INFORMATION SECURITY AUDIT

DO YOU MEET THE CYBERNETIC LAW REQUIREMENTS?

- We will screen your security policies and guidelines.

IS YOUR NETWORK SAFE FROM INTERNET ATTACTS?

- We will perform a penetration test in practice.

CAN YOU TRUST YOUR SECURITY SOLUTIONS?

- We will verify that the setting of your technologies complies with your security policy.

IXPERTA

SECURITY AUDIT WILL OPEN YOUR EYES

- Verifies that your present security solutions are really protecting you.
- Proves that you meet the requirements of the legislature and of your business partners.
- Helps to maintain your security policy up-to-date.
- Shows you where to invest the security equipment effectively.

Security Technology Audit

- Inspects security solutions such as firewall, IPS or VPN.
- Proves that your security solution configuration corresponds to current trends in the field as well as your own security policies and guidelines.
- Provides proposals for their improvement.

Security Process Audit

- Performs the required security policies and guidelines.
- Provides certification according to ISO 27000 standards family or to the cybernetic security law.
- Appropriate for both cases to be performed by an independent 3rd party.

Security Scan

Vulnerability Scan

- Reveals vulnerabilities in an IT system. The aim is to remove those weak points and take protective measures to secure the system.

Penetration Test

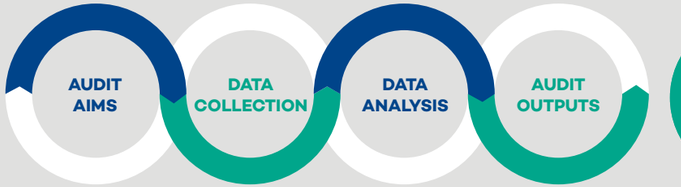
- Discovers the entire security level of chosen IT systems. It will not only screen the system itself, but also all levels of protection from it (e. g. firewall).
- This test can be performed by an independent 3rd party as well.

SECURITY AUDIT HAS ITS RULE

The security audit has a firm order of steps and activities given by methodology. During the audit, we proceed by ISO 27006, 27007 and ISO 19011 standards. You can be sure insofar that nothing significant would escape our attention.

In the audit program, the organization will designate the targets of each audit which will specify the audit scope, criteria and methods. During the audit, we will gather and analyze the necessary data, and compare them with the audit criteria. The output is a final report discussed and agreed with the customer and including parts intended for particular roles (CEO, CFO, CIO, CTO, IT specialist) along with a needed detail extent.

The audit output will assist the management in planning the right investments in information security, and to invest where really necessary, and not invest uselessly without real effect.



IXPERTA

Order
the first scan of vulnerabilities free of charge.

HelpDesk 24 x 7

t: +420 266 063 333 – Czech Republic
t: +421 232 292 700 – Slovakia
e: helpdesk@ixperta.com

InfoLine

t: +420 266 061 111 – Czech Republic
t: +421 232 292 722 – Slovakia
e: info@ixperta.com

PRAHA BRATISLAVA BRNO OSTRAVA ŽILINA

www.ixperta.com