



**« The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards. »**  
— Gene Spafford

## Intrusion Testing Services

*Information systems are facing a wide variety of threats that are constantly evolving over time. Having an adequate security environment in place and following security best practices or policies for are key elements to ensure the safety of your systems. But do you know what risks your infrastructure is facing? And how confident are you that the implemented approach suffices in protecting your assets? Have you (recently) been the victim of a cyber attack?*

*Intrusion testing is an efficient way of determining whether your infrastructure is prone to hacker attacks and to what extent the existing risks may damage your organization. By recurring intrusion tests, you also get a view on the overall evolution of the organization's risk level.*

*Aszure offers a broad range of intrusion testing services, each one targeting a specific aspect of the infrastructure. This is a non limited list of our intrusion tests: network intrusion testing (external, internal), systems intrusion testing, web application testing, wireless testing and VOIP testing.*

### Risk Management Framework



Risk management is the ongoing process of identifying risks and implementing plans to address them. Risk is determined by considering the likelihood that known threats will exploit valuable assets and the impact if an exploit is successful. It is very important to know where to apply available resources to mitigate risk in an efficient and cost-effective manner. That's where risk assessments come in the picture. Risk assessment is the part of the ongoing risk management process that assigns relative priorities for mitigation plans and implementation.

### Aszure Assessment Program

Aszure's Assessment Program situated in Step 4. Assess Controls. Aszure performs activities in all 6 steps of the risk management framework and can help in implementing such a framework within your company.

This program has 4 pillars:

- Logical tests
- Physical tests
- Social tests
- Strategic tests

Logical testing concerns everything on the network, system and application layer. This includes intrusion testing (external, internal, web applications, database systems...), system auditing (servers, workstations, network components...), code reviews, architecture reviews.

### About Aszure

Aszure is specialized in operational risk management consultancy and staffing. Operational risk management, information security, business continuity and compliance to laws and regulations are major cornerstones of our services.

Aszure assists its customers with the incorporation of operational risk management at all levels and in all areas of their organization, including day-to-day operational decisions. No decision should be taken in any organization without applying proper operational risk management. It can be applied throughout the entire life cycle of any activity or project. In order to minimize risk, it is however preferable to apply operational risk management at the beginning phase of a project or operational activity.

### About Aszure Academy

Aszure offers an extensive education and awareness program through the Aszure Academy which covers several open classes, events and customized education experiences.

### Contact

For further and additional information, please contact us on Tel. +32 (0)9 243 10 20 or [info@aszure.com](mailto:info@aszure.com)

Aszure's general terms of delivery are applicable to all our services.

In physical and social tests we try to exploit the human factor to gain access to your information and/or your network.

Strategic tests are higher level tests and can be risk analysis, Business Impact Analyses, High Level Risk Management Audits, Gap analysis between your situation and regulations/standards (ISO27002, CBFA guidelines, PCI...)

We can assist in setting up such an assessment & intrusion program and assisting your Audit department in tackling these different pillars.

### **Network Intrusion Testing**

We will attempt to discover your network infrastructure and try to gain access to it. There are typically two types of testing: external network intrusion (from the internet) and internal network intrusion (from the local network). Although most organizations implement a good perimeter security, attackers are not necessarily acting from the Internet: they might proceed from hijacked company devices and accounts (laptops, PDA's, VPN accounts ...) or they might even be employees themselves. It is therefore important to assess the infrastructure's security from several different network locations: the Internet, the company LAN, wireless connection, VPN ...

### **System Intrusion Testing**

With system intrusion tests we try to detect, attack and exploit vulnerabilities on systems and devices of your infrastructure. Depending on the exploited vulnerability, an attacker can acquire privileged access to a system and use it as a gateway to other machines of the internal network. This test is useful to assess the risk of your critical system and, in addition, to identify how much damage can be done by systems which are supposedly trusted.

System intrusion tests are generally combined with system audits, where an in-depth analysis of specific system and service configurations is done.

### **Web Application Testing**

Web applications are prominent business enablers which grow more and more complex over time. Unfortunately, their increasing complexity goes paired with the widening of the attack surface they are facing. To name a few, the main threats targeting web applications are SQL code injection, Cross-Site Scripting (XSS) and cookie manipulation.

### **Wireless Testing**

When badly configured, wireless access points can provide an attacker with a direct access to the internal network even if he is not located inside the company's premises. In the first phase of the test, we try to establish a connection with your wireless infrastructure. When successful, the second phase consists of an intrusion attempt where we try to identify which parts of the network are accessible to wireless users. If possible, the discovered risks are mapped to their eventual business impact.



### **VoIP Testing**

Although Voice over IP telephony offers great opportunities for cost reduction within corporate environments, a lack of good protection and configuration of its setup might put your whole infrastructure at risk. Attackers may misuse the voice LAN to access an organization's internal network, to intercept voice and video calls or even to use it as a relay for expensive communications.

We will investigate on the security of the VoIP setup on both operational and architectural level. This involves an analysis of the overall protection of the VoIP components and their integration in the organization's environment.

### **Deliverables**

You will be provided with a comprehensive multi-level reporting ranging from management level to detailed technical level. All discovered issues and weaknesses will be described and discussed in these reports, as well as the possible methods of remediation to mitigate the risk factors. A list of improvement actions which will increase the overall network security level will be included as well. You will also receive a list of tests that have been performed together with their outcome.

### **Added Values**

Our trained and certified security consultants are specialized in ethical hacking techniques, among which detecting, attacking and exploiting vulnerabilities. We have members in various local security chapters, like OWASP and ISSA.

We strive to deliver complete and accurate, yet understandable reports of the conducted tests. We strongly believe that adopting your business jargon is the best way to assure an unambiguous description of our assessment.

When an intrusion test is combined with a business impact analysis, we map the detected issues on an estimation of their effect and remediation costs. We can thereby coach you in the selection of the best fitting remediation for the discovered issues.

Aszure's procedures for assessments are based on strict guidelines and methodologies such as OSSTMM, OWASP, ISSAF and the NIST 800-53a and 800-115.

***“One of the tests of leadership is the ability to recognize a problem before it becomes an emergency.”***

**— Arnold Glasgow**

Interested in world-class education and training: visit the website of the Aszure Academy ([www.ascureacademy.eu](http://www.ascureacademy.eu)).

For more information, please contact:

Tel.: +32 (0)9 243 10 20

E-mail: [info@ascure.com](mailto:info@ascure.com) [www.ascure.com](http://www.ascure.com)  
Bijenstraat 16-17, B-9051 Ghent, Belgium

