IT Protection and Security: MIT 264
Alden A. Quiñones
Activity 8 - Ransomware_Response

Scenario: One machine is infected with ransomware

A. Immediate actions

1. Isolate Affected Systems - Disconnect infected devices from the network to prevent the spread of ransomware.
2. Activate the Incident Response Team - Mobilize your pre-established incident response team to assess and manage the situation.
3. Identify and Contain the Threat - Determine the scope of the attack and implement measures to contain it, such as disabling compromised accounts or services.
4. Eradicate the Ransomware - Remove the ransomware from affected systems by cleaning or rebuilding them, ensuring that no remnants remain.
5. Restore from Backups - Recover data and systems using clean backups, ensuring they are free from malware before restoration.
6. Communicate with Stakeholders - Inform internal and external stakeholders, including employees, customers, and partners, about the incident and the steps being taken.
7. Engage Law Enforcement and Legal Counsel - Report the incident to appropriate law enforcement agencies and consult legal counsel to understand obligations and implications.
8. Conduct a Post-Incident Review - Analyse the incident to identify lessons learned and update the incident response plan accordingly.

B. Why You Should NOT Pay the Ransom

I wouldn’t pay the ransom because there's no sure that the hackers will really give back the data or unlock our system after paying. Giving them money just makes them do it more, and maybe even come back to attack again. It's like saying what they did is okay. Also, paying could be a problem with the law if the group is part of some banned or criminal list. It's better to just focus on stopping the attack, bringing back the system using clean backups, and fixing how they got in. That way, we protect our system and stop this from happening again.

C. Long-term security improvements

1. Implement Multi-Factor Authentication (MFA) - MFA adds an extra layer of security by requiring a second form of verification, making it much harder for attackers to access accounts even if they have stolen passwords.
2. Regularly Backup Critical Data - Regular, encrypted backups ensure that if ransomware does lock or encrypt data, we can restore it without paying the ransom.
3. Keep Systems and Software Updated - Attackers often exploit unpatched vulnerabilities to deliver ransomware.
4. Conduct Regular Security Awareness Training - Many ransomware attacks begin with phishing emails tricking employees into opening malicious attachments or clicking on harmful links.
5. Use Endpoint Detection and Response (EDR) Tools - EDR tools help detect suspicious behavior on devices, such as unusual file modifications or attempts to encrypt large numbers of files.

6. Limit Access with Least Privilege Principle - By restricting access to only the necessary data and systems, attackers have less opportunity to move through the network and deploy ransomware.
7. Segment Your Network - Network segmentation creates barriers between different parts of the network.
8. Develop and Test an Incident Response Plan - Having a pre-established and practiced plan ensures that the team responds quickly and effectively in the event of a ransomware attack.
9. Monitor Logs and Set Alerts - Continuous monitoring of system logs can help detect unusual activity that may indicate a ransomware infection, such as file modifications or attempts to communicate with command-and-control servers.
10. Use Secure Configurations and Hardening Guidelines - Applying security best practices to configure systems securely reduces the number of vulnerabilities available for exploitation.