Cybersecurity: Ransomware

Spruce Point GROUP

What is Ransomware?

Ransomware is a type of malicious software, or malware, that encrypts a victim's files, making them inaccessible. The attacker then demands a ransom in exchange for decrypting the files. In some cases, the attacker may also threaten to leak sensitive data if the ransom isn't paid.

How Ransomware Spreads

1. **Phishing emails:** Attackers send emails containing malicious attachments or links that, when clicked, install the ransomware on the victim's computer.
2. **Exploit kits:** These are tools that attackers use to exploit security vulnerabilities in software, allowing them to install ransomware without user interaction.
3. **Remote Desktop Protocol (RDP) attacks:** Cybercriminals can access a victim's computer through weak or stolen RDP credentials and then deploy ransomware.

Protecting Against Ransomware

1. **Keep your software and operating systems up to date** with the latest patches.
2. **Use a reputable antivirus** software and enable automatic updates.
3. **Enable email filtering** to block phishing emails and malicious attachments.
4. **Disable macros** in Microsoft Office documents and only enable them when necessary.
5. **Limit user access** to the minimum required for their job roles, and educate employees on ransomware risks and best practices.
6. **Regularly back up your data** to an offline or secure cloud storage solution, and test your backups for data integrity.

Detecting Ransomware

1. **Unusually slow system performance** or unresponsive applications.
2. **Inability to access files or folders**, or files with unusual extensions.
3. **Suspicious network activity** or increased traffic to known malicious IP addresses.
4. **Unexpected system reboots** or shutdowns.
5. **Ransomware messages** or screens demanding payment for file decryption.

Responding to Ransomware

1. **Disconnect affected devices:** Immediately disconnect the infected devices from the network to prevent the ransomware from spreading.
2. **Notify your IT team or service provider:** Contact your IT support team or managed service provider to assess the situation and begin the remediation process.
3. **Report the incident:** Notify law enforcement and any relevant regulatory authorities about the attack.
4. Restore from backups: Assess the extent of the damage and recover your data from backups if possible