Cyber
Weerbaarheidscentrum
Greenport

Noodkaart Cyberaanval

1. Documenteer meldingen en/of berichten van de aanvaller

Documenteer eventuele 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.

2. 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 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.

3. Schakel incident response hulp in

Denk aan uw IT-leverancier of een derde partij met een 24/7 noodnummer. Bijvoorbeeld:

- Cyberwacht - Nederlands Cyber Collectief: 070-5135555 *(werkdagen van 08.00 tot 21.00 en zaterdag van 9.00 tot 15.00)*
- Digital Investigation BV: +31 356 77 4411 *(24/7 ondersteuning)*
- EYE: +31 88 644 48 00 *(24/7 ondersteuning)*
- Fox-IT: +31 800 369 2378 *(24/7 ondersteuning)*
- NFIR IT Forensics & Incident Response: +3188 133 0700 *(24/7 ondersteuning)*
- Northwave: 0800-1744 *(24/7 ondersteuning)*
- Tesorion: 088 274 7800 *(24/7 ondersteuning)*

4. In het geval van ransomware, 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.
Het betalen van losgeld stimuleert computercriminelen om meer aanvallen uit te voeren, dus het is niet aan te raden dit te doen.

5. Communiceer

Waarschuw belangrijke klanten en toeleveranciers.
Deel z.s.m. meer achtergrondinformatie met hen over de aanval om te voorkomen dat hen hetzelfde overkomt. Laat de informatie aub (anoniem) delen door het Nederlands Security Meldpunt (info@securitymeldpunt.nl)