Healthcare Sector

This document contains information about this sector in relation to cyber security and incident response. The information can be used for scoping an Incident response game play. This information is for guidance purposes only. Not all information will match every industry.

Examples of some health care sector industries:

- Independent doctor offices
- X-ray labs
- Dental offices
- Chiropractors
- Psychiatrists
- Hospitals (public and private)
- Health enterprises (public and private)

Known Cyberattacks against the health sector:

https://ieeexplore.ieee.org/abstract/document/8888271

https://healthitsecurity.com/news/hc3-outlines-history-of-healthcare-cybersecurity-from-1980s-to-now

https://www.cisecurity.org/insights/blog/cyber-attacks-in-the-healthcare-sector

More information:

The history shows that the healthcare sector has been under cyberattacks from the very birth of the internet and network connected devices. As technology evolves so does the attacks. In 2014 Boston Children's hospital was subjected to DDoS attacks which denied users and other connected hospitals and universities access to the internet. The attack was launched by Anonymous in the wake of Boston Children's hospital assessment of a 14-year-old girl health issues.

Other common attacks are phishing and fraud scams. Attackers target a large organization which have an org chart publicly available, and find a middle management, or top management person to impersonate. They ask for the targets to access a link, buy gift certificates and the like to gain unwilful access or monetary values.

The health sector was in 2017 the target of a massive WannaCry campaign. The attacks hit over 200 000 systems in 150 countries. The attackers utilized IoT devices, poorly designed proprietary software as well as weak networks to gain access.

In 2020 in the wake of the SolarWinds attack a ransomware compromised Accellion causing one of the largest data breaches in healthcare history.

Systems important to the healthcare sector:

Any business that is in the healthcare sector has some sort of journal system for their patients. These journals usually contains an extensive medical history, whether it is all registered in that facility, or if its comprised of several journals from several facilities. These data are considered sensitive as they depict a person's health status, physical and mental. If these journals are leaked, it will cause a massive media backlash, as well as potential GDPR fines if the services are delivered to an European citizen.

Recommended Incident Response Training Scenarios:

- Phishing
- Ransomware
- Credential theft
- Weak open networks
- IoT devices
- Network breaches

Important review focus:

Awareness training

Make the employees aware of what to look after in potential phishing emails, or people that look out of place. Question even those who look like they belong

General computer etiquette

An unlocked computer with the journal system open, or just access gives an attacker ample opportunity to plant a malware, reverse shell or a C2 beacon.

Recommendations for adapting the scenario to the sector:

To make the game more immersive, it is recommended to adapt the scenario by adding names familiar to the organization. This will bring more value to the exercise as the players can relate and get involved. This can for instance be (but not limited to):

Industry specific systems	Important Vendors of Equipment	Other People not in the Game
journal system mailing system booking system	Device vendors (EKG machines etc.)	Cleaning personnel Janitors Secretary

General info about Implementing an Incident Response Plan Into a Custom Scenario

Using the current incident response plan work out how it fits to the scenario, and create injects based on this. The injects need to be realistic and pertain to the organization as well as the sector the organization is located.

The incident response plan should contain information on who to contact, how to handle media, as well as any reputation saving exercises. The plan should also have clear RTO and RPO lined out, so the leadership knows how fast the employees can get up and running in the event of a total disaster.

In case of information leak there should also be a media campaign running, or some PR mitigation. It should be clear who will be the media contact, as well as the customer contact, if those data are lost. If this is not in the incident response plan, it is a good learning experience to test out what the incident handlers will do under stress.