Orange
Cyberdefense
Live 2022

Ahead of the storm in healthcare

Technology partner of the day:

Juniper Networks®

orange™

UZ LEUVEN

Zijn Europese ziekenhuizen klaar voor een cyberaanval?

SAMEN GRENZEN VERLEGGEN

Introductie UZ Leuven

Grootste UZ van België

1.764

10.000

Centralized IT

135

De enisa – cyberaanval oefening

enisa

- Europees Agentschap voor netwerk- en informatiebeveiliging.
- Klassieke opdrachten zoals kennisdeling, beleidsvoorbereidingen/advies, coördinatie tussen de lidstaten, bewustwording, …
- Dit jaar organiseerde het een 2-daagse cyberoefening rond Healthcare.
- In totaal 762 deelnemers waarvan 50% zorginstellingen
- Gecoördineerd per lidstaat: bij ons door CCB

SAMEN GRENZEN VERLEGGEN

Doel van de oefening

- Training voor de deelnemende organisaties
- Meten hoe “klaar” de deelnemende organisaties zijn
- Samenwerking testen tussen alle partijen

SAMEN GRENZEN VERLEGGEN

Deelnemers in de Belgische oefening

- CCB
- Federale overheid, dept gezondheid en E-health
- UZ Brussel
- UZ Leuven
- HUB Erasme
- St Luc
- Philips
- Federaal agentschap voor Geneesmiddelen en Gezondheidsproducten

SAMEN GRENZEN VERLEGGEN

Scenario

Multi-problem aanval:

- 2 hackers groepen met verschillend doel maar die samenwerkte
- Klassieke ransomware – data extractie – data verkopen – DDOS aanvallen – IoT aanval (slechte firmware voor specifieke lab toestellen) - …
- Lastige pers – communicatie met de hackers – gezellig sfeertje op sociale media

SAMEN GRENZEN VERLEGGEN

Scenario

- Hadden op voorhand een “speel omgeving” gekregen waar alles in gebeurde.
- Waren technische uitdagingen
- Waren project management/crisis management uitdagingen
- Waren communicatie uitdagingen

SAMEN GRENZEN VERLEGGEN

Lessons learned (algemeen)

- Zeer nuttige oefening: zouden we met zijn allen meer moeten kunnen doen. Helaas heel complex om op te zetten!
- Iedereen probeerde het eerst alleen op te lossen!
  - Te laat contact met cert.be/CCB/overheid
  - Te laat contact/samenwerking met elkaar
- Eens contact met CCB/cert.be gelegd, ging het oplossen beter/sneller. Maar coördinatie was onduidelijk.
- Informatiedelen en communiceren was het moeilijkst.
- Problemen met de “speelomgeving” maakte sommige oefeningen moeilijk.

SAMEN GRENZEN VERLEGGEN

Lessons learned UZ Leuven

- We wisten weken op voorhand dat het ging komen, dus alle resources waren aanwezig. Maar is dat in realiteit ook zo?
- Communicatie en aansluiting met de noodplannen van UZ Leuven werkte goed (wordt ook af en toe geoefend).
- Duidelijk dat een aantal specifieke kennis ontbrak: normaal hulp via cyberverzekering of een A-team. Extra opleiding voorzien?
- Specifiek netwerk voorzien (4/5G), laptops, tools, storage, … Een soort EHBO-kit voor cyberaanval.

SAMEN GRENZEN VERLEGGEN

Zijn Europese ziekenhuizen klaar?

- NEEN

Maar niemand is er klaar voor …

SAMEN GRENZEN VERLEGGEN

Zijn Europese ziekenhuizen klaar?

- Wat kunnen we nog doen om ons te versterken:
  - Samenwerken!
    - Informatie deling
    - Resource pooling
    - Gemeenschappelijke aankopen/services afnemen
    - …
  - Meer van zulke oefeningen – voor een bredere groep.

SAMEN GRENZEN VERLEGGEN