Skreddersydd dobbeltangrep mot Hydro

nrk.no/norge/skreddersydd-dobbeltangrep-mot-hydro-1.14480202

Henrik Lied, Peter Svaar, Dennis Ravndal, Anders Brekke, Kristine Hirsti

Data-angriperne krevde løsepenger av Hydro for å «låse opp» datasystemet deres. Samtidig ble det gjennomført et målrettet angrep på brukerdatabasen til industrigiganten.

Publisert 19.03.2019, kl. 12.52 Oppdatert 19.03.2019, kl. 16.47

Artikkelen er flere år gammel.

Etter det NRK får opplyst, har Nasjonalt Cybersikkerhetssenter (NorCERT) sendt ut et varsel til en rekke samarbeidspartnere om dagens dataangrep på Hydro.

Alle offentlige virksomheter i Norge er nå satt i beredskap for å se etter ytterligere spredning av denne typen løsepengevirus.

NRKbeta forklarer: Løsepenge-viruset «WannaCry»

Løsepenge-virus

«NorCERT varsler om at Hydro er utsatt for et ransomwareangrep (LockerGoga). Angrepet ble kombinert med et angrep mot Active Directory (AD).

NorCERT ber om informasjon om andre er rammet av tilsvarende hendelser. NorCERT bistår Hydro og hendelsen regnes som pågående», står det i varselet.

I klartekst betyr dette at data-angriperne både har brukt et såkalt løsepengevirus (ransomware), som gjør alt innholdet på datamaskinen utilgjengelig, samtidig som det foregår et angrep mot Hydros bruker- og påloggingssystemer (active directory).

– Jeg vil ikke bekrefte at det dreier seg om et active directory-angrep, sier Håkon Bergsjø, leder for NorCERT.

Hydro har varslet alle ansatte om å ikke skru på datamaskinene sine eller koble til nettverket.

Foto: Terje Pedersen / NTB scanpix

– Alvorlig

Hydro holdt en pressekonferanse tirsdag ettermiddag, der finansdirektør Eivind Kallevik bekreftet at systemet er rammet av et krypteringsvirus.

– Situasjonen er alvorlig. Hele det globale nettverket er nede. Vi jobber hardt for å begrense viruset og løse situasjonen. Det har ikke ført til noen andre sikkerhetsrelaterte hendelser, sier Kallevik.

Hydro vet ikke hvem som står bak eller når systemene kan bli friskmeldt. Ifølge Kallevik er det ikke et tema å etterkomme eventuelle krav om løsepenger.

– Vi har gode backup-rutiner. Hovedstrategien er å reinstallere data fra backupsystemene, sier han.

Anleggene er nå isolert fra systemet for å hindre spredning, og Hydro har fått hjelp fra eksterne eksperter til å identifisere og analysere viruset.

– Vi jobber døgnet rundt til problemet er løst. Produksjonen går som normalt, og vi gjør det vi kan for å minimere konsekvensene for kundene, sier Kallevik.

Hydros finansdirektør Eivind Kallevik.

Foto: Fredrik Hagen / NTB scanpix

«Nytt» virus

Løsepenge-viruset som er blitt brukt i angrepet mot Hydro heter LockerGoga, og ble oppdaget for første gang i januar. Den gang ble det brukt mot det franske konsulentfirmaet Altran.

– Dette var et løsepengevirus som brukte en helt ny kode. Denne kunne ikke oppdages selv med den beste type brannmur og datasikkerhetsløsninger, skriver de i en pressemelding.

Håkon Bergsjø i NorCERT.

Foto: Siri Vålberg Saugstad /NRK

Samtidig skriver selskapet at man måtte skreddersy en løsning for å motstå dette angrepet og fjerne viruset.

– Det er et krypteringsvirus som vi har sett brukt før i Europa, men det er alt jeg kan si på nåværende tidspunkt, sier Bergsjø.

Datasikkerhetsekspertene i selskapet Malwarehunter har lastet opp et løsepengekrav som har blitt fremmet i et angrep med det samme viruset tidligere i år.

Det er ikke kjent om Hydro har mottatt et lignende krav.

KRAV: Hackere som angrep et annet selskap med det samme viruset tidligere i år, sendte et slikt krav.

Omfattende angrep

Kommunikasjonsdirektør Halvor Molland i Hydro sa tidligere tirsdag at de først oppdaget forstyrrelser i nettverket og opplevde problemer med noen av styringssystemene.

– Vi opplevde en unormal datatrafikk sent i går kveld. Det viste seg utover natta at vi er utsatt for et dataangrep, sier han.

Hydros nettsider er fortsatt nede for telling. Ved flere av fabrikkene må operatørene styre produksjonen manuelt, og mindre anlegg er stengt inntil videre.

De ansatte har fått beskjed om å ikke skru på datamaskinene sine eller koble seg på nettverket.

E-tjenesten koblet inn

Nasjonal sikkerhetsmyndighet (NSM) bekrefter at de også er orientert om angrepet.

Ifølge fungerende avdelingsdirektør for Nasjonalt cybersikkerhetssenter i Nasjonal sikkerhetsmyndighet, Bente Hoff, er både PST, Kripos og E-tjenesten er koblet inn i etterforskningen.

– Vår rolle er å støtte Hydro, få en oversikt over situasjonen og redusere skade, sier Hoff.

Næringslivets Sikkerhetsråd (NSR) er en medlemsorganisasjon med formål å forebygge kriminalitet i og mot næringslivet.

– Det er sjelden vi ser et slikt omfang, men det er veldig vanskelig å unngå slike hendelser. De kriminelle, uansett hvem dette måtte være, har stadig nye metoder. 40 prosent av næringslivet rammes av ett eller flere alvorlige angrep hvert år, sier direktør Jack Fischer Eriksen i Næringslivets Sikkerhetsråd.

Det generelle rådet til Næringslivets Sikkerhetsråd er å ikke betale løsepenger.

– Å betale ut løsepenger er en farlig trend. Hvis de kriminelle tjener penger på dette, blir det motivasjon for andre, sier han.

- Les: Hydro utsatt for dataangrep: – Ikke opplevd lignende
- Les: IKT-Norge-direktør om dataangrepet mot Hydro: – En annen stat kan stå bak