



I kontorene til NorCERT i Nasjonal sikkerhetsmyndighet overvåkes dataangrep mot Norge. – Siste innbrudd skjedde denne måneden, sier avdelingsdirektør Eiliv Ofigsbø. FOTO: OLAV OLSEN

Stjeler kontrakter, tegninger, passord og hemmelige data

Ti datainnbrudd er oppdaget i norske selskaper innen forsvar, olje og energi. Dette er den største dataspionasjesaken som er avdekket i Norge. - Meget alvorlig, sier en PST-sjef.

[Per Anders Johansen](#)

Oppdatert: 16.nov. 2011 07:48

Lagre a

- Dette er en operasjon som har pågått over lengre tid, og som fremdeles pågår, advarer Nasjonal sikkerhetsmyndighet. Databasene til en rekke selskaper er systematisk tappet over flere måneder.

Den teknisk svært avanserte spionasjeoperasjonen er nå under etterforskning av Politiets sikkerhetstjeneste. Både PST og NSM mener dette er det mest omfattende angrepet som er avdekket her i landet.

- Dette ser vi på som meget alvorlig, sier operativ sjef i Politiets sikkerhetstjeneste, Tore Risberget.

Det siste innbruddet fant sted i november. Målet har vært å hente ut data som hemmelige kontrakter, industritegninger, brukernavn og passord.

- Siste rapporterte hendelse skjedde denne måneden, og vi jobber fremdeles med håndteringen av denne, sier avdelingsdirektør i NSM og sjef for NorCERT Eiliv Ofigsbø.

De ti datainnbruddene mot selskaper innen olje, gass, energi- og forsvarssektoren hittil i år er bare toppen av isfjellet. Flere andre er trolig allerede tappet for industrihemmeligheter uten at de har oppdaget det. Som regel skjer det via e-post med infiserte vedlegg til ledere fra falske avsendere.

Stjeler norske hemmeligheter

NorCERT i Nasjonal sikkerhetsmyndighet, som har ansvaret for å koordinere innsatsen ved alvorlige dataangrep i Norge, mener innbruddene har så mange likhetstrekk at samme aktør står bak:

- Dataspionene tømmer selskapenes databaser skjult i den vanlige nettverkstrafikken.

- Målet er sjefer og nøkkelmedarbeidere.

- Spionviruset er programmert så likt at man antar at samme aktør står bak.

- Hvert innbrudd er skreddersydd for å omgå antivirus.

- Angrepene er i metode og teknologi meget avanserte. Vi ble overrasket da vi begynte med en analyse av flere ulike saker og oppdaget så store likheter mellom dem, sier Ofigsbø.

Har spionert i flere måneder

Dataspionene har slått til i perioder hvor selskaper forhandler om kontrakter og store mengder e-poster sendes frem og tilbake. Utvalgte personer plukkes ut.

Fleire av innbruddene ble oppdaget flere måneder i

ettertid. I praksis betyr det at industrihemmelighetene forlengst er sendt ut av landet.

- I mange tilfeller har vi sett at angriperen har vært inne på systemene i flere måneder, og da må vi anta at de har tatt med seg store mengder informasjon, noe annet ville være naivt, sier Ofigsbø.

Milliardindustri

Omfanget av dataspionasje har økt kraftig de siste årene, og datatveri regnes nå for å være en større internasjonal industri enn narkotikahandel. Det er billig, og risikoen for å bli tatt er nærmest null.

Hverken PST eller NSM vil si noe om hvilke selskaper som er rammet, eller hvem man tror står bak. Selskapene selv er redde for dårlig PR dersom de innrømmer at hemmeligheter kan ha kommet på avveie.

- I ytterste konsekvens kan dette ramme Norge både politisk og økonomisk. Når vi ser på hvilke bedrifter og deler av det norske samfunnet som her blir forsøkt rammet, gjør det at vi totalt sett ser meget alvorlig på dette, sier PSTs operative sjef Tore Risberget.

Publisert: 15.nov. 2011 21:07

art