Beskyttelse av norsk teknologi

Beskyttelse av norsk teknologi: Trusler mot norsk industri i en urolig tid

Den nylig publiserte kronikken i Teknisk Ukeblad (https://deksa.no/nyhet/kronikk-eksport-av-sensitiv-teknologi-i-en-urolig-tid/) og tidligere informasjon fra PST (https://www.pst.no/alle-artikler/artikler/ulovlige-anskaffelser-og-indikatorer/) belyser de økende sikkerhetsutfordringene knyttet til eksport av sensitiv teknologi i en tid preget av geopolitisk uro. Den globale sikkerhetssituasjonen har endret seg fundamentalt, og Norge står overfor nye trusler mot teknologi, næringsliv og akademia. Selskaper som utvikler strategisk viktig teknologi har blitt attraktive mål for både statlige og ikke-statlige aktører, og dagens trusselbilde krever større årvåkenhet enn noensinne.

En teknologisk ressurskamp

Norske selskaper som arbeider med forsvarsteknologi, kunstig intelligens, sensorteknologi, romfart og halvlederteknologi befinner seg i en industriell ressurskamp. Globale makter ønsker tilgang til denne teknologien, enten for økonomisk vinning eller for strategisk maktfordeling. Teknologi som tidligere ble ansett som sivil, kan i dag brukes i militære sammenhenger, og grensen mellom sivil og militær anvendelse har blitt mer flytende.

Flere nasjoner bruker omfattende ressurser på industrispionasje for å tilegne seg strategisk teknologi. Norske selskaper kan være utsatt for både tradisjonelle spionasjemetoder, som menneskelig rekruttering, og moderne cyberangrep som gir aktører tilgang til sensitiv informasjon uten fysisk tilstedeværelse. PST har særlig advart mot forsøk på å utnytte teknologiutvikling gjennom mellommenn, forskningssamarbeid eller skjulte nettverk av selskaper.

Kompleksiteten i globale verdikjeder

Norsk næringsliv opererer i stadig mer komplekse verdikjeder, hvor teknologiske produkter og tjenester kan passere gjennom flere ledd før de når sluttbrukeren. Dette skaper utfordringer med å verifisere hvem som til syvende og sist får tilgang til kritisk teknologi. Når produkter eksporteres, kan de omdirigeres eller videreselges uten at produsenten har kontroll over sluttkunden. Dette gjør det vanskelig å sikre at teknologien ikke havner hos aktører som kan bruke den til destruktive formål.

Eksportkontroll er et viktig verktøy for å redusere risikoen for at norske varer, teknologi og kunnskap misbrukes. Likevel er det den enkelte virksomhet sitt ansvar å forstå hvorvidt deres produkter er underlagt eksportkontrollregelverket. Norske myndigheter, med DEKSA i spissen, gir veiledning, men de avhenger av at selskaper selv er proaktive i å identifisere potensielle sårbarheter.

Sanksjoner og risiko for brudd på regelverket

De omfattende sanksjonene mot Russland har hatt store konsekvenser for norsk næringsliv. Mange selskaper opplever utfordringer med å navigere i et stadig mer komplekst sanksjonsregime, hvor feilaktige transaksjoner kan føre til alvorlige juridiske og økonomiske konsekvenser. Et økende antall selskaper har blitt rammet av restriksjoner uten nødvendigvis å ha vært klar over risikoen.

Det er viktig å forstå at sanksjoner ikke bare gjelder direkte handel med sanksjonerte land, men også indirekte transaksjoner gjennom tredjeparter. Noen aktører forsøker å omgå sanksjonene ved å bruke selskaper i nøytrale land som mellomledd. Norske selskaper kan dermed uvitende bli en del av slike nettverk dersom de ikke har tilstrekkelig kontroll over sine handelsforbindelser.

Cyberangrep og digital etterretning

Cyberangrep er en av de største truslene mot norske virksomheter i dag. Statlige aktører og organiserte kriminelle grupper bruker avanserte teknikker for å infiltrere IT-systemer, hente ut sensitiv informasjon og sabotere virksomheter. Slike angrep kan ta form av:

- Sofistikerte phishing-angrep, der ansatte manipuleres til å oppgi passord eller åpne ondsinnede vedlegg.
- Zero-day-angrep, hvor angripere utnytter sårbarheter i programvare før de blir kjent for produsenten.
- Ransomware-angrep, hvor systemer låses ned og løsepenger kreves for å gjenopprette tilgangen.
- Leverandørkjedeangrep, hvor en tredjepartsleverandør kompromitteres for å gi angripere tilgang til sluttbrukeren.

For norske teknologiselskaper er cybertrusselen særlig alvorlig, da mange av dem utvikler eller håndterer informasjon av høy strategisk verdi. Mange aktører innen sensor- og deteksjonsteknologi, halvlederindustrien og rom- og satellitteknologi har allerede opplevd forsøk på datainnbrudd fra utenlandske trusselaktører.

Ulovlige anskaffelser og skjulte metoder

PST advarer om at enkelte aktører forsøker å anskaffe teknologi på ulovlige måter, ofte gjennom mellomledd eller dekkfirmaer. Noen av metodene inkluderer:

- Bruk av mellommenn: Kunder som insisterer på å bruke ukjente tredjeparter for kjøp og transport kan indikere en skjult sluttbruker.
- Vage sluttbrukererklæringer: Når kunden er motvillig til å gi opplysninger om hvor utstyret skal brukes eller hvordan det skal installeres.
- Endringer i etablerte kundeforhold: Når en eksisterende kunde plutselig begynner å be om varer som er utenfor deres normale forretningsområde.
- Bruk av offshore-lokasjoner: Når et spedisjonsfirma, havn eller lager blir oppgitt som endelig destinasjon uten en klar sluttbruker.

Bruk av fiktive selskaper: Når informasjon om kunden er vanskelig å verifisere, det finnes ingen kredittopplysninger eller selskapet har kun en postboksadresse.

Økende krav til sikkerhetsbevissthet

Både kronikken fra Teknisk Ukeblad og PSTs informasjon understreker behovet for at norske selskaper tar en mer aktiv rolle i egen sikkerhet. Mens myndighetene gir veiledning og håndhever regelverk, er det næringslivet selv som må oppdage og håndtere truslene i sin daglige drift.

I møte med dette landskapet er det viktigere enn noen gang at norske selskaper forstår hvordan trusselaktører opererer og hvilke tegn de må se etter for å unngå at deres teknologi blir misbrukt. Bedrifter må være oppmerksomme på hvilke aktører de samarbeider med, hvilken informasjon de deler, og hvilke sikkerhetstiltak de har på plass for å beskytte sin virksomhet.

Konklusjon

Norge er en teknologisk stormakt innenfor flere sektorer, og dette gjør norske selskaper attraktive mål for spionasje, cyberangrep og ulovlige anskaffelser. Den globale sikkerhetssituasjonen krever at selskaper tar en mer proaktiv tilnærming til sikkerhet, enten det gjelder eksportkontroll, digitale trusler eller fysisk sikring av teknologi.

For at norsk næringsliv skal forbli konkurransedyktig og trygt, må det bygges opp en større sikkerhetsbevissthet i alle ledd av organisasjonen. Árvakr bistår selskaper med å forstå hvordan disse truslene opererer og hvilke tiltak som kan iverksettes for å redusere risikoen. Gjennom risikoanalyser, implementering av sikkerhetsmekanismer, sikkerhetstrening og rådgivning hjelper Árvakr bedrifter med å styrke sin forsvarsevne mot ulike typer angrep.

Med økt samarbeid mellom næringsliv, akademia og myndigheter, samt støtte fra sikkerhetsaktører som Árvakr, kan Norge styrke sin motstandskraft mot de truslene som preger dagens globale landskap.