MorganFranklin Consulting
A Vaco Company

CYBERSECURITY SERVICES
CASE STUDY

Cyber Attack Rapid Response

Helping a medical group recover from a cyber attack and bolster defenses for the future.

Client
Regional Healthcare Provider

Services
Cyber Incident Response & Recovery

Areas of Expertise
Response & Recovery, Digital Forensics

Industry
Healthcare

Our Challenge

Our client, a regional healthcare provider, downloaded and installed a security update for their on-premises Microsoft Exchange 2016 server. After the installation was completed, issues began to surfacethat resulted in all email delivery being suspended. They suspected the newly discovered HAFNIUM vulnerability may have compromised their mail server. This event impacted the entire clinical and business operations of the medical group.

Throughout the course of the assessment, MFC and the medical group noted the mail server performance was severely degraded. The most resilient path forward was to rebuild the Microsoft Exchange server including the latest cumulative update and security patches to ensure all activity related to the malicious activities would be removed. This rebuild also addressed performance issues. After MFC validated the Microsoft Exchange server was back online and operational, and confirmed that the external interface was secure, it was opened up to external access. As an additional safety measure, they blocked all inbound and outbound internet traffic to/from IP addresses associated with the HAFNIUM attack.

Our Solution

Pivot Point Consulting and its Vaco sister company, MorganFranklin Cyber (MFC), were called in to provide a rapid response to the critical situation.
The scope of our services included:

- Performing an initial incident response to identify the cause of the mail delivery issues
- Determining if the mail server was compromised by malicious activity related to the HAFNIUM zero-day attack
- Identifying malicious activities performed by the attacker(s)
- Rebuilding Microsoft Exchange email services
- Securing the rebuilt system(s) from known exploitable vulnerabilities

Our Results

In addition to resolving the HAFNIUM vulnerability issue and fully restoring the medical group's Microsoft Exchange server in less than 48 hours, Pivot Point Consulting and MFC recommended the following measures to prevent future breaches:

- Implement multi-factor authentication (MFA) for all users across the organization for remote access to their systems
- Ensure processes are in place to regularly scan all external interfaces in their environment for known vulnerabilities
- Perform internal and external penetration tests on an annual basis at the network and application level