Ransomware (Gijzelsoftware)

Wat is het?

- Kwaadaardige software (computervirus) met als doel gegevens “op slot” te zetten.
- Cybercriminelen willen hiermee geld verdienen en/of schade aanrichten.
- Geld wordt verdiend door losgeld (in bitcoin) te eisen om toegang tot de gegevens te krijgen, die versleuteld zijn.
- Schade wordt aangericht doordat computersystemen en -gegevens onbruikbaar worden.
- Gegevens worden versleuteld (encryptie), in vrijwel alle gevallen zijn de gegevens voorgoed verloren als het slachtoffer niet betaald of geen (werkende) back-up heeft.
- Tegenwoordig worden de gegevens niet alleen op slot gezet, maar ook gestolen. Wanneer het slachtoffer niet betaald worden de gegevens online gepubliceerd als tweede chantagemiddel.

Belang voor Nederland

- Het beschermen van vitale infrastructuur en zorginstellingen tegen gijzelsoftware is van cruciaal belang voor onze nationale veiligheid.
- Vanwege het digitale DNA en verbondenheid vormt ransomware een extra groot risico.
- Nederland is o.a. kwetsbaar door het niet direct updaten, slecht wachtwoordbeleid en het ontbreken van meerfactorauthenticatie (wachtwoord + eenmalige code);
- Het beschermen van het midden- en kleinbedrijf is cruciaal voor de economische stabiliteit & groei.
- De bescherming van persoonsgegevens wordt massaal bedreigd door gijzelsoftware.

Gevolgen bij misbruik

- Schade aan Individuele organisaties
  - Bijvoorbeeld: de volledige bedrijfsvoering kan stil komen te liggen, ernstige imagoschade wanneer gegevens openbaar worden gemaakt, faillissement door herstelkosten;
- Ernstige negatieve economische gevolgen
  - Bijvoorbeeld: de economie kan grote schade ondervinden door het grootschalig stilvallen van gedeelten van de Nederlandse economie;
- Serieuze bedreiging voor de nationale veiligheid
  - Bijvoorbeeld: ziekenhuizen, energiecentrales etc. kunnen gedeeltelijk of volledig stilvallen;
- Internationale reputatieschade
  - Nederland als koploper van datalekken / privacymeldingen
  - Ontwrichting van de maatschappij door het stilvallen van vitale infrastructuur of grote gedeelten van de Nederlandse economie.

Is misbruik al eens voorgekomen?

- Wereldwijd: Ja, bekende voorbeelden:
  - WannaCry (2017), 300.000 computers in meer dan 150 landen;
- Europa: Ja, bekend voorbeeld:
  - NotPetya, (2017) cyberaanval met Ransomware op Oekraïne me veel schade in NL
- Nederland: Ja, bekende voorbeelden:
  - Universiteit Maastricht , NWO, Hof van Twente, Haven van Rotterdam (MAERSK);

Cybersecurity specifieke relevante nationale wetgeving of andere richtlijnen

- AVG (Algemene verordening gegevensbescherming)
- BIO (Baseline Informatiebeveiliging Overheid)

Ransomware uitgelegd
Ransomware kopen = simpel (en zo wapen je ertegen) - NPO3.nl

Onze digitale samenleving heeft een “uit” knop
https://www.youtube.com/watch?v=1hIlTFG-RsU&t=101s