CSW Cyber SecurityWorks

An American Public Affairs Company

Case Study

About Client

This client is a major American public affairs company. They are spread across eight (8) locations globally with domestic and international customers. Their employees work across the globe for fortune 500 brands in healthcare, FMCG, sports teams, aviation, energy, travel, automobile, real estate, telecommunication, banking, tourism and others.

They operate as an agency that creates, builds and protects various brands. They offer services in the areas of research, digital, public relations, brand strategy, creative, production, government and public affairs, and media.

They also provide services ranging from product launches and spin-offs to mergers, line-extensions, and cause-related marketing.

Challenge

The attack surface of the organization has increased over the last several years. As the organization has global presence, they have increased the connected devices, employee-owned devices and the number of access points in the organization/locations. Client did not have a clear understanding about their strengths and weaknesses of their current security program.

Threat actors usually target large organizations to pilfer a treasure chest of customer and employee data, intellectual property and other sensitive data. Client was not aware of the gaps within their ecosystem. Being a leader in their space, they have a lot of sensitive client information.

They quickly realized the need for a risk assessment, CSW was contracted to complete an assessment of their entire IT infrastructure (500 IPs) and provide a remediation strategy to improve the security posture of the entire organization. CSW was tasked to provide the client the list of identified security gaps and demonstrate a real-world attack without getting detected by their existing defence controls.

CSW's Solution

Client's network is located in the USA. They contracted with CSW for a full internal and external security assessment for their range of 500 IPs. The requirement from the client was to provide an in-depth analysis of all vulnerabilities and possible threats they would be face against their IT infrastructure from an internal and external perspective.

CSW's methodology involves reconnaissance of discovering devices (IPs), discovering vulnerabilities using multiple scanners to identify the vulnerable services, misconfigurations. Followed by manual and automated penetration testing, analysis of the results with POC's with an established goal of providing a remediation steps.

CSW experts successfully gained access to their internal network and moved laterally within the organization to compromise their entire network (domain controller). The team gained access to

employee and client details, credentials, sensitive files across several database servers, password hashes, and hence were able to take control of the entire company.

> *"I just want to commend you guys on a work well done!! The presentation of the results today was done very professionally, a good job."*
>
> Principal Security Architect

Benefits

Client was under the assumption that a breach of this nature was hypothetical and not possible but CSW team demonstrated by presenting the attack path and exposing internal data that this is possible and real. Client was able to identify and understand the security gaps in their IT infrastructure and the potential business impact. Client received a detailed vulnerability report with prioritized list of vulnerabilities (in excel/pdf/xml/SaS formats) according to risk ranking/criticality. The detailed technical report helped them completely visualize the risk exposure and helped the IT operations team with recommendations and action plans to remediate these risks.

The executive report submitted by CSW helped the management understand the cyber risks faced by the organization. Recommending them with actions to improve the security posture of their exposed IT infrastructure and hence preventing the organization from a real-world attack.