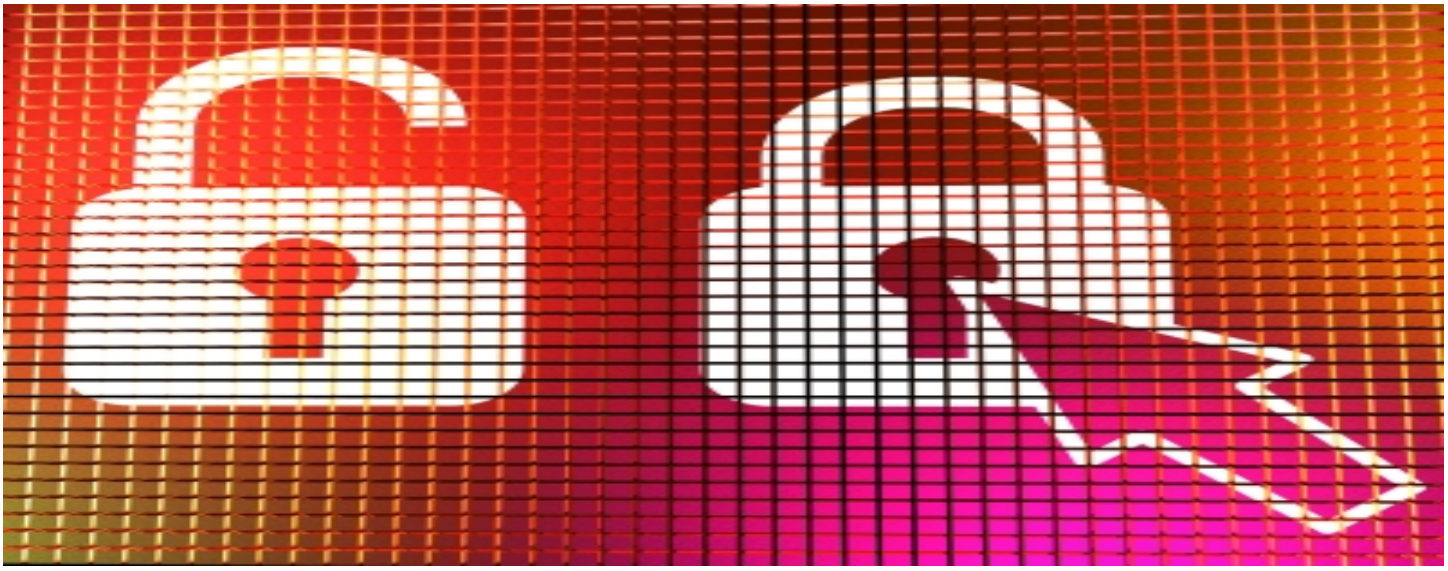
Vulnerability Assessment by Axxera



"Nine out of ten successful hacks are launched against unpatched computers."

Why Do You Need a Vulnerability Assessment?

While it is nearly impossible to protect critical IT systems from unknown vulnerabilities and unknown threats, it is possible to protect against known vulnerabilities and known threats. Axxera's Vulnerability Assessments help identify known vulnerabilities and system misconfigurations, which could result in network breeches.

2015

Axxera Security Services

Axxera's Security Professional Services core premise is that Information Security solutions should be based upon each client's fundamental business models and processes. Axxera's consultants work in collaboration with a client's staff to determine both high level strategic threats to critical business assets, and specific technical vulnerabilities.

Axxera Vulnerability Assessment

Axxera begins with the discovery of the customer's internet presence. This includes the discovery of e-mail domains, e-mail addresses, DNS domains, registered network blocks, and hosts. This information is cross-referenced with web searches for public servers and user e-mail addresses. Discovered targets are verified with the customer before any active scanning is performed. The customer has ultimate control over the systems evaluated.

A combination of common and advanced network and host discovery techniques are used to find internet connected devices even when firewalls and filters are blocking traditional host discovery techniques. The system discovery and vulnerability scanning techniques are always as sophisticated as current attack technology. As the "State of the Hack" changes, so does Axxera's Vulnerability Assessment technology.

- **Host Service Scanning** Physical network design and routing are determined through use of IP scanning tools, as well as simple network management protocol (SNMP) queries for network devices. The team uses IP and/or UDP scanning tools to perform discovery of systems within the customer's IP address space. Each system that is discovered is scanned for active network services using a combination of public, commercial off the shelf, and proprietary scanning tools. These scan results reveal the hosts which are accessible from the internet and the active services which are permitted to pass through firewalls and routing filters.
- **Vulnerability Identification** After host discovery, each identified system is probed for applications that respond to network stimulation. Information about the operating system, network applications, and system configuration is collected and analyzed. Potential vulnerabilities in the systems are verified and categorized by risk. Each exposed system is evaluated for vulnerabilities that reduce its security profile.. Once all active hosts and services have been identified, Axxera probes these services to identify their make and versions, and cross-references the active services against a database of potentially vulnerable services.

Detailed Assessment Reports

The Vulnerability Assessment Report:

- Identifies the systems being tested
- Describes the network protection scheme
- Lists the active and accessible services on each system
- Describes specific vulnerabilities for each applicable system

Each specific vulnerability is accompanied by a description of its potential to permit compromise or denial of service, as well as recommended actions to correct them. The report also documents any recommended modifications to the gateway or the external network topology or architecture, and explains why the change is necessary.

The assessment is truly a snapshot in time. Therefore, in addition to the findings, recommendations and conclusions, Axxera includes as much of the collected data as possible. Reports are typically delivered within two weeks of assessment conclusion.

AXXERA INC
5251 California Ave, Suite 140
Irvine, CA 92617

PHONE
949-238-7500

WEB
http://axxera.net