsenter: 23 20 80 00, døgnbemannet
4. Økokrim: 23 29 10 00, telefon åpent fra kl. 8 – 15
5. PST: 23 30 50 00, døgnbemannet
   Tips til PST: https://www.pst.no/tips-oss/
6. Informasjon om observasjon, tips mv. som har skjedd
   Meld fra om mistenkelige hendelser. For melding om observasjoner, aktivitet, digitale forsøk mv. som har skjedd kan "Tips politiet" benyttes
   Velg skjema for generelle tips; https://tips.politiet.no/web
   Velg skjema for datakriminalitet: https://www.politiet.no/rad/datakriminalitet/

Viktige ressurser

Kontaktinformasjon til næringslivskontakt i Oslo politidistrikt
christina.rooth@politiet.no

Oversikt over næringslivskontakter i andre politidistrikt
https://www.politiet.no/kontakt-politiet/naringslivskontakter/

Henvisninger til annen relevant informasjon

Politiets sikkerhetstjenestes nasjonale trusselvurdering 2022
https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2022/

Etterretningstjenestens trusselvurdering «Fokus 2022»
https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus

Politiets trusselvurdering 2022
https://www.politiet.no/om-politiet/tall-og-fakta/politiets-trusselvurdering/

Nasjonal sikkerhetsmyndighets «Digitalt risikobilde 2022»
https://nsm.no/aktuelt/digitalt-risikobilde-2022-cyberangrep-har-blitt-hverdagskost

Nasjonal sikkerhetsmyndighet sine grunnprinsipper for digital sikkerhet
https://nsm.no/grunnprinsipper/

Oslo politidistrikt sin enkle informasjon om hvordan du skal beskytte bedriften din mot datainnbrudd og digital utpressing
https://www.politiet.no/globalassets/dokumenter/oslo/naringslivskontakten---forebyggende/datainnbrudd-og-digital-utpressing.pdf

Politiets lille brosjyre om datasikkerhet
https://www.politiet.no/globalassets/03-rad-og-forebygging/datakriminalitet/den-lille-brosjyren-om-datasikkerhet-no.pdf

Næringslivets sikkerhetsråd (NSR) har laget en enkel nødplakat som kan benyttes ved digitale angrep
https://www.nsr-org.no/aktuelt/nodplakat

Politiet, PST, NSM og NSR sin veileder for sikkerhet ved ansettelsesforhold
https://www.pst.no/globalassets/artikler/utgivelser/sikkerhet_ved_ansettelsesforhold_2017_utskrift.pdf

Informasjonsside fra norske universiteter, høyskole og forskningsvirksomheter
https://www.sikresiden.no/

Næringslivets sikkerhetsråd (NSR) Leadership Guideline The war in Ukraine
https://www.nsr-org.no/uploads/documents/Publikasjoner/Lederveiledning-omsorg-for-ansatte.pdf

Økokrims trusselvurdering 2022
https://www.okokrim.no/oekokrims-trusselvurdering-2022.6527255-549350.html

Nasjonal risikovurdering 2022
https://www.okokrim.no/nasjonal-risikovurdering-2022.6567231-549350.html