Enhancing Cyber Security with Vulnerability Scanning

The Challenge

Businesses rely heavily on computer systems to store, process and transmit sensitive data. To ensure the security and integrity of this information, it is crucial for business to regularly assess their IT infrastructure and identify vulnerabilities that could be exploited by malicious actors, especially those know to be currently exploited around the world.

Impact IT have engaged with one of their customers (Liaison Group) and have made huge strides in hardening their security, reducing exposure to known vulnerabilities by identifying and updating out-of-date software and restricting access to administrative functions. Data is reported to a web-based dashboard that both Impact IT and Liaison Group have access to, with which they can filter and verify results.

Project Overview

Vulnerability scanning can identify and be used to remedy:

1. Out-of-Date Software: Liaison Group had a diverse range of software applications, and maintaining updates across all systems was a challenging task.

2. Exposure to Vulnerabilities: Outdated software posed a substantial risk as it often contains known vulnerabilities that cybercriminals can exploit.

3. Compliance Concerns: Liaison Group needed to adhere to industry-specific regulations and compliance standards and outdated software could lead to non-compliance.

4. Cyber Essentials: Liaison Group pursues and maintains Cyber Essentials Plus certification (a government and industry recognised certification that demonstrates to other businesses and their customers that they take security seriously.

Implementing Vulnerability Scanning

To address these challenges, Liaison Group decided to implement a comprehensive vulnerability scanning program across its IT infrastructure. This tool is installed across the estate and checks in daily to a web-based dashboard, with trends and reporting available to show progression.

Cyber Security Facts:

95% of cyber-attacks are due to human error.

40% off businesses in the UK have experienced an attack.

Only around 5% of an organisation's data are protected, on average.

The average cost of lost data/asset breaches is £4,180.

Contact Us:

If your business is committed to preventing Cyber Security threats

Scan the QR code below to get in touch with us.

The vulnerability scanning tool was used to scan for known vulnerabilities, particularly in software applications, operating systems, and network configurations.

The scanning tool provided a risk assessment of each vulnerability, especially those known to be currently exploited, allowing the IT team to prioritise remediation based on the severity and potential impact on the organisation.

Benefits of Vulnerability Scanning

1. Risk Reduction: Vulnerability scanning helps identify and mitigate known security vulnerabilities, reducing the risk of data breaches, cyber-attacks and data loss.

2. Cost Savings: Proactively addressing vulnerabilities through scanning and patching reduces the potential financial losses associated with security breaches and the costs of incident response. It also ensures a "smooth experience" when attempting to renew annual Cyber Essentials certification.

3. Compliance Adherence: The company was better equipped to meet industry-specific regulations and compliance standards, ensuring they maintained a strong reputation and avoided potential fines.

4. Improved Productivity: Employees experienced few disruptions due to software updates, resulting in improved productivity.

5. Enhanced Reputation: Demonstrating a commitment to cybersecurity and customer data protection, Liaison Group's reputation as a secure technology provider was strengthened (when paired with Cyber Essentials Plus).

6. Long-Term Security: Regular vulnerability scanning became a part of Liaison Group's ongoing security strategy, ensuring that their systems remained secure in the face of evolving threats.

Summary

If your IT department or MSP is responsible for keeping your systems up to date, speak with them about what this means specifically. Patching Windows and Office applications is only one small part of keeping your endpoints up to date, for example, does your IT support provider track the version of and patch 3rd party applications such as Zoom, Chrome, Firefox and Skype? These applications do not necessarily keep themselves up to date.

The implementation of vulnerability scanning at the Liaison Group proved to be a proactive and effective strategy for reducing exposure to known exploitable vulnerabilities. By identifying and patching outdated software and addressing vulnerabilities in a systematic manner, Liaison Group enhanced its overall cybersecurity posture.

This case study demonstrates the tangible benefits of vulnerability scanning in a corporate environment, highlighting the critical role it plays in safeguarding sensitive data and maintaining the trust of clients and stakeholders in an ever-evolving threat landscape.

Testimonial:

"We have been working closely with experts from both Cognisys and Impact IT to identify and remediate vulnerabilities in our estate.

In five months, we have reduced by over 70% and have clear line of sight on Critical and Exploitable vulnerabilities and plans in place to action.

After penetration testing and Cyber Essentials Plus this is definitely a key area that businesses need to have visibility and action on – ahead of phishing in how "bad actors" access a business through software vulnerabilities!

Managed by our own IG team we keep close tabs on this key threat management vector, but it takes all three parties pulling together to succeed here."

Matthew Willman
CTO
Liaison Group

Impact IT work in collaboration with Cognisys to provide our customers with vulneratbility assessment services

COGNISYS
Smarter Cyber Security
cognisys.co.uk