# Vulnerability management

In today's world, where IT technologies have penetrated every pore of business life, maintaining business and IT systems is a constant challenge. With increased threats in terms of cyber security, it is important that all changes include accurate security controls.

## What does system vulnerability testing represent for Ibis instruments?

As a Hi-tech company, Ibis instruments understands the need to be agile in a business sense, with the purpose of meeting the ever-increasing needs of the information society, introducing new systems, technologies and new ways of doing business in order to gain competitive advantage and increase business efficiency. Our approach to testing system vulnerability maximizes the possibility of reducing business risk arising from using IT technologies, and all with the request that the said testing has no impact on the company's daily business.

Our approach to testing is based on the system vulnerability assessment regardless of the incoming threat vector – whether the attack vector is external (Internet attacks) or internal (internal attacks). Using our services in regular intervals, our clients have the opportunity to stay one step ahead of malicious users, enabling IT systems to develop and grow together with the company's business. Our approach to testing the safety of information systems provides a detailed, quality service, with enabling the flexibility necessary for testing the wide specter of IT systems.

## Challenges placed before IT sectors of companie

Organizations depend on business and IT systems which must act efficiently and competitively in this digital age. These systems are often upgraded or replaced, whereby even the smallest change may cause new vulnerabilities. Even though we believe that every company puts in significant effort in order to ensure that the systems function efficiently and that the necessary security controls are built in, we have to mention that many organizations do not always test whether security controls are being implemented properly or whether the particular measures are sufficient or correct. The result of this is that the vulnerability will be discovered only when security is compromised, leaving the organization open for a possible regulatory penalty, financial loss, damage to reputation or theft of critical information or intellectual property.

# Vulnerability testing: How is it done?

Since any kind of protection can be penetrated after a while and with required skill, we have to say that risk is always present. Based on this, we can deduce that the essence lies in understanding and accepting risks arising from the company's business and which the company itself must understand.

Our services help the organization to:

- Identify the technical and architectural vulnerabilities that may be used by malicious users
- Evaluate the company's ability to respond to attacks
- Ensure the possibility of detecting certain vulnerabilities that cannot be detected by automated tools
- Prioritize on the basis of the importance of findings with the purpose of correcting detected vulnerabilities
- Provide recommendations based on its practice of many years, as well as industrial recommendations
- Evaluate the company's ability to detect and respond to attacks

All our activities are based on the most important and recognized testing methodologies, standards and recommendations, including OWASP, NIST, special recommendations, instructions, as well as different publicly or privately available sources.

After our assessment we provide the following:

- Management-level summary
- Results that give clear indicators of what actions need to be taken
- A written report on performed activities with clear findings
- Clear and precise report for the management and the company's internal IT
- The summary report contains the following:
  - Priority of each of the detected vulnerabilities
  - Possible activities with the purpose of resolving detected problems
  - Findings grouped according to levels of risk

# Advantages of system vulnerability testing

Our basic goals are to prove, with the highest possible level of certainty, that the system is either vulnerable or not intended for certain security threats, in order to provide clear recommendations for resolving vulnerabilities, which are suited for the company with the purpose of ensuring a safe work environment for further company development, both in the internal and the external context.

Ibis Instruments
Measurement & Telecommunication Systems


**Ibis Instruments Belgrade**
Tošin bunar 272, 11070 Belgrade, Serbia
Office: +381 11 7152 200, Fax: +381 11 7152 201
e-mail: info@ibis-instruments.com
www.ibis-instruments.com

**Ibis Instruments Banja Luka (branch office)**
Jovana Dučića 37, 78000 Banja Luka
Office: 387 51 223 840, Fax: 387 51 223 841
e-mail: office-bl@ibis-instruments.com
www.ibis-instruments.com

**Ibis Instruments DOOEL import-export Skopje**
Veljko Vlahović 1-2/2, 1000 Skopje, Macedonia
Office: +389 2 321 5700, Fax: +389 2 321 5700
e-mail: info@ibis-instruments.mk
www.ibis-instruments.com/mk

**Telecom Instruments Romania**
Azur 2 - House F17, 31-33 Emil Racovita Street,
077190 Voluntari, Ilfov, Romania
Office: 4 021 320 3356 , Fax: 40 21 2110884
e-mail: office@telecominstruments.ro
www.telecominstruments.ro

**Telecom Instruments Ltd. Bulgaria**
Address: 15, Sveti Naum Blvd., 1421 Sofia, Bulgaria
Office: 359 2 969 1060, Fax: 359 2 969 1080
e-mail: office@telecominstruments.bg
www.telecominstruments.bg