Choosing the Right Security Assessment

An **internal test** is performed from the point of view of a possible inside threat. The tester will imitate someone inside the company, such as an employee or partner, and will be allowed to utilize privileged information that a specific employee/partner should be able to access under normal circumstances. From there the tester will determine whether an employee/partner can access priviledged information that they should typically not be allowed to see.

Many threats come from within the organization's firewall - from employees with access to privileged information. These threats, (while often not malicious in their intent,) can have the same damaging results as an external attack from a malevolent hacker. In an internal test, the ethical hacker is given network authorization equivalent to that of an employee or guest user, and conducts the penetration or vulnerability test from the vantage point of users within your own network.

III. Determine testing type and frequency.

A comprehensive technical security assessment will include internal and external vulnerability assessments, penetration testing and web application testing. It will afford the organization the opportunity to:

- Protect its reputation
- Protect data & assets
- Protect against data breach
- Demonstrate third-party verification
- Execute corporate due diligence
- Ensure customer privacy
- Guarantee regulatory compliance
- Comply with legislative mandates
- Reduce risk exposure
- Validate existing security measures

It is up to your organization to determine what an acceptable level of risk may be, and what areas you want to ensure are safeguarded.

Internal or External?
If your most common threats are believed to be from the outside (as in most organizations), then an external test is going to be the most effective solution to meet your needs. Once a penetration is achieved, the tester can work from inside the network to find more weaknesses. If your greatest potential threat is from those who are inside your company, then the internal test may be the best place to begin.

An ICS Whitepaper

Choosing the Right Security Assessment

When and how often?
Industry standards suggest that vulnerability assessments be performed quarterly, while network penetration tests should be performed at least bi-annually. Web application assessments should be performed at least annually and whenever new applications are added. Remember, each time you upgrade your system or your software, you open new portals for possible exploitation. To protect against new threats, you should consider running security assessments before and after any new software is introduced into your infrastructure.

Another important element to consider is timing.
Penetration Tests have the potential to cause interruptions for the daily work routine of your employees. Because of this, you must balance security with convenience. An important factor to consider is whether or not the assessment will hinder your employees, your network, or your infrastructure. Testing has the potential to disrupt normal network operations if the tester is successful. Therefore, it is important to know what protocol the security firm has in place in case the network is compromised. Every information security firm should provide your organization with "rules of engagement" to mitigate the possibility of network interruptions and eliminate any surprises. If you require a less obtrusive method, then a vulnerability assessment may be the best solution for you. However, if your company requires that you actually test these threats and you need a higher level of confidence in your security posture, then a penetration test is the best approach for your company.

IV. Overview

The following service comparison chart can serve as a good starting point for most organizations in understanding the various types of security assessments and the recommended frequency with which each should be performed:

Service Comparison | ICS Technical Security Offerings	Technical Security Assessment	Web Application Assessment	Vulnerability Assessment	Network Penetration Test
Protect Corporate Reputation	●	●	●	●
Third Party Verification	●	●	●	●
Protect Data & Assets	●	●	●	●
Data Breach Protection	●	●	●	●
Corporate Due Diligence	●	◑	●	●
Cost Justification	●	◑	●	●
Customer Assurance	●	●	◑	●
Compliance	●	●	●	◑
Legislative Mandates	●	●	●	
Reduce Risk Exposure	●	●	●	
Validate Existing Security Measures	●		●	●
Regulatory	●	●		
Recommended Frequency		at least annually *and as new applications added*	quarterly	bi-annually

About ICS, Inc.

Integrated Computer Solutions, Inc. (ICS) is a full-service information technology and IT security consulting and professional services firm headquartered in Montgomery, AL with operating locations throughout the United States.

Established in 1997, ICS provides a robust portfolio of technology and information security services that combine comprehensive strategy with cutting edge security. Our services provide a balance of cost and quality that enables our clients to maximize their return on IT investments.

ICS has an established track record of providing enterprise technology and security services to a wide range of Federal, State, and Fortune 1000 clients.

ICS Inc. Integrated Computer Solutions
ISO 9001:2015 Certified

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com
www.ICSInc.com