FOCUS TECHNOLOGY

Case Study: Cyber Security Attack and Remediation

How an industrial services company saved an estimated $1M in ransomware cost damages

Background

A leading Boston-based industrial services company with multiple locations across the country has trusted Focus Technology as their IT Solutions and Managed Services provider for the past several years. Focus provides the client with technology refreshes, managed backups, server maintenance and monitoring, workstation patching along with onsite routine vCIO visits with stakeholders to ensure the highest level of service and support.

Business Challenge

The client started to experience the tell-tale signs of ransomware: a lot of activity on files in the organization's network shares, multiple files with recent modified times within seconds of each other, documents given bizarre file extensions (ex: .pdf or .docx files renamed as .mp3 or other foreign extension types.) and corrupted files that would not open correctly. The infection was quickly spreading throughout their network and across many of their remote locations. Sensitive company data was now encrypted, and the hackers demanded a high ransom payment to recover these files. Focus Technology quickly assembled a Cyber Security Incident Response Team (CSIRT) who was onsite the next day to respond to the cyber security attack and provide remediation.

Solution

The first step was to identify the malware. Focus Technology Cyber Security team identified that the initial infection was gained through a malicious email attachment. Phishing and scam emails are the most common approach to gain unauthorized access by hackers. Because these are constantly evolving, it becomes increasingly challenging for organizations to protect against cyber security attacks.

Once the malware was identified, the second step was to contain the infection. With ransomware and any malware that propagates itself, encrypts or corrupts files, certain operations must be shut down until the infection is contained. This presented a business challenge because employees needed to access documents and services in order continue normal business operations. With that in mind, Focus Technology deployed Endpoint Protection tools and a SIEM (Security Information and Event Management) to provide visibility into the entire network. After determining there was no data exfiltration or any persistent backdoor access, Focus restored initial access in a read-only mode.

The final step was to recover the systems back to normal operations. Focus Technology provides managed backups for the client which was crucial for this incident. Without validated current backups, the organization would have lost a significant amount of data or had been forced to pay ransom for it. Paying the ransomware is generally not recommended; the hackers are given more resources to develop further ransomware and there is no guarantee that the antidote decryption tool is delivered once paid. Focus Technology's Cyber Security team successfully restored all affected systems across multiple remote locations and restored all ransomware-encrypted document prior to the infection.

Focus now maintains the client's patching process and endpoint protection to ensure the security holes are patched and virus definitions are kept up to date, as well as providing higher level protections such as behavioral-based endpoint protection.

Business Outcome

As a result of fast deployment and response, combined with the availability of good current backups, the client experienced minimal disruption to their business operations and was not held responsible for paying a cyber security ransom which saved the company an estimated $1M in ransom cost damages. One of the most lasting outcomes is that sensitive company data was saved and there was no damage to their reputation. Focus Technology Cyber Security Incident Response Team worked in partnership with key stakeholders to ensure the best possible outcome.

Why Choose Focus Technology for Cyber Security Services

The challenges of cybersecurity are complex but solving them does not need to be. At Focus Technology Solutions, we deliver a tailored information security program with expert security leadership that aligns with your company's security posture, business priorities and long-term goals. Focus Technology helps customers take a proactive approach to tightened IT security. Services include our Virtual Chief Information Security Officer (vCISO) program providing cybersecurity leadership, expert-driven guidance and implementation that aligns with your business strategy. Get access to valuable guidance of a security leader, without having to bring one in-house. Additional Cyber Security services include incident response, managed security services, education and training.