zayo CYBER SECURITY

Penetration Testing

HOW MUCH RISK IS YOUR ORGANIZATION WILLING TO ACCEPT?

Penetration testing is important for organizations which need to meet regulatory requirements for security or adopt a specific information security management standard.

For some organizations, these tests are mandatory as part of governance rules or guidelines widely adopted by an industry, for example, with PCI Data Security Standard (DSS) requirements. Other organizations may require penetration tests in order to adhere to a specific security control framework like the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS). Many still conduct penetration tests on a regular schedule and/or after system changes. Numerous published studies confirm it is one of the most effective security controls. Every organization should consider including some form of penetration testing as a part of their overall security program.

Zayo Professional Services

Penetration tests can encompass a range of activities and outcomes. They can target access methods, devices on a network, or applications existing in the cloud, on the web, or in the network. It can be difficult to hire and maintain the specialized staff necessary to perform the recommended annual or semi-annual penetration tests. Many companies of all sizes and industries leverage Zayo's decades experience with, and understanding of, complex network infrastructure and how to secure them. As part of our suite of Professional Services, we work with companies to provide one-time and ongoing penetration testing services.

Vulnerability Assessment

Penetration tests are most effective when paired with a vulnerability assessment. This method, known as white box testing, gives testers significantly more information about the environment they are auditing and provides the highest chance of discovering exposures.

Scope of Testing

For any penetration test, success requires a clearly defined scope and goals. Furthermore, a risk-based approach to defining the scope of testing is needed. Mission-critical infrastructure and systems containing the most sensitive data are prioritized above everything else. Zayo helps customers review the big picture and devise a cost-effective plan to maximize their penetration testing return on investment.

- Network and Security Appliances (Routers, Switches, Firewalls, etc.)
- Windows / Linux / Unix Workstations and Servers
- Commercial Off-The-Shelf Web Applications
- Custom Web Applications
- Application Programming Interfaces (API)
- Cloud Infrastructure

About Penetration Testing

Regular penetration testing is a recognized best practice for any information security program.

Third party penetration testing is mandated by PCI DSS and satisfes requirements for GLBA, HIPAA, SOX, NERC CIP and FISMA compliance.

Service Benefits

- *Obtain a true understanding of your security and risk posture*
- *Leverage our deep knowledge base gained by delivering services to thousands of customers*
- *Understand the techniques used by attackers*
- *See your organization as it would be seen by a cybercriminal*
- *In-depth reporting, relevant to your organization and stakeholders*
- *Comply with industry regulations and information security best practices*

GLOBAL HQ
1805 29th St.
Boulder, CO USA 80301
+1 866 364 8033

CANADA
200 Wellington St. West
Suite 800
Toronto, ON, M5V 3G2
+1 844 687 0000

FRANCE
19/21 Rue Poissonnièrre
75002 Paris
+33(0)1 79 97 96 46

UK
4th Floor, Harmsworth House
13-15 Bouverie St.
London, EC4Y 8DP
+44(0)20 3326 9500

zayo.com/ca
@Zayo_Canada

zayo CYBER SECURITY

Penetration Testing

Testing Options

There are many types of penetration testing. Zayo will help customers explore their options to determine the number and type of tests best suited to meet their needs.

- Black-Box Testing
- White-Box Testing
- Red Teaming
- Blue Teaming
- Purple Teaming

Independent 3rd-Party Audit

An important tenet of information security is the separation of duties. This principle requires that two or more parties be involved any security control to reduce the risk of human error or malicious activity. As such, Zayo recommends organizations managing their own security infrastructure don't perform their own penetration testing. Zayo has partnered with reliable firms throughout North America and Europe to ensure separation of duty, especially in cases where Zayo is managing the security infrastructure on the customer's behalf.

Your Penetration Testing Report

For organizations to derive any benefit from penetration testing, they must enact recommended changes to their processes and tools as recommended by the resulting report. Zayo's report includes a plain language executive summary of the test results, making it clear to management what needs to be done, without the need to decipher any technical jargon.

Each report also includes a detailed technical summary of the testing actions taken, including which systems were breached, which vulnerabilities were exploited, and what level of access was gained. For each successful breach, Zayo provides a root cause analysis, a description of the risk associated with the vulnerability, and remedial recommendations.

For more information on how Zayo Cyber Security can help your business meet its cyber security requirements, contact us by:
Email: cybersecurity@zayo.com
Phone: 1.844.687.0000
Or visit our website at zayo.com/ca/services/managed-cyber-security