COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

Piek ransomware-aanvallen op zorgsector Europa

De afgelopen weken zien de security analisten van Z-CERT een toename in het aantal cyberaanvallen op de Europese zorgsector. Meerdere zorginstellingen in België en Frankrijk zijn de hard geraakt door cybercriminelen die losgeld eisen. Ten aanzien van dezelfde periode vorig jaar is het aantal ransomware aanvallen op de zorg meer dan verdubbeld. Vooralsnog is niet duidelijk waarom het aantal aanvallen nu zo piekt. Maar de ontwikkeling is voor Z-CERT genoeg reden om de Nederlandse zorgsector extra te waarschuwen.

18 februari 2021 | Malware

Van de volgende zorginstellingen is bekend dat zij de afgelopen weken zijn geraakt door ransomware.

- 28-12-2020 : Algemeen Medisch Lab (België)
- 17-01-2021 : Ziekenhuis Chwapi (België)
- 05-02-2021 : MNH: Franse zorgverzekeraar voor zorgpersoneel (RansomExx)
- 09-02-2021 : Dax-Côte d'Argent hospital (Frankrijk) (Egregor)
- 11-02-2021: Dordogne ziekenhuis groep (Frankrijk) – 2 locaties besmet maar geringe impact
- 15-02-2021 : Ziekenhuis Nord-Oues (Frankrijk) (met impact op 3 locaties) (Ryuk)

Cybercrime

Mogelijk zijn meer zorginstellingen geraakt, maar is dat nu nog niet bekend gemaakt. Cyberspecialisten van Z-CERT gaan op basis van ingeziene informatie uit van georganiseerde cybercrime. Van een aantal incidenten is bekend welke ransomware-groepen erachter zitten, namelijk: Egregor, Ruyk en RansomExx. Dit zijn bekende cybercrime-actoren die al vele slachtoffers hebben gemaakt. Zo richtte Ruyk vorig jaar nog een ravage aan onder de zorgsector in Amerika.

Dreigingsbeeld

In het onlangs gepubliceerde Cybersecurity Dreigingsbeeld Zorg 2020 beschrijven securityspecialisten van Z-CERT de gevolgen van ransomware voor de zorg en de maatregelen die zorginstellingen kunnen nemen. Het is bekend dat cybercriminelen vaak standaardmethoden gebruiken om bij een organisatie binnen te komen. In onze handreiking ’10 tips tegen ransomware’ beschrijven we welke (preventieve) maatregelen de zorg kan nemen. Denk bijvoorbeeld aan het maken van back-ups. Deel deze handreiking binnen uw organisatie.

Techniek

Het wordt lastiger als de cybercriminelen eenmaal een organisatie zijn binnengedrongen. Het gaat hier om professionele cybercriminelen die acteren op een zeer hoog technisch niveau. We geven op onze website in een serie artikelen meer informatie hoe u uw detectie op een hoger niveau kan krijgen en deze cybercriminelen kan “vangen” in een detectieweb.