

Security Assessment Service

We offer clients a thorough, methodical analysis of their current security program as compared to accepted industry best practices. Our Security Assessment Service is provided by xwave's Security and Business Continuity Team, one of the most comprehensive and dynamic security teams in Canada. Our approach emphasizes practical, realistic recommendations that reflect the culture and strategy of our clients, avoiding a "cookie cutter" approach and delivering top value.

DESCRIPTION

We use a proven methodology to provide clients with the most thorough and cost-effective security assessment possible. We use a combination of automated and manual testing techniques, and conduct both remote and on-site analysis in order to provide a comprehensive, well-rounded view of the organization's security capabilities.

Our assessment focuses not only on technical issues, but on critical processes, procedures, and policies used by the organization. Security is an ongoing process, and people and process issues have a much more significant impact than the technologies currently used. An assessment that focuses solely on technology becomes outdated with the next vulnerability discovered, system deployed, or service introduced.

We deliver a comprehensive review of security controls, infrastructure, initiatives, and operations. Detailed analysis and documentation phases utilize the data collected during the field work phases,

providing specific findings and recommendations regarding the various systems and practices reviewed. Additionally, an analysis of the overall effectiveness and appropriateness of current security measures will be provided, focusing on adherence to best practices for information security.

No matter what your organization, we can tailor a security assessment to suit your needs.

BENEFITS

We will provide an accurate depiction of your security strengths and weaknesses. Our comprehensive security assessment gives you an objective comparison of the organization's security practices and technologies against those currently recommended in the industry. By prioritizing recommendations for improvement, we will identify both areas to be corrected immediately, as well as those to be included in short- and long-term security improvement initiatives.

METHODOLOGY

We utilize a robust and thorough approach to performing security assessments. Specific activities included in the assessment can be customized as required. Key phases in the assessment process include:

Perimeter Testing

Perimeter Testing provides an accurate view of the organization from the outside. This allows us to identify critical exposures that are readily apparent to external attackers. Specific activities include network probes, vulnerability scans, war dialing, wireless network detection and manual testing.

Internal Scans

Internal scans provide visibility into an organization's security by conducting tests from within the customer network. This complements the perimeter testing by revealing details that might not be readily apparent, but which represent significant security issues. Tasks included in this phase include automated scans, packet sniffing, password tests, infrastructure probes, and examination of network services such as web servers.

Configuration Reviews

Detailed configuration reviews of sample servers, security devices, and network infrastructure components are conducted to extend and validate the findings of the previous phases. In-depth automated and manual analyses of representative systems provide insight into specific vulnerabilities. Security architecture reviews and network design analysis are used to evaluate overall infrastructure security and identify specific weaknesses or limitations.

Physical Security

Physical security is a vital part of an information protection program. It is well-known security doctrine that if someone has physical access to a computing resource, that system can inevitably be compromised. As part of a security assessment, we will examine server rooms, environmental controls, and physical access control within your key facilities.

Anti-Virus Assessment

Viruses, worms, Trojan Horses, and other forms of malicious software are among the most widespread security threats faced by organizations today. As part of the security assessment, we will review the existing anti-virus products, procedures for deploying software and signature updates, preventative measures used to defend against malicious email attachments, and management tools.

Security Strategy and Operations

An effective security strategy, supported by appropriate policies and procedures, is the key to a successful information protection program. Such a program guides how security technologies are managed and deployed, and more importantly how the organization and individual users deal with security issues. We will review existing policies and procedures, and conduct interviews with representative staff members to determine further details, requirements, and priorities. We will also identify additional procedures or policies that may be required.

Analysis and Research

Security issues in key applications and technologies will be researched. The data collected will be reviewed, analyzed, and specific solutions prepared.

Report Preparation

The report provides details on specific risks and issues uncovered, as well as feedback on areas where best practices have been well applied. Prioritized and specific recommendations for addressing issues are described. In addition to opportunities for feedback and discussion during development of the report, you will be given a presentation highlighting the key findings and results of the assessment.

SUMMARY

We offers a security assessment service which provides a thorough analysis of your organization's security. We can customize the scope and activities included in order to meet the needs of your organization, regardless of size.