COMPASS
CYBER SECURITY

IDENTIFYING AND REMEDIATING CRITICAL NETWORK VULNERABILITIES

A large wholesaler of dining equipment and products was concerned about their current cyber security infrastructure. To assist in identifying their weaknesses, COMPASS performed an IT Assessment. The results showed a large amount of vulnerabilities at varying levels of criticality. While severe, these vulnerabilities were able to be remedied using COMPASS' report details and expertise.

THE CHALLENGE

Our client, a food wholesaler in the United States, was struggling to develop a roadmap that enabled their information technology (IT) staff to properly secure their network. They have 6 sites across the country and did not know where to start.

Our client came to us for assistance in securing their network and wanted to start with the initial scope being their Headquarters. To effectively and efficiently identify the current areas of weakness within the client's network, COMPASS performed an IT security assessment. **The assessment was broken up into 3 phases:**

- **HOST DISCOVERY:** Identifying all active hosts connected to the network
- **NETWORK VULNERABILITY SCANNING:** Identifying the vulnerabilities within each host
- **WEB APPLICATION VULNERABILITY SCANNING:** Identifying the vulnerabilities within the client's website

The report showed that there were a high number of Critical, High, Medium, and Low level vulnerabilities within their network. As a standard practice we recommend that Critical level vulnerabilities are addressed immediately, High within 2 weeks, Medium within a month, and Low within 3 months. It is important to prioritize the vulnerabilities that are identified to ensure the client's time and resources are properly utilized.

THE SOLUTION

COMPASS security engineers used several tools to analyze the client's network and identify unique vulnerabilities across their network infrastructure. The detailed reports provided by COMPASS allowed the client further insight into their specific and relevant vulnerabilities.

Using COMPASS' reports and our team of security professionals, our client identified **the following as their top critical vulnerabilities:**

OUTDATED SOFTWARE APPLICATIONS ON DEVICES

- Applications such as Adobe and Microsoft send frequent patch updates for security reasons.

WEAK PASSWORDS ON SELECT DEVICES

- Many of the devices COMPASS scanned were using weak or default passwords.

LACK OF POLICIES

- In order to keep up with software patch updates, set strong password, and ensure employee cooperation, it is important to have formal policies and procedure implemented throughout an organization.

COMPASS assisted our client in identifying the devices related to the above vulnerabilities and gave recommendations on the best ways to remediate.

THE RESULTS

Determining these high priority areas of focus allowed our client to immediately address their weakest links. The lower priority vulnerabilities were then incorporated into a security roadmap. Our client then built out their roadmap to include future assessments and remediation of network vulnerabilities. Also included in the roadmap was a plan for non-technical security items, such as the development of an Acceptable Use of Assets Policy. Our client is looking to undergo assessments for the other 5 of their 6 sites to ensure all facets of their organization are incorporated into their security posture.

INDUSTRY:	Hospitality
SIZE:	160 Employees
NUMBER OF LOCATIONS:	6

250 South President Street, Suite 2300, Baltimore, MD 21202 | 667-401-5108 | mflora@compasscyber.com