Nordkoreanske IT-arbeidere er fordekt ansatt i norske bedrifter

Introduksjon

Politiets sikkerhetstjeneste (PST) har det siste året blitt kjent med flere tilfeller hvor norske virksomheter har blitt rammet av aktivitet fra nordkoreanske aktører. Disse virksomhetene har blitt lurt til å ansette det som sannsynlig er nordkoreanske IT-arbeidere i stillinger på hjemmekontor.

Aktiviteten knyttes til en kampanje som har gått over flere år hvor nordkoreanske IT-arbeidere, ved hjelp av falske eller stjålne identiteter, ansettes i vestlige virksomheter på hjemmekontor. Virksomhetene har ikke selv hatt kjennskap til jobbsøkernes opprinnelsesland. Lønnsinntektene nordkoreanske ansatte mottar gjennom slike stillinger, går trolig til å finansiere landets våpen- og atomvåpenprogram. Aktiviteten befinner seg dermed i en gråsone mellom statssponset kriminell aktivitet og statlig etterretningsvirksomhet.

Denne kortrapporten redegjør for modus for denne aktiviteten.

Nordkoreansk cyberaktivitet

Nord-Korea har over tid utviklet sine cyberkapabiliteter betydelig, og representerer i dag en vesentlig trussel mot norske mål. Det er enkelte kjennetegn ved nordkoreansk cyberaktivitet som skiller seg fra tradisjonell cyberetterretning fra andre statlige aktører.

For det første er et av hovedformålene med nordkoreansk cyberaktivitet økonomisk vinning. Det nordkoreanske regimet bruker cyberoperasjoner for å omgå sanksjonsregimet og finansiere sitt atomvåpenprogram. På bakgrunn av dette rammer nordkoreansk aktivitet også virksomheter som ikke tradisjonelt vurderes som prioriterte etterretningsmål, eksempelvis bedrifter som besitter større mengder kryptovaluta.

For det andre kjennetegnes nordkoreanske cyberaktører av at de er hurtige og kreative når det kommer til valg og videreutvikling av teknikkene de benytter. Dette ser vi eksempelvis i deres anvendelse av teknikker som tradisjonelt assosieres med kriminelle cyberaktører slik som løsepengevirus.

For det tredje indikerer observert aktivitet i vestlige land at nordkoreanske aktører operer med en meget høy risikovilje. De fokuserer eksempelvis lite på å unngå at de etterlater tekniske spor som brukes for å attribuere aktivitet til Nord-Korea i etterkant av en cyberoperasjon. Fokuset er hovedsakelig på å oppnå formålet ved den enkelte operasjonen, uavhengig av eventuelle konsekvenser hvis dette blir oppdaget i etterkant.

Disse kjennetegnene observerer vi også i den nordkoreanske aktiviteten i Norge, som er tema for denne rapporten. Aktiviteten er en del av en større kampanje hvor nordkoreanske aktører utnytter økt bruk av hjemmekontor hos vestlige virksomheter. Disse virksomhetene har blir lurt til å ansette det som i realiteten er nordkoreanske borgere i stillinger som IT-arbeidere.

Til tross for at kampanjen har blitt godt beskrevet i åpne kilder, blant annet gjennom amerikanske tiltaledokumenter og rapportering fra cybersikkerhetsfirmaer, er det få indikasjoner på at aktiviteten avtar. Tidligere har aktiviteten særlig rammet amerikanske mål innenfor blant annet teknologi og transportsektoren. I dag retter aktiviteten seg bredt mot virksomheter globalt, inklusiv i Norge, som ansetter i IT-relaterte stillinger.

Rapportering fra cybersikkerhetsfirmaer tilsier også at kampanjen i senere tid har økt i omfang og kompleksitet. De observer blant annet at aktøren har begynt å benytte seg av AI-verktøy for å lage identitetspapirer og for å endre stemmen til IT-arbeiderne.

Fremgangsmåte i Norge

Nord-Korea har utviklet et sofistikert system for å skjule identitetene til de nordkoreanske IT-arbeiderne. I tilfellene i Norge har de benyttet falske identitetspapirer knyttet både til fiktive karakterer, men også til faktiske individer som de har stjålet identiteten til. Identitetspapirene fremstår autentiske og er profesjonelt produsert, hvor de har hevdet å være borgere av forskjellige europeiske land.

De norske firmaene har i hovedsak kommet i kontakt med IT-arbeiderne gjennom LinkedIn, men i et tilfelle ble også personen ansatt ved hjelp av et utenlandsk rekrutteringsfirma. IT-arbeiderene har blitt ansatt som programvareutviklere og har i de fleste tilfeller gjennomført arbeidsoppgavene sine på en tilfredsstillende måte. De norske firmaene har derfor hatt liten grunn til å stille spørsmål ved ansettelsesforholdet.

Imidlertid har det vært en rekke uvanligheter knyttet til de ansatte i norske bedrifter, både når det kommer til ansettelsesprosessen og perioden disse var ansatt hos virksomhetene.

Dette inkluderer:

- Ansatt snakker med en aksent som ikke samsvarer med hevdet opprinnelsesland
- Ansatt er motvillig til å snakke språket fra hevdet opprinnelsesland
- Ansatt ønsker ikke å skru på kamera i møter
- Ansatt vil i tilfeller hvor kameraet har vært på befinne seg i et lokale som beskrives som «kundeservice-lignende»
- Ansatt ønsker å motta lønnsbetalinger på en konto som befinner seg i et land som ikke korresponderer med hevdet opprinnelsesland
- Ansatt har utstrakt bruk av anonymiseringstjenester som VPN eller proxy
- Ansatt er registrert med VOIP-telefonnummer
- Ansatt forsøker å få tilgang til ulike tjenester som ikke naturlig tilhører arbeidsoppgaver
- Ansatt har påloggінger utenfor arbeidstid

Aktiviteten i Norge kjennetegnes av at den også rammer virksomheter som ikke tradisjonelt er prioriterte mål for fremmede lands etterretningstjenester. Dette er fordi hovedformålet med aktiviteten som nevnt er økonomisk vinning og sanksjonsomgåelse, og ikke informasjonsinnhenting. Det er ingen fellesnevner når det kommer til sektor for virksomheter påvirket i Norge.

Vurdering

Aktiviteten beskrevet i denne rapporten illustrerer variasjonen og kompleksiteten i aktiviteter som norske virksomheter kan utsettes for fra nordkoreanske etterretningstjenester. Slik aktivitet rammer ikke bare virksomheter som besitter skjermingsverdig informasjon, men også de som tradisjonelt ikke har vært mål for fremmede etterretnings- og sikkerhetstjenester tidligere. Videre understreker aktiviteten hvordan trusselaktører kan utnytte potensielle sårbarheter knyttet til den økte bruken av hjemmekontor, samt viktigheten av at virksomheter gjennomfører undersøkelser som verifiserer identitet i nyansettelser.

Nord-Korea er en aktør som har vist at de evner å kontinuerlig utvikle modus for å omgå sanksjonsregimet som landet er underlagt. Dette betyr at norske virksomheter må være forberedt på at de kan utsettes også for annen type aktivitet fra nordkoreanske aktører i fremtiden.