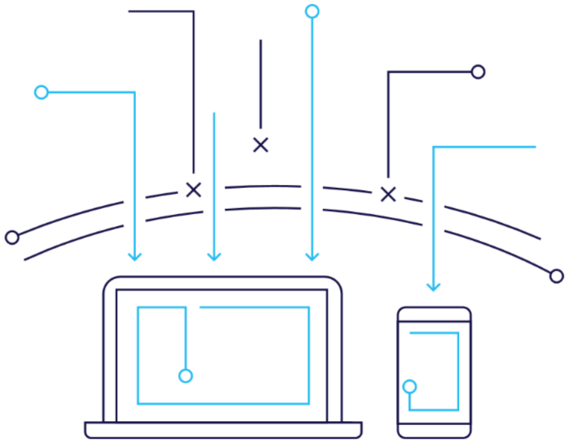
Vulnerability Assessment and Penetration Testing

Gaining Awareness of the Security Vulnerabilities of your Infrastructure and Providing a Roadmap for Remediation

IBM K-12

Highlights

- Helps identify network security threats and risks across your organization
- Leverages IBM expertise and technology to help you anticipate and prevent attacks
- Provides recommendations for reducing risk and increasing compliance



School districts today are often unaware of just how vulnerable they are to security risks. Implementing new technologies, the mobilization of students, falling victim to advanced threats — all these can expose gaps in an organization's security strategy that often lead to unauthorized access or a data breach. Failure to protect data and prevent intrusions can result in significant financial costs to address the breach and a damaged reputation.

You need to understand your current level of network security so you can effectively safeguard your systems and data and properly plan for tomorrow. IBM K-12 can provide a cost-effective solution that can identify the security vulnerabilities in your environment and provide a roadmap of activities to prevent network compromise.

Identifies and prioritizes weaknesses and provides detailed remediation steps.

IBM's Vulnerability Assessment Service provides a deep security assessment of external network infrastructure and applications, internal network infrastructure, servers and client devices. The purpose is to identify and document security exposures that may be used to infiltrate the network, assess systems for known vulnerabilities, and evaluate the identified vulnerabilities. Recommendations are provided for addressing identified security weaknesses or implementing viable mitigation strategies.

IBM's Penetration Testing Service exploits identified vulnerabilities and demonstrates the impact of those vulnerabilities in terms of successful attack scenarios. Our penetration methodology is focused on real world attack scenarios and the same techniques used by a motivated attacker. Internal penetration testing simulates an attacker with established access to a compromised system or malicious insider and attempts to elevate network privileges to access sensitive information, including applications and file servers containing sensitive data or financial information.

Socially engineering "phishing" activities may also be included in penetration testing, based on pre-approved scenarios, to validate a district's security awareness program.

The IBM K-12 Security Services methodology can include:

- Network discovery and reconnaissance – extensive inspection of online hosts and services
- Perimeter or internal probing – controlled exploitation of key vulnerabilities
- Remote exploitation – attempt to further penetrate the network and breach valuable or confidential data
- A quality service delivered safely by an expert security professional, through both manual penetration techniques and automated scanning
- Real-life demonstrations of covert and hostile activities typical of malicious attackers' attempts to compromise perimeter devices and security controls
- Findings and analysis deliverables – detailed report, including findings and actionable recommendations

These services validate existing security controls and quantify real-world risks, providing you with a detailed security roadmap that prioritizes the weaknesses in the network environment. By providing specific guidance and recommendations to reduce exposure, we help you reduce risk and downtime, protect business-critical information, manage compliance and significantly improve your return on investment.

Significant benefits may include:

- Identifies vulnerabilities and risks in your networking infrastructure
- Validates the effectiveness of current security safeguards
- Quantifies the risk to internal systems and confidential information
- Raises executive awareness of corporate liability
- Provides detailed remediation steps to prevent network compromise
- Validates the security of system upgrades
- Helps protect the integrity of online assets

Typical Length of Engagement 2 – 3 weeks

Why IBM?

We have the understanding and experience, manual investigation techniques as well as proprietary and industry-leading security assessment tools to identify and exploit vulnerabilities. With an in-depth analysis of vulnerability data for evaluation, we will help you build an effective security program that enhances your business operations.

For more information

To learn more about IBM K-12 Security Services – Vulnerability Assessment and Penetration Testing, please contact your IBM Marketing Representative.
For more information on all our IBM K-12 Consulting and Professional Services, visit: www.ibm.com/industries/education/canada-k-12-service-briefs

IBM Corporation
3600 Steeles Ave. East
Markham, ON L3R 9Z7 Canada
December 2017 (Revised)