CASE STUDY: Retailer with new CISO needed an in-depth view of their cybersecurity in order to prioritize investments.

BACKGROUND

A retail chain was aware that they had experienced a few minor cybersecurity incidents and wanted to be sure that they had fully remediated. The CISO was new to the organization as well, so having an outside firm report on current state would be helpful to him as he reviewed pending projects to decide where to invest first.

OBJECTIVES

- Confirm remediation from past cyber incidents;
- Look for signs of compromise to address before they become a reportable breach;
- Provide recommendations for improvements based on our findings;
- Leverage Carbon Black tool used in assessment as Proof of Concept for endpoint security.

A compromise assessment leverages the same Foresite Incident Response team and tools that we use when we are responding to a known cyber attack or breach. In the assessment, we proactively gather logs over a period of time from key devices, such as firewall, IDS/IPS, servers and endpoints. The log data is then analyzed to look for indicators of suspicious behaviors, connections to known malicious IPs or unknown applications that could be malware running in the background.

For this engagement, over 1300 devices were monitored, and the results were eye-opening for the Client. We detected numerous remote access and file transfer applications that were not approved applications and potentially malicious that were then removed. Connections were found to suspicious domains in China and Russia. We also recommended a full discovery and documentation of devices, applications and users be conducted to verify that all non-approved accounts and connections were disabled.

The results of our analysis showed that outbound filtration rules were not stringent enough to protect the business from disclosure of sensitive data, and that multiple clear-text outbound FTP connections were identified.

While the client knew they lacked endpoint protection that could stop threats that did not have known malware signatures, the installation of Carbon Black's endpoint solution as part of this engagement was able to find at 46 potential malware applications running that had gone undetected by traditional anti-virus software.

With so many devices creating logs, it had gone undetected that there were VNC connections being made to suspicious IP addresses, even though there was an internal SIEM solution in place. 24/7/365 monitoring is also critical to analyze this data and be able to proactively address potential threats.

Now that we had the data, the Deliverables included not only our findings, but a Cybersecurity Roadmap with prioritized short term, mid-term, and long-term goals for the organization so they could effectively prioritize budget and resources.

INDUSTRY

Retail chain

BUSINESS CHALLENGES

- Past incidents left them concerned that there could be residual malware
- Lack of 24/7 monitoring to be alerted to potential threats in real-time
- Internal staff not formally trained in cybersecurity analysis or response

FORESITE SOLUTION

- Compromise Assessment

OPPORTUNITIES

- Determine current state and provide actionable intelligence for next steps
- Provide a road map to get from current state to optimal state in manageable stages