Deloitte.

Cyber Risk services

Our Cyber Risk Services group is designed to provide practical support to our clients in the region and internationally. Our professionals serve clients in all aspects of IT security.

Services

We provide services in all aspects of cyber risk to our clients, including:

- **Information security**
  - Penetration testing and Vulnerability assessment
  - Security Risk Assessment
  - Information security design
  - Data Leakage Prevention (DLP)
  - Compliance (e.g. ISO27001, COBIT, PCI DSS)
- **Forensic services**
  - Incident response
  - Computer forensics
  - Fraud investigation

Penetration Testing and Vulnerability Assessment

Many organisations have invested substantially in a web presence in order to provide a better and interactive service for their customers, suppliers and business partners. The frequency and level of sophistication of attacks against Internet facing systems has grown spectacularly over the last couple of years, whilst at the same time, the level of skills and knowledge required to carry out these attacks has decreased.

We provide state-of-the-art security services to reveal how client data are protected. Should these systems be Internet facing or internal ones, web-based or client/server applications, run on mainframe or Intel-based system, our team is capable to provide the highest quality to check their real security controls.

Security Risk Assessment

We carry out IT security risk assessment in the client organisation or about specific systems including the following tasks:

- Threat analysis: identifying threat agents and threat scenarios, which can have adverse effect on the target
- Risk rating: assign clear, understandable and quantifiable metrics to the risks identified
- Mitigation: develop actions plans including risk reduction, avoidance and transfer

We perform the security risk assessment in a manner compliant with the relevant international standards (e.g. COBIT, ISO 27001).

Information security design

Information security is a critical component in an organisation's life. We offer services to design information security at our clients:

- Analyse the current process against best-practices in security design.
- Define an updated process which includes security in all phases: design, implementation, testing and operation.
- Assist the organisation in developing methodologies, templates, test-plans to implement the security.
- Enable organisations to ensure that 3rd party suppliers meet their requirements by implementing guidelines, assessment methodologies and processes.

Data Leakage Prevention (DLP)

The serious impact of data breaches is prompting organizations to take measures. Deloitte offers an approach within all areas of the organization: governance, people, process, technology:

- We first look at understanding the critical information the client organization processes, where it comes from, how it is stored and sent.
- Then we undertake a controls review to assess who has access to it, which applications process it and what controls are in place.

Compliance

Our team provides services related to compliance in the IT security area including:

- Gap analysis: gain an understanding over where the organisation currently is in relation to the requirements regarding compliance
- Action plan and implementation: develop the approach and execute the tasks to achieve compliance
- Quality assurance: ensure that compliance is achieved in the most efficient way

Amongst other standards, the most important drivers in compliance are:

- ISO 27001 – Information technology – Security techniques – Information security management systems
- COBIT – Control Objectives for Information and related Technology
- PCI DSS – Payment Card Industry Data Security Standard

Forensic services

Our computer incident response experts provide:

- Strong, remote, third-level support – to help the management assess an incident or threat and provide guidance for tactical risk mitigation.
- Remote or on-site expert help for immediate incident containment.
- A professional team for root-cause analysis, continuous improvement of incident response procedures, and assistance in complex investigations.
- Specially trained experts in forensics to ensure legally accepted evidence for litigation.
- Fraud investigation

Environment

Our working environment has been designed to meet the strictest client requirements:

- The group operates in an isolated office area, with separated internal network.
- We enforce strict access control both physically and logically to all the assets on a need-to-know and need-to-access basis.
- We encrypt data we handle both during communication with our clients (e.g. PGP or S/MIME) and storage.

Contact

Lajos Antal

Deloitte Central Europe Lead Partner
Cyber Risk Services
Tel: +36 (1) 428 6402
Mobile: +36 (20) 981 5304
Email: lantal@deloitteCE.com