



ENISA Planspiel Cyber Europe 2022

Europäisches Cyberplanspiel der ENISA im Gesundheitswesen



Christian Jedinger

Leiter IT-Architektur

Mail: christian.jedinger@oog.at

Linkedin: <https://www.linkedin.com/in/christianjedinger>

Oberösterreichische Gesundheitsholding GmbH
Medizininformatik und Informationstechnologie

Der Gesundheitssektor als Angriffsziel

Was sind mögliche Risiken und ist der Gesundheitssektor nach über 2 Jahren Covid-19-Pandemie vor diesen sicher?

Ransomware

Datenleaks

Lösegeldforderungen

Cryptowährungen

vs

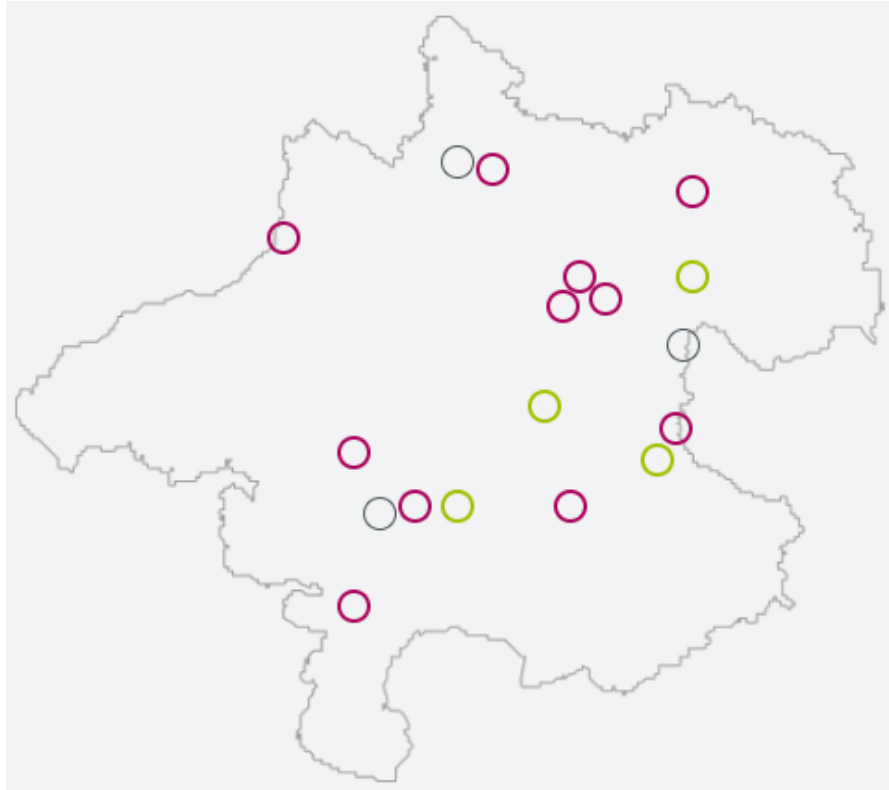
Medizintechnik

Wartungszugänge

Gesundheitsdaten

Krisenmanagement

Oberösterreichische Gesundheitsholding GmbH



Verteilt über Oberösterreich

- 6 Kliniken
- 12 Standorte
- 4 Betreuungszentren

<https://www.ooeg.at/>

Planung | Cyber Europe 2022


- Planung & Leitung durch die Europäische Union (ENISA)
 - ENISA (**E**uropean **N**etwork and **I**nformation **S**ecurity **A**gency)
- Nationaler Koordinator Bundeskanzleramt
- Pro Teilnehmer eine „Kontaktstelle“ vor Ort
- Definierte EXIT Strategie bei nicht geplanter Störung

Teilnehmer

- 29 Länder der Europäischen Union
- Organe und Einrichtungen der EU
- Insgesamt mehr als 800 Cybersicherheitsexperten als Übungsteilnehmer
- Übungsteilnehmer OÖG
 - Public Relations (PR)
 - CISO-Team
 - Medizininformatik und Informationstechnologie

Nationale Mitspieler

 Bundeskanzleramt

 Bundesministerium
Inneres

 Bundesministerium
Soziales, Gesundheit, Pflege
und Konsumentenschutz

 Bundesministerium
Inneres
Direktion Staatsschutz
und Nachrichtendienst



KABEG



Rahmenbedingung der OÖG

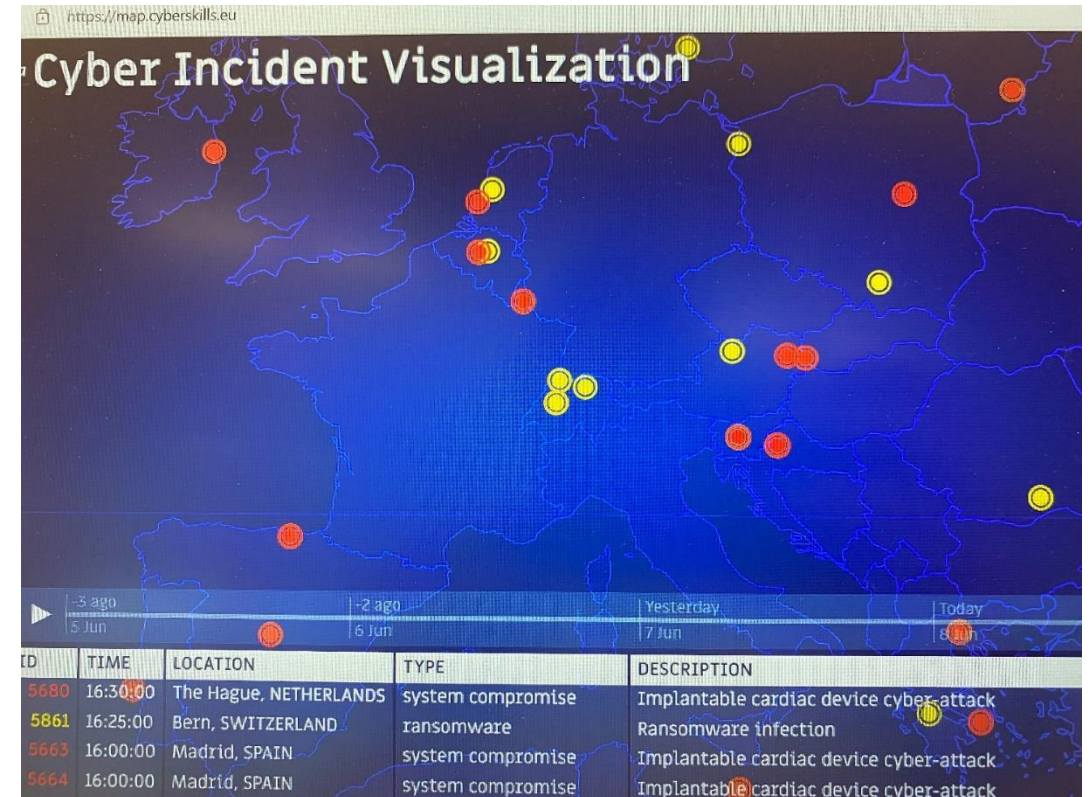
- Konstruktive Fehlerkultur
 - Es geht nicht darum, wer Schuld ist
 - Was lernen wir daraus
 - Was müssen wir Verändern/ Anpassen damit es nicht mehr passiert
 - Umsetzen

Ziel der Übung | Vorbereitung

- Organisation
 - Stabsarbeit
 - Krisenkommunikation intern/ extern
- Technik
 - Forensik
- Allgemein
 - Aufzeigen von Stärken und potentiellen Schwächen

Beginn | Phase 1

- Hinweise auf Anomalie am Perimeter
 - Analyse von Firewall und Proxy
- Hinweise bestätigen sich
 - Information an den CTO
 - Bildung Krisenstab
 - Information an die IT Führungskräfte
 - Information an die Geschäftsführung



Phase 1 | Learning

- Rasche Eskalation / Krisenstabsarbeit ist ein Erfolgsfaktor
- Sicherheit durch die duale Video Strategie Cloud + On-Premises
- Mitarbeiter/innen müssen die Notfallpläne kennen
- Notfallorganisation = Linienorganisation
- Vernetzung / gegenseitiges Verständnis der Führungskräfte

Phase 2

- Integrität von Daten gefährdet
- Firmware Fehler
- Angriff auf Systeme der Primärversorgung
- Erpressung
- Medien- und VIP Anfragen im Krisenstab

Phase 2

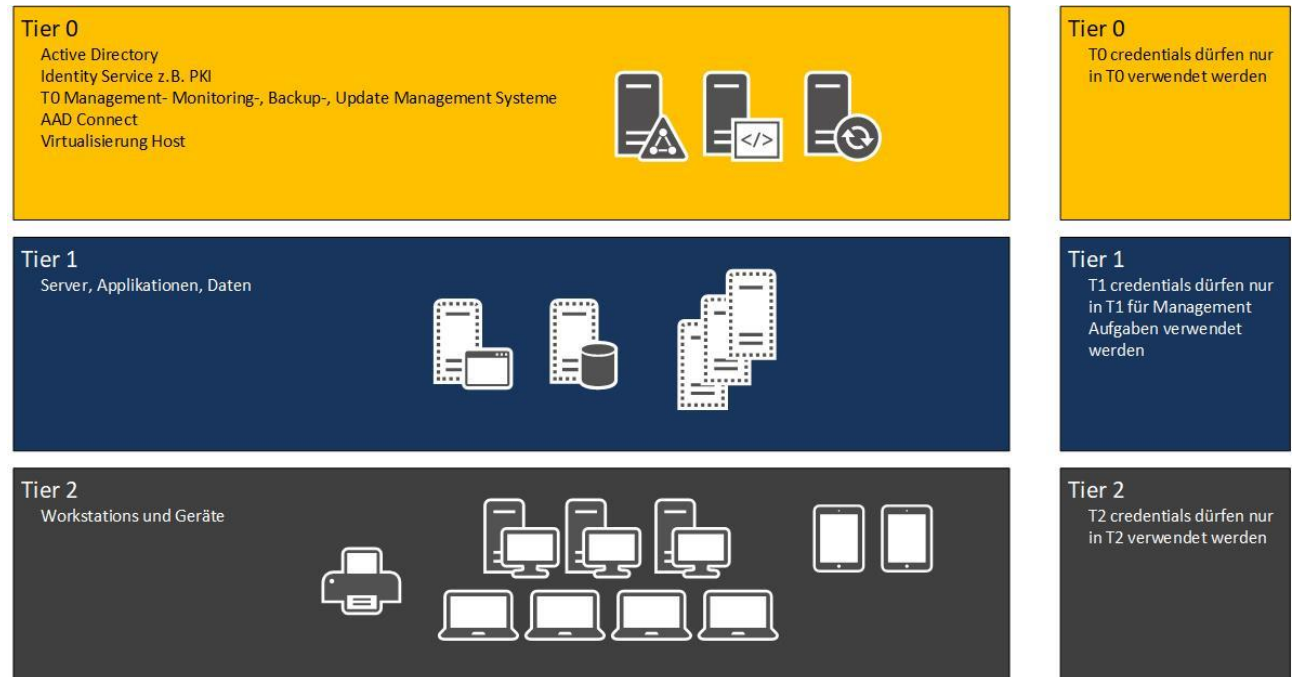
- Trennung des gesamten Konzerns vom Internet
- Einbeziehung von externen Partnern
- Beeinträchtigung wesentlicher Dienste
 - Meldungen lt. Netz- und Informationssystemsicherheitsgesetz (NISG)
<https://www.nis.gv.at/>
- Themengebiete Aufteilung & Priorisierung

Phase 2 | Learning

- Eine selektive Steuerung des Internetzugriffes wird notwendig werden. Anwender und „Systeme“ müssen getrennt werden.

- Segmentierung

- Netzwerk
- Applikation
- Credentials



Phase 2 | Learning

- Wie kommuniziert das Unternehmen nach extern z.B. Medien ohne Internetzugriff?

Zusammenfassend (1/2)

- Aus Sicht der OÖG sehr positiv verlaufen
- Rasche Eskalation / Krisenstabsarbeit ist ein Erfolgsfaktor
 - Krisenstab physisch an einem Standort
- Anpassung der Krisenstäbe an die S-Funktionen (Bsp. Feuerwehr)
- Lageführung | Übersicht z.B. mit Microsoft Teams hat gut funktioniert
- Übung: Ausfall Internet wäre sinnvoll zu Evaluierung der Schadenslage

Zusammenfassend (2/2)

- Übung Stabsarbeit
 - Planspiel mit Krisenstab der Unternehmensleitung und Kliniken
 - Trägerübergreifender Krisenstab
- Ressourcen
 - Bereitstellung eines externen Forensik Teams
 - Unterstützung durch Fremdfirmen in der Security
- Forensische Ausbildung der Mitarbeiter/innen hat sich gelohnt

Umsetzung in der OÖG

- Internetausfall bzw. gezielte Abschaltung (wie im Planspiel angenommen)
- Weiterführendes Planspiel mit Eskalation Land/Bund
 - Beispiel: Wie werden viele Intensivpatienten in kurzer Zeit verlagert?

Danke! Fragen?

Danke für Ihre Aufmerksamkeit