iterasec

Pentesting client's external network

Client:
Global Software Engineering Company

Industry:
Software Engineering and Technology Consulting

Company Size:
1500+ Employees

Services Used:
External Network Pentesting, Vulnerability Research, Remediation Support

Client

A global provider of software engineering, technology consulting, and quality assurance services, renowned for delivering innovative and high-quality solutions. Operating across multiple industries, this company helps businesses transform their operations with cutting-edge technology. Their extensive portfolio includes custom software development, product design, data science, and digital transformation services for clients worldwide.

Background

Initially, the client approached Iterasec for external penetration testing to fulfill annual compliance and certification requirements, focusing primarily on safeguarding their public-facing services. As their operations expanded, so did the complexity of their external network environment, including VPN servers, collaborative platforms like Jira and Confluence, and multiple publicly accessible websites. Recognizing the increasing threat landscape, the client prioritized enhancing the security of their demilitarized zones (DMZ) and external services.

Upon beginning the penetration testing, Iterasec quickly identified additional areas requiring security improvements, resulting in a broader and ongoing collaboration. Regular penetration testing has since become an integral part of the company's cybersecurity strategy.

The Challenge

The company engaged Iterasec with several key objectives:

- **External Penetration Testing:**
  Identify vulnerabilities within their external network infrastructure
- **Critical Vulnerability Identification and Remediation:**
  Detect and address high-risk security flaws.
- **Continuous Security Enhancement:**
  Ensure ongoing security validation and improvement.

The Solution

Iterasec deployed a team of seasoned security professionals to execute comprehensive penetration tests and enhance security measures:

External Network Penetration Testing

- **Scope Definition:**
  Identified and evaluated all external assets, including VPN endpoints, web applications, and public services.
- **Vulnerability Scanning and Exploitation:**
  Conducted scans and manual assessments to discover vulnerabilities such as outdated software, misconfigurations, and exposed services.
- **Exploitation of Critical Vulnerabilities:**
  Prioritized vulnerabilities capable of compromising internal networks.

Discovery of Critical GLPI Vulnerability

During the initial assessment, Iterasec identified a severe vulnerability in GLPI, an open-source IT asset management system deployed by the client:

- **Authentication Bypass:**
  Gained unauthorized access to GLPI.
- **Remote Access to Workstations:**
  Leveraged GLPI's FusionInventory plugin to control company workstations remotely.
- **Potential for Full Infrastructure Compromise:**
  Demonstrated risk of malware or ransomware deployment.

In-depth Vulnerability Research

- **Source Code Analysis:**
  Reviewed GLPI's publicly available source code to pinpoint the vulnerability.
- **New CVE Discovery:**
  Identified and disclosed CVE-2021-21327, affecting GLPI instances up to version 9.5.3.
- **Responsible Disclosure:**
  Coordinated with GLPI developers, leading to a patched version release.

Remediation Support

- **Immediate Mitigation:**
  Provided temporary protective measures for GLPI.
- **Patch Implementation:**
  Assisted in upgrading GLPI to a secure version and advised on security configurations.
- **System Hardening:**
  Recommended securing additional external services.

Iterative Testing and Validation

- **Follow-up Assessments:**
  Regular penetration tests validated the effectiveness of remediation.
- **Continuous Monitoring:**
  Implemented ongoing security assessments for proactive vulnerability management.

The Outcome

The Iterasec team's ongoing engagement resulted in significant security enhancements:

- **Critical Vulnerabilities Addressed:**
  Eliminated severe flaws, reducing the risk of major compromises.
- **Enhanced Security Posture:**
  Strengthened the resilience and reduced vulnerabilities of external services.
- **Operational Stability:**
  Prevented potential disruptions through proactive threat identification and mitigation.
- **Community Contribution:**
  The discovery and disclosure of CVE-2021-21327 improved security for the broader GLPI user community.
- **Extended Impact Through Continued Assessments:**
  Follow-up testing in subsequent years revealed additional critical risks, further reinforcing the importance of regular security evaluations:
  - 2022: Identified the presence of a vulnerable Microsoft Exchange Server instance affected by the ProxyShell vulnerability chain (CVSS 9.8), capable of unauthenticated remote code execution.
  - 2024: Detected a critical Remote Code Execution vulnerability (CVSS 10.0) in an MS SQL Server instance via insecure stored procedure exposure, allowing unauthenticated attackers to execute system commands and potentially compromise the entire infrastructure.
- **Reinforced Long-Term Collaboration:**
  These findings helped the client recognize the value of maintaining a regular testing cadence and adaptive security strategies to stay ahead of evolving threats.

Conclusion

Initially engaged for penetration testing alone, Iterasec's comprehensive approach uncovered critical vulnerabilities and led to continuous, proactive security improvements. Regular penetration testing has since become a recurring element of the client's cybersecurity program, ensuring ongoing protection against emerging threats. This case underscores the importance of proactive security measures in safeguarding sensitive information and maintaining operational resilience.