Case Study

CyberSecurity **Assessment & Incident Response**

The following case study highlights a matter for which Secure Cyber Defense and Vestige Digital Investigations were retained for CyberSecurity Assessment and Incident Response services respectively. This is a real matter that we have worked together, but the client information has been sanitized for privacy and confidentiality purposes.

Scenario

Secure Cyber Defense was hired by a medical practice to perform a CyberSecurity Assessment. During the assessment they discovered the client had some liberal firewall settings. These were pointed out along with recommendations for remediation at the completion of the audit. However, the client did not fully comply with the suggestions.

The Incident

Fast forward several months. One of the client's users noticed some odd behavior on her computer, including errant mouse movements and things not arranged the way she had left them.

The client noticed and reported the anomalies relatively quickly to their I.T. company first, who called Secure Cyber Defense. Seeing the nature of the situation, Secure Cyber Defense contacted one of their Premier Partners, Vestige Digital Investigations, Experts in Incident Response and Digital Forensics.

Vestige worked hand-in-hand with Secure Cyber Defense to pull appropriate logs. Then Vestige preserved the memory and hard drives of the device, and performed a comprehensive Incident Response Analysis.

Findings & Results

Vestige found evidence of three attempts at hacking into a particular end-user's computer from Nigeria. The attacker used the built-in remote desktop feature to gain virtual access to one of the client's computers. This occurred because of the aforementioned firewall exceptions were not corrected by the client.

Vestige also uncovered that the client was not preserving or managing their log files properly and were using manufacturer default settings. As a result, Vestige had to rely much more heavily on other artifacts and circumstantial evidence. This created a slight delay and increased analysis cost for the client. But, in the end, based on the digital evidence found, Vestige was able to prove that no data was exfiltrated from the client's system.

Unfortunately, the client did not have proper log management and providers in place to capture the all appropriate digital artifacts. Fortunately, because they acted quickly and called the right resource, Secure Cyber Defense whom they had a pre-established relationship with, Secure Cyber was then able to recommend Vestige. The two company's combined their unique talents to answer the critical questions of why their system was hacked, where it was being hacked from, and whether their data had been stolen or not.

over

Lessons Learned

- Every organization regardless of size and the type of data they have is a potential cyber incident or breach victim.
- Constant vigilance in regard to putting into place proper cybersecurity controls can prevent or at least significantly help detect issues.
- Taking recommendations seriously and remediating the gap is critical.
- Having a process to collect and manage appropriate logs and digital artifacts is essential.
- Most importantly, having a pre-established relationship for both proactive and reactive security providers, such as Secure Cyber Defense and Vestige Digital Investigations, helps lead to a more secure environment and the ability to detect and react to a threat very quickly and cost-effectively.

Contact Us for more information on your CyberSecurity needs.

VESTIGE
Digital Investigations
Data Breach & Incident Response Experts

www.VestigeLtd.com

SECURECYBER DEFENSE
Managed Cybersecurity Service

https://secdef.com/