Granskningsrapport for IT-sikkerhetshendelse

Analytiker: XXXXXXX. Dato: YYYYYY.

# Oppsummering

En alvorlig IT-sikkerhetshendelse ble oppdaget i BjørneKraft, hvor en phishing-angriper klarte å omgå tofaktorautentisering (MFA) og kompromittere en brukerkonto. Dette førte til uautorisert tilgang til sensitive dokumenter.

# Funn

* Kompromittert konto: Økon
* Avdekket mistenkelige innlogginger fra internasjonale lokasjoner (Panama, Hong Kong)
* Brudd på MFA-beskyttelse: sannsynligvis AITM
* Trusselaktøren har lagt inn regler om videresending av all e-post fra Økon til en Gmail-adresse
* Trusselaktør har lagt til egen ny MFA-metode
* Trusselaktør har lastet ned dokumenter fra M&A-mappe på brukers OneDrive-konto. Det er også laget en dele-link uten passord.

# Tolkning

Vi anser det som sannsynlig at angrepet er målrettet mot Økon, siden så langt har vi ikke funnet noen andre som ser ut til å være kompromitterte. Vi ser at det kun er dokumenter fra mappen M&A som er eksfiltrert. Dette tyder på at de har ønsket spesifikt å finne denne informasjonen.

Vi vet at det er utenlandske eiere bak fondet som i dag eier Kraftservice. Det er mulig at de ønsker å skaffe seg en bedre forhandlingsposisjon i forbindelse med oppkjøp.

# Mulige videre søk

* Undersøk andre brukerkontoer for lignende uautoriserte tilgangsforsøk
* Sjekk for e-poster fra samme avsender
* Sjekk for innlogginger fra Panama og Hong Kong + spesifikke IP-adresser
* Sjekk for utgående trafikk til detektert URL

# Liste over indikatorer

* Avsender av phishing-epost: docshare@bjoerrnekrft.no
* E-poster videresendt til okonsmart@gmail.com
* URL til phishing-link: h[XX]ps://www.bjoerrnekrft.no/login
* IP-adresse for innlogging fra Panama: xx.xx.xx.xx
* IP-adresse for innlogging fra Hong Kong: yy.yy.yy.yy
* Ekstra MFA-device med OTP lagt til på brukerkonto