alliuris

ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

IT-Security Management

Ulrich Herfurth, Lawyer in Hanover, and Brussels
Eduardo Isaac Soto Barrera, Lawyer (Mexico) Mag. iur. (Mx), Mag. iur. (D), Hanover

July 2021

The security of the IT system and the protection of company data is essential for every company. According to industry findings, the total loss of data leads to the insolvency of the affected company in 90% of cases within 12 months, either because the company processes are massively damaged or because essential data stocks on production and customers have been lost.

The causes can be easily distinguished: they are either accidents or attacks. In the case of accidents, the greatly increased complexity and networking of IT systems lead to an ever-broader impact and greater damage. Attacks, in contrast, can be divided into internal perpetrators and external perpetrators.

The number and severity of external attacks has increased massively in recent years: security gaps are found in IT systems again and again, and attackers are now exploiting this within the framework of organised crime with rapidly increasing numbers.

Cybercrime is now organised like classic industry: the perpetrators can use standard software for malicious encryption, process it and infiltrate it into regular distribution systems. The most successful model is blackmail with random software: the first step is sabotage; by encrypting the files, they can no longer be used. The second step is blackmail: if the company does not pay a ransom (usually in cryptocurrency), the files remain inaccessible.

This concept is used hundreds of thousands of times, starting with masses of small users for a ransom of less than a thousand euros up to large companies that not rarely pay a ransom of several million. Many attacks and payments remain unknown because the victims do not want to provoke any imitations.

The security of IT systems and company data is therefore essential and a high-priority task for company management.

For managing directors, neglecting the required IT security regularly means a breach of duty of care and thus a liability risk vis-à-vis the company.

The requirements for the necessary IT security include the technical IT system itself (incl. servers, cloud systems, etc.), but also the IT operation (operational part) and the IT security management (risk identification, guidelines, and monitoring).

A secure IT system

The IT system includes all computers (clients and servers), industrial controllers (production equipment, mobile phones, smartphones, tablets, end devices such as scanners or printers connected to these PCs), IoT components (webcams, smart home components or voice assistants), routers, switches, firewalls, and more.

Each of these systems must be fully recorded and described, especially where and how they are used, and which people are authorised to access them and to what extent.

The management must establish organisational guidelines for this, the BSI (Federal Office for IT Security) offers corresponding information on measures, at least

- Criteria for the acquisition and use of software and hardware
- Access via non-networked systems
- Use, configuration, and disposal of mobile systems (BYOD), ISO-27002 for mobile devices and teleworking.
- Authentication and access controls
- Session starts and end protocols
- Automatic screen locks
- Access to management information
- Use of encryption

In terms of access and control rights, each user should have only the necessary rights. The company must clearly define who is an administrator and who is a user.

Processes in IT Operations

In the operation of systems, all applications and systems must be documented and protected by passwords, if possible. There must also be control of log files, regular backups, etc.

Many of these requirements are covered by BSI guidelines, especially by the now comprehensive BSI Basic Protection Compendium even more extensive is the ISO 27001 standard.

It is important to implement guidelines (also for the IT systems) that enable the information processed to be secured.

The guidelines for the infrastructure cover the most diverse areas:

- Building security including air conditioning of servers.
- Power supply as local and central uninterruptible supply with reserves until restoration for up to 6 days.
- Fire protection with fire alarm system, smoking ban and video surveillance with corresponding alarm and monitoring system (cooperative with data protection officer and works council).

Organisation and governance concern binding guidelines for the behaviour of employees and other members. These include:

- Security, data protection, data backup, data transmission, data media disposal, maintenance, and repairs,
- Maintenance and repair work,
- Emergency procedures, handling of technical vulnerabilities
- Right of entry, access, and disposal of documents.

Further guidelines are directed at protection against threats, both from the use of computers and from external threats to the physical infrastructure itself. Continuous training and education of staff is essential for protection.

Measures in IT security management

IT security management identifies potential risks in operational processes and takes measures to monitor systems, detect faults and minimise damage.

The BSI audits federal authorities for IT security, but its so-called minimum standards are also a benchmark for companies, especially on topics relevant to them such as web browsers or mobile device management, external cloud services, logging and detection, interface controls, Transport Layer Security (TLS) and more. Further standards are in progress.

Information Security Management System (ISMS)

With an information security management system (ISMS), companies determine, among other things, measures, rules, and procedures to secure and control the flow of information and to identify those accountable for its execution and to monitor it.

Companies can develop their ISMS themselves or, within the framework of a certification procedure, use its rules or be based on guidelines, e.g., from the BSI.

Security management according to ISO 27001

Companies can set up their system according to the ISO 27001 standard - and have it certified.

Certificates are valid for up to three years, after which they can be renewed. It may even be possible for a certification to be renewed for only one or two years, provided that annual audits are carried out in certain cases.

This norm comprises 11 chapters and an Annex A. In total, it includes 32 mandatory sheets, 250 option sheets and 114 controls that have international recognition. Its focus is on organisational environment, planning, implementation, support, operation, performance evaluation and improvement actions.

Real-time detection

In addition to an ISMS, a company can also establish a Security Information and Event Management (SIEM).

The SIEM's tasks include analysing data and logs, providing alerts to headquarters, detecting security breaches or threats in real time, e.g., attempts to access a user account by entering incorrect passwords, etc.

However, the use of such a system is associated with high costs for companies. However, these investments have led to a new way of dealing with cyber security: the use of artificial intelligence. It enables even faster, more accurate and more effective detection of threats in real time. This system "learns" user behaviour by creating user profiles, system access points, etc. to detect unusual behaviour that would not be detected by traditional means. This type of technology also protects the so-called "cloud" and takes instant decisions to ensure the integrity of IT systems. These systems are used in many different industries (restaurants, hospitals, airports, credit institutions, insurance agencies, etc.). Innovative examples include airport profiling, where the system analyses the behaviour of tourists. In infrastructure systems, sometimes a single computer controls numerous processes online, e.g., in gas supply or in the handling of hazardous substances, which AI systems can isolate from possible cyber-attacks. Another application is monitoring mail systems against weekend attacks.

Internally within the company, AI-supported systems can monitor whether employees are violating internal policies, such as downloading files or programmes. AI-based defence systems "learn" the reality and state of the company and its ongoing development, and then search for anomalies before they can cause any damage.

Critical Infrastructures – KRITIS

For Critical Infrastructures (KRITIS), the KRITIS Ordinance provides for special requirements, summarised in sectors and branches. These are facilities, installations, or parts thereof that belong to the sectors of energy, information technology and telecommunications, transport and traffic, health, water, food and finance and insurance and are of high importance for the functioning of the community.

Although the KRITIS Regulation is directly addressed to infrastructure companies, almost all companies with business relations to KRITIS companies are indirectly affected if they are in data exchange or online connection with them - the KRITIS companies regularly include such business partners in their security concept and obligations via their general terms and conditions (mostly purchasing terms and conditions).

Contracts with providers and platforms

Because the interconnectedness of IT services is constantly increasing, a large part of the functionality in the company is often already outsourced, external services are standard from the very beginning. Security management for the Cloud, Saas, IaaS, etc., backup hosting, outsourcing, services, and maintenance must necessarily include contractual obligations of the providers, which standards are to be guaranteed, how these are monitored and how the provider is liable to the company as client or user in case of infringements.

Cyber-Insurance

Finally, companies can also insure themselves against financial losses. Electronics insurance (especially with a software clause) covers the system, business interruption insurance covers the losses due to the system failure, and cyber policies cover certain attack risks. What all policies have in common, however, is that the insurance cover requires extensive operational security measures - due to the massive increase in attacks last year, the premiums have also risen extremely.

+++

ALLIURIS

The ALLIURIS GROUP consists of 20 law firms and 400 business lawyers within Europe, Asia and America. (www.alliuris.law).

…………………………………………………………………………………………………….

Your contact:
Alisha Daley-Stehr,
Alliuris Communication

info@alliuris.org
Fon 0049-511-307 56-0
Fax 0049-511-307 56-10

……………………………………………………………………………………………………….

IMPRINT

EDITORS

ALLIURIS A.S.B.L.
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS
BRUSSELS

MANAGEMENT
Luisenstr. 5, D-30159 Hannover
Fon +49-511-307 56-50 505056-20 Fax +49-511-307 56-60

BRUSSELS · PARIS · LONDON · AMSTERDAM · AMERSFOORT . LUXEMBURG · LYON · MADRID · BARCELONA · LISBON · MILAN · COPENHAGEN · HANOVER · ZUG · VIENNA · MOSCOW · MINSK · ATHENS · ISTANBUL · BEIJING · SHANGHAI ·GUANGZHOU NEW DELHI · NEW YORK · MEXICO CITY · SAO PAULO · RIO DE JANEIRO · BRASILIA BUENOS AIRES

EDITORIAL DEPARTMENT
Ulrich Herfurth, Rechtsanwalt

All information is correct to the best of our knowledge; liability is limited to intent or gross negligence. Reproduction, even in excerpts, requires the permission of the editors.