SysGroup

CASE STUDY

UK-based investment firm

Introduction 01

Company Overview

SysGroup is a trusted provider of penetration testing, cyber maturity assessments, and compliance solutions. We empower organizations to secure their infrastructure, reduce risk exposure, and build long-term cyber resilience.

Client Background

Our client, a UK-based investment firm, manages sensitive financial data and operates across multiple offices. Recognizing the heightened risk of insider threats and misconfigurations in internal systems, the firm engaged SysGroup to conduct an internal penetration test and simulate real-world attack scenarios.

Challenges 02

Initial Situation

The firm wanted to understand its resilience against both unauthorized external access (e.g., "walk-in-off-the-street" attempts to connect devices to the corporate network) and malicious insider threats (e.g., disgruntled employees with unprivileged accounts).

Objectives

- Identify vulnerabilities in internal networks, wireless access, and standard device builds.
- Assess risks posed by outdated software, patching gaps, and weak configurations.
- Provide clear, prioritized remediation guidance to strengthen security posture.

Solution 03

Approach

- SysGroup conducted a **scenario-based internal penetration test,** combining black-box and grey-box methodologies:
- Black-box testing: simulated an outsider attempting to connect to network ports without credentials.
- Grey-box testing: simulated an insider with limited access (e.g., a contractor with a standard laptop).

Implementation

- Tested across multiple subnets, wireless networks, and user devices.
- Conducted vulnerability scanning, exploitation attempts, and password analysis.
- Delivered a comprehensive report detailing each finding, risk severity, evidence, and remediation recommendations.

Results 04

Outcomes

- High-risk findings: Missing OS and application patches, end-of-life software, outdated VMware hypervisors, Cisco IOS XE vulnerability (CVE-2023-20198), and insecure IPMI/Dell iDRAC configurations. These exposed the firm to risks of remote code execution, privilege escalation, and session hijacking.
- Medium-risk findings: Shared domain account passwords, weak RDP configurations, lack of SMB signing, and wireless networks using pre-shared keys susceptible to brute-force attacks.
- Low-risk and best practice gaps: Expired SSL certificates, users able to run unrestricted PowerShell/command scripts, and reliance on TPM-only BitLocker unlocking.

Benefits

- Provided the firm with clear visibility of its internal attack surface and the potential impact of insider or lateral attacks.
- Delivered a prioritized action plan including patching, configuration hardening, stronger authentication, and improved access controls.
- Increased awareness among IT leadership of the need for continuous vulnerability management and regular penetration testing.

Conclusion 05

Summary

SysGroup successfully simulated both outsider and insider threats, identifying critical vulnerabilities within the investment firm's internal infrastructure. The findings highlighted urgent patching requirements, account security weaknesses, and opportunities to strengthen defenses against modern attack techniques.

Future Plans

- Implement a robust patch management process across servers, endpoints, and hypervisors.
- Replace shared and default passwords with unique, complex credentials.
- Transition to WPA2 Enterprise authentication for wireless networks.
- Conduct regular internal penetration tests to ensure ongoing security improvements. SysGroup will continue to support with expert testing, remediation guidance, and compliance alignment.