ORGANIZATION SECURITY TESTING

Test your organization's security with the insight of a real attacker using an arsenal of offensive methods!

Offensive security methods provide a realistic assessment of an organization's protections. CENSUS Security Testing Services examine all components of an IT infrastructure against publicly known and previously undisclosed (0-day) vulnerabilities and attack vectors, without disrupting the organization's processes.

CENSUS offers the following Organization Security Testing Services as both independent and combined security testing modules, based on field best practices.

TIGER TEAM

Tiger Team testing is the ultimate way to execute an asymmetric attack against an organization. The Tiger Team targets the core business, testing all layers of the organization's security architecture, making every effort to remain undetected and sharing information about the attack only with upper management.
This black box-only engagement does not have a specific project plan or scope. The attack may occur anytime.

RED TEAMING

In a Red Teaming assessment, CENSUS consultants adopt an adversary mindset and simulate different threat agents of the organization, ranging from motivated cyberwarriors to internal spies and reckless employees. The team identifies vulnerabilities in the utilized technology, the corporate processes and the human element, exploits gaps in the organization's security model and attacks the in-scope assets. All aspects of an organization's attack surface (deployed software solutions, specialized hardware as part of the organization's products, external network perimeter, internal network segmentation, cloud infrastructure, on-premises physical controls, corporate employees) may be targeted according to the project scope. A predefined project plan for all Red Teaming operations includes what information should be shared with the team, as decided by the client.

PENETRATION TESTING

Penetration testing is the process of testing an IT infrastructure for security vulnerabilities in a controlled manner. The testing is conducted against specific organization assets or infrastructure components. The process varies according to the degree of knowledge provided by the client (Black-Box, White-Box, Grey-Box testing, etc.); a mixture of these degrees of knowledge can also be applied for evaluating the effects of both insider and outsider attacks. Providing more knowledge can also shorten the time required to assess a system. Penetration testing evaluates the organization's controls deployed as part of an in-depth security model, and its main target is to unveil previously unknown attack paths that could be used to affect the confidentiality, integrity, and availability of the targeted assets.

WEB APPLICATION TESTING

Web applications are the most common entry point of an organization's security perimeter. This process examines all functions and API calls of a Web Application (and their effects on a user's browser), all layers of its stack (from the application itself to the underlying operating system) and all tiers of its architecture (from the front-facing web server and load balancer to the back-end database and application server or to the distributed cloud infrastructure). User privileges and role-based testing can also be included in the assessment.

MOBILE APPLICATIONS, CLIENT-SIDE SOFTWARE & MDM TESTING

Mobile or client-side applications are usually provided to corporate employees in order to facilitate the organization's inner workings. Similarly, Bring-Your-Own-Device (BYOD) policies allow employees that use Mobile Device Management solutions to connect their own devices to the corporate network. The testing team examines the security posture of these solutions and searches for vulnerabilities that can be used to gain further access to the organization network infrastructure.

NETWORK AND CLOUD INFRASTRUCTURE TESTING

Network Infrastructure Testing examines all measures and controls used to implement security policies in an organization's network architecture, in order to assess the provided protection. These include:

- Network Firewalls: Firewall-bypassing methodologies are used to ensure that the implemented rules offer maximum protection.
- Routers & Wireless Access Points: The network routing infrastructure is tested for security vulnerabilities, malfunctions and misconfigurations.
- Cloud Infrastructure Controls: The team evaluates the attack surface of the cloud deployments, and examines integration with third-party services, such as monitoring and authentication controls for data exposure.
- Workstation Device Management Controls: The team assesses the enforced limitations of the corporate workstations and identifies attack paths that could escalate user privileges.
- Network Segmentation Controls: The enforced access privileges between different corporate VLANs are examined for security gaps.
- Intrusion Detection / Prevention Systems: Among others, polymorphic and metamorphic techniques are used to assess the quality of the detection engines found in the client's infrastructure. The IDS/IPS themselves are also examined for vulnerabilities using a wide variety of payloads.

SOCIAL ENGINEERING

Social Engineering tests the security awareness of the target organization's personnel. Social Engineering attacks are performed through remote channels (landline/mobile telephones, VoIP, e-mail, "snail" mail) and local means. This module extends security testing to the human factor, exploiting the personnel's knowledge, privileges and habits.

PHYSICAL SECURITY TESTING

For the holistic assessment of an organization's security, CENSUS offers a Physical Security Testing module which evaluates the reliability and integrity of physical security controls, such as access authorization mechanisms for restricted zones. Physical Security Testing also assesses the effectiveness of the implemented physical controls in terms of:

- Protecting sensitive information & physical assets.
- Collecting sufficient evidence that may later be used for intruder prosecution.

CENSUS
Cybersecurity Engineering

www.census-labs.com

USA
607 Boylston Street, Suite 165L, Boston, MA 02116
T. +1 8882 029 846
E. usa@census-labs.com

UK
Unit 2.15 Barley Mow Centre
10 Barley Mow Passage
W4 4PH, London
T. +44 1293 324 069
E. uk@census-labs.com

EUROPE
128 A. Siggrou Ave.,
Athens 117 45, Greece
T. +30 2102 208 989
T. +30 2102 208 990
E. eu@ census-labs.com

ABU DHABI
Office 110 - First Floor
Incubator Building
Masdar City, Abu Dhabi
United Arab Emirates
T. +971 8003 110 047
E. uae@census-labs.com

DUBAI
Unit GA-00-SZ-L1-RT-201,
Level 1, Gate Avenue - South Zone, Dubai International Financial Centre, Dubai
United Arab Emirates
T. +971 8003 110 047
E. uae@census-labs.com