ISC – Instant Security Check

ISC – Instant Security Check

What is the status of your IT-security?

Most organizations today have competent IT-departments that meet the business requirements on availability and functionality. But despite well-functioning IT-support, the IT-security is often lacking. It is only when an incident occurs that the vulnerabilities are noticed – and by then it is often too late.

Previous year's trend has shown that IT-security is a strategic issue for most businesses – and therefore a management issue. With an overview of current IT-security status, management will be able to prioritize and lead the organization effectively towards adequate IT-security.

Everdon Security Corp is a trusted and reliable business partner for cyber security services focusing on supporting corporations with sensitive security issues related to espionage and information leakage.

Everdon Security

ISC – Instant Security Check

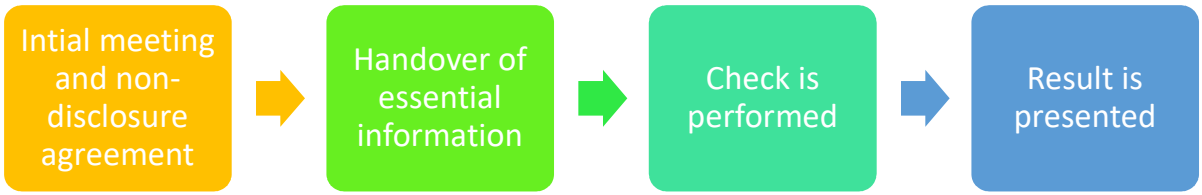
Everdon Security has developed the concept *ISC – Instant Security Check* to meet the need of a quick overview of the IT-security status of an organization. The ISC can be performed as a stand alone quick-fire test to ascertain an overview of the current security posture. The check is conducted to provide a quick base line for the security status and can provide the basis of in-depth security audits and targeted penetration tests. The ISC is developed specifically to provide a quick overview of the most important aspects of IT-security. ISC quickly evaluates:

- Credential management
- Resilience against common attack vectors
- Vulnerabilities in system components
- Architectural robustness
- Ability to detect attacks

Instant Security Check is based on, and adheres to the quality requirements of the OSSTM (Open Source Security Testing Methodology)

ISC – Instant Security Check

How an instant security check is conducted



At the initial meeting, the steps of the ISC are presented and the roles that needs to be accessible during the test is clarified. A non-disclosure agreement concerning partial- and end result of the check is also met and signed at this point.

In order to conduct the ISC, Everdon Security needs access to certain information e.g. IP-ranges for the target environment, credentials so that a vulnerability scan can be performed and a list of e-mail addresses for usage in a phishing campaign. Furthermore, Everdon Security needs access to the technical staff that is able to answer questions about the environment.

Duration and Limitations

The ISC is conducted over a period of 2 days and includes a visualized protocol of the overall IT-Security and subsidiary parts of the IT-environment.

The vulnerability scans cover a maximum of 100 active IP addresses.

For additional information, contact:

Do not hesitate contacting Everdon's Snr Cyber Security Experts for in-depth technical details and scope including the visualized result of the current IT-Security levels in your organization.

Johan Öhman, CTO, +46 70 825 00 82, johan.ohman@everdonsecurity.com

Patrick Bladh, Senior Cyber Security Expert, +46 73 255 17 13, patrick.bladh@everdonsecurity.com

Per-Olov Humla, CEO, +46 70 880 88 70, per-olov.humla@everdonsecurity.com