NOODKAART

RANSOMWARE

Najaar 2022

Cyber Weerbaarheidscentrum
BRAINPORT
Voor hightech- & maakindustrie in NL

1 > BETAAL GEEN LOSGELD

Betalen lost het probleem nooit direct op en stimuleert computercriminelen om meer aanvallen uit te voeren.

2 > DOCUMENTEER HET BERICHT VAN DE AANVALLER

Documenteer berichten van de aanvaller. Ziet u een melding op het beeldscherm? Noteer datum, tijd en activiteit en maak hiervan een foto, screenshot of schrijf het bericht over.

3 > ISOLEER DE GEÏNFECTEERDE COMPUTER(S) DOOR DEZE LOS TE KOPPELEN VAN HET NETWERK°

LET OP! Schakel de stroom pas uit als u de apparaten NIET kunt loskoppelen.
Zo voorkomt u verdere verspreiding van de infectie, maar zonder stroom verliest u mogelijk nuttig bewijsmateriaal. Isoleer de geïnfecteerde computer(s) door deze los te koppelen van het netwerk 'of zet de wifi uit als je op een draadloos netwerk zit.

4 > SCHAKEL INCIDENT RESPONSE HULP IN

Denk aan uw IT-leverancier, (cyber)verzekeraar of een derde partij met 24/7 noodnummer, bijvoorbeeld: Eye Security: **088-6444800** ; IP4Sure: **040-2095020** ; BDO: **088-2364899**

5 > BEKIJK - EVENTUEEL MET DE ONDERSTEUNENDE PARTIJ - OF ER EEN SLEUTEL BESTAAT

Op **www.nomoreransom.org** staat misschien een sleutel om de gegevens weer toegankelijk te maken.

6 > COMMUNICEER

Waarschuw belangrijke klanten en toeleveranciers.
Deel z.s.m. Indicators of Compromise met hen om te voorkomen dat hen hetzelfde overkomt. Laat de informatie aub (anoniem) delen door het Nationaal Cyber Security Centrum **(cert@ncsc.nl)** e/o het Nederlands Security meldpunt **(info@securitymeldpunt.nl)**.

° *Als de infectie zich op grotere schaal heeft verspreid, zijn mogelijk meer ingrijpende maatregelen nodig om verdere verspreiding te voorkomen. Deze zijn zeer afhankelijk van het type ransomware en de mate van verspreiding.*
Heeft u voldoende kennis in huis? Start uw incident response. Identificeer en prioriteer kritieke systemen voor herstel en controleer en bevestig de status van data op getroffen systemen. Zo ontdekt u of data nog bereikbaar of versleuteld is. Geef prioriteit aan herstel op basis van een vooraf gedefinieerde lijst met kritieke bedrijfsmiddelen met informatie- systemen die essentieel zijn voor gezondheid en veiligheid, het genereren van inkomsten of andere kritieke services, net als systemen waarvan ze afhankelijk zijn.

i

Meer informatie over dit onderwerp deelt Cyber Weerbaarheidscentrum Brainport met haar participanten. Ook lid worden van deze stichting zonder winstoogmerk? Bezoek **www.cwbrainport.nl** of mail naar **info@cwbrainport.nl**.

Met dank aan

BRAINPORT EINDHOVEN
METROPOOL REGIO EINDHOVEN
Provincie Noord-Brabant