ZONES™

Case Study

Network Risk Assessment

Security FORTIFICATION | Security Assessments

Aligning investments and resources to reduce business risks.

When the Board of Directors of a software publishing company wanted confirmation that current security investments and resources were addressing risks and vulnerabilities, Zones nfrastructure, the services company of Zones, stepped in to help. Based on information gathered by assessments, the Zones security team identified security vulnerabilities for remediation and helped resolve investment and resource allocation.

Challenge

- Better align security investments and resources to address risks and vulnerabilities across multiple attack vectors.

Solution

Zones nfrastructure services, including:

- Network Risk & Vulnerability Assessment.
- Zones Penetration Testing.
- Zones Application Security Assessment.

Results

- Validate security policies, procedures, and standards.
- Reduce data breach or data loss risk.
- Improve visibility, management, and control of data through lifecycle.
- Ensure compliance with standards/best practices.
- Extend value of internal IT security team with certified security experts.

ZONES

Network Risk Assessment

Case Study | Security FORTIFICATION | Security Assessments

The Challenge

The CIO and the IT team needed to act quickly to produce a report of the company's existing security posture. The objective was to help the company align investment and resources, expose any security gaps and risks, and get facts to help with strategic planning.

The Solution

Zones proposed a comprehensive Network Risk & Vulnerability Assessment, Penetration Testing, and an Application Security Assessment, to identify existing security gaps and establish a baseline to improve their overall security posture.

Network Risk & Vulnerability Assessment

- Identify, categorize, and prioritize present vulnerabilities that can be exploited.
- Identify gaps in policies, procedures or regulatory compliance requirements.
- Identify network deficiencies and correlate them to practical solutions.
- Uncover specific security threats that may require penetration testing.

Penetration Testing

- Review of network, operating system, application and endpoint security measures.
- Assess the magnitude of potential business and operational impacts of successful attacks.
- Enable compliance with industry-driven regulatory requirements.
- Provide evidence to support increased investments based on external, internal, or website application penetration testing.

The Solution (continued)

Application Security Assessment

- Probe, identify, and exploit systems with manual techniques and automated tools.
- Attempt to escape out of network and application boundaries of the systems.
- Attempt to gain unauthorized access to systems connected to the web application.
- Run black box unauthenticated and authenticated testing using roles and workflows.
- Evaluate source code, infrastructure, operating systems, and application functionality.

The Results

When summarizing the project, the client said "Zones provided a comprehensive solution to help us in identifying existing gaps in our security program and a cost-effective strategy for improving our overall security posture through a combination of security products and services. Most importantly, Zones was able to highlight and prioritize the areas needing attention so that we could focus our limited resources in the most efficient and effective manner."

Through the Network Risk & Vulnerability Assessment, Zones delivered the following:

- Client Scorecard highlighting level of risk by examined attack area with detailed findings to help the client focus their resources and investment on the most critical areas in their environment.
- SANS Security Controls Benchmark summary for comparison against the industry-standard SANS cyber-security maturity model, providing a comprehensive summary of their overall risk by functional area.
- Strategic recommendations allowing the client to prioritize areas of focus based on assessment findings, security goals, and level of effort for remediation.
- Maturity Roadmap, including a step-by-step framework and timeline to enhance security posture based on identified goals or compliance requirements.

The Results (continued)

Based on the detailed finding of the Network Risk & Vulnerability Assessment and recommendations from Zones, the company remediated the identified risk areas and implemented a Security Information and Event Management (SIEM) solution to provide real-time event logging and analysis of security alerts generated by their network applications.

Additionally, since they are a software publisher, the company invested in an Application Security Assessment to help identify vulnerabilities in their software, including unauthorized access to critical data and application functionality.

Due to the comprehensive approach to security proposed by Zones, the client is currently investing in an Intrusion Detection/Prevention System (IDS/IPS) as well as a Data Loss Prevention (DLP) solution to improve visibility to inbound threats and to data throughout its lifecycle to reduce data loss risk.

Client Benefits

- Identified weaknesses in existing policies, procedures, and standards.
- Validated security monitoring, incident identification, and response procedures.
- Identified security vulnerabilities for remediation, identified investment, and resource allocation.
- Reducing data breach or data loss risk.
- Improved visibility, management, and control of data through lifecycle.
- Ensuring compliance with standards/best practices.
- Extended value of internal IT security team with certified security experts.