Koios

Education 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 gameplay. This information is for guidance purposes only. Not all information will match every industry.

Examples of some education sector industries:

- K-12 schools
- Upper elementary
- Vocational schools
- Universities

Known Cyberattacks against the education sector:

- https://www.csoonline.com/article/3647760/education-sector-hounded-by-cyberattacks-in-2021.html
- https://www.academia.edu/download/62002199/Proceedings_Digital_Privacy_and_Security_Conference_202020200205-127731-1fr50ut.pdf#page=43
- https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/rise-of-ransomware-attacks-on-the-education-sector-during-the-covid-19-pandemic

More information:

The education sector is highly dependent on its online learning management systems, which are used to distribute grades, give out assignments, and the general information forum. These are often bought as a Software-as-a-Service. The institutions do not have any say in hardening or protecting these platforms.

In December 2021, the log4j vulnerability was released, and it affected many webservers as it is an open-source part of the Apache web service. The vulnerability was mitigated very quickly, but it was still utilized in attacks, allowing the attackers to gain a remote shell within the network of that webserver.

In addition to these attacks, the education system is often hit by ransomware, crypto viruses as well as targeted phishing attacks. These are usually done by studying the organizational map or structure online, which many institutions post willingly. The attackers target middle management and often ask for gift cards with the pretense of an anniversary or a celebration. The request is sent to someone below the middle manager, stating that they are busy in a meeting, and prompts the employee to buy some iTunes gift cards or something similar and send the codes to the sender.

Other means of attacks are phishing emails that are used to try to harvest credentials or that contain malware as a PDF attachment that encrypts anything the user has access to, locally or on shared storage.

Systems important to the education sector:

Any institution that is in the education sector has student records. These student records contain contact information and social security number for each student. The records include any information an attacker can sell to scammers, attackers, or anyone interested in this information. Some students have secret addresses to hide them from legal guardians, parents, or other people that should not know where they live. If these data get stolen, it can potentially become a dangerous situation for those with secret addresses.

Student records containing grades are also sensitive information that should be protected at all costs. If the grades are publicly available, students can sue the institution for disclosing them.

The network is also a critical point in today’s educational systems. Most systems rely on online material in some way or the other. If the institution is under a DDoS attack, or if the network itself is crippled in some other way, it may hinder the educational process massively, resulting in a reduced learning impact on the students.

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.

General computer etiquette

An unlocked computer connected to the network is a golden opportunity for an attacker. Inserting a USB drive with malicious software, trojans, reverse shells, crypto viruses, etc., will spread quickly within an educational network. The network is often structured very flat or open with little or no controls implemented.

It is important for all users and faculty always to lock their computers. Teachers or professors also usually have Single sign-on (SSO) access to learning management systems and grading systems that can be downloaded, screenshot, or dumped in other ways to be spread online for anyone to see.

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 is not limited to):

Industry specific systems	Important Vendors of Equipment	Other People not in the game
Learning management system Mailing system	Printer vendors Projector vendors	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 the scenario and create “injects” based on this. The “injects” need to be realistic and pertain to the organization as well as the organization’s sector.

The incident response plan should contain information on whom to contact, how to handle media and any reputation-saving exercises. The plan should also have a clear recovery time objective (RTO), and recovery point objective (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 an information leak, there should also be a media campaign running or some PR mitigation. It should be clear who will be the media contact and 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.