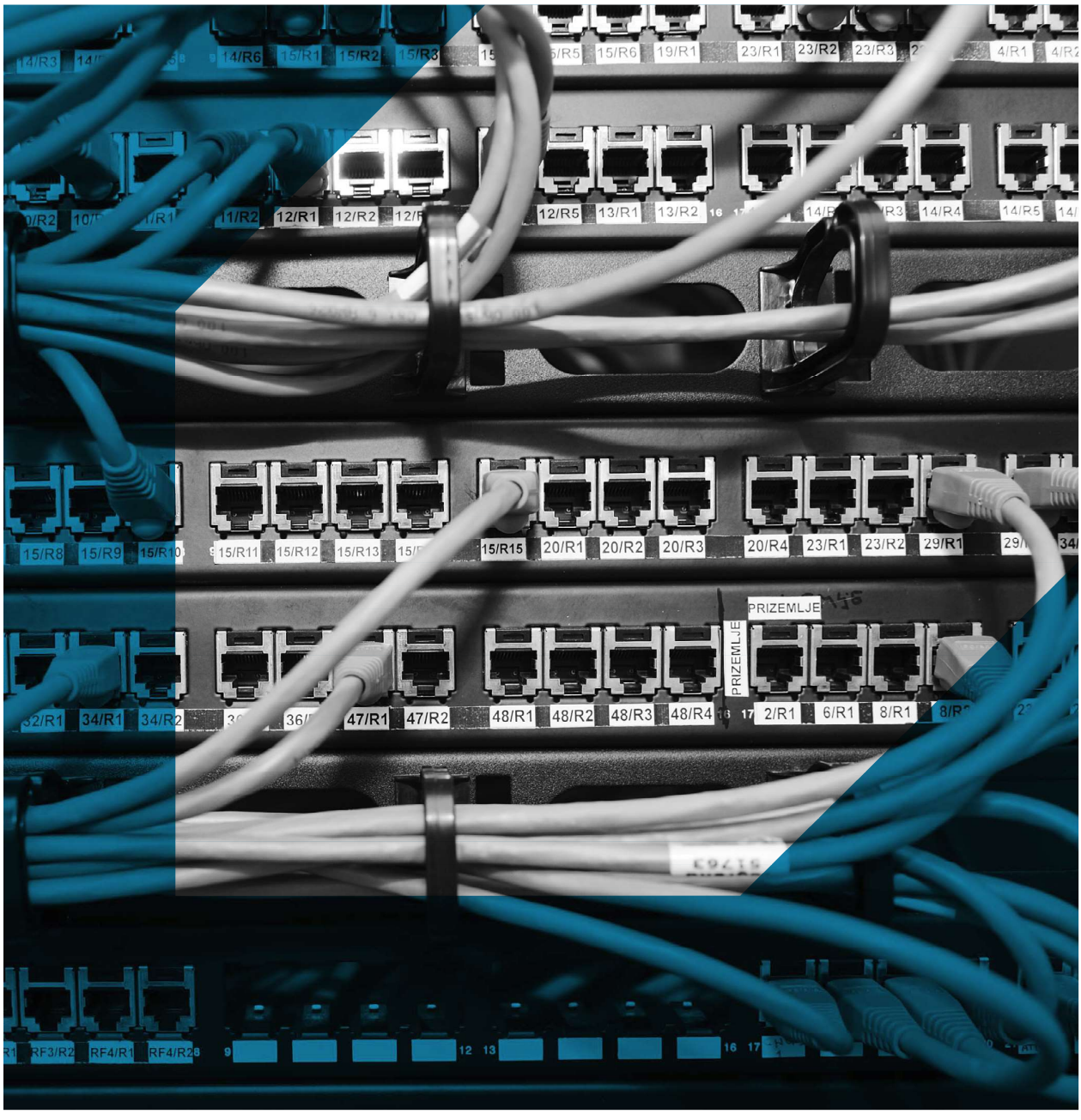
SWISS FTS
Forensic Technology Solutions

A PRACTICAL CASE – INFORMATION GOVERNANCE

SABOTAGE ATTACK ON THE SERVER INFRASTRUCTURE OF AN INDUSTRIAL COMPANY



Cyber-attacks targeted at corporate IT infrastructure have been constantly increasing in recent years. The major reasons for this are that more and more business processes and data are digitized and corporate systems are networked. Therefore, IT security and governance are increasingly important aspects to ensure data security and integrity. In addition to data protection, a key objective is to avoid financial damage.

Industrial corporations in particular are targets of cyber-attacks. In-depth awareness training about these risks is necessary since there is a risk of significant financial and reputational damage.

THE SITUATION

Cyber-attacks are launched for different reasons. Besides financial gain, hackers often want to test their skills or have other personal or idealistic motives. In certain cases attackers might have obtained information granting them access to the networks from an internal or external access point.

In the presented case, a former employee of an industrial corporation launched a sabotage attack on the corporation's server infrastructure, affecting more than 200 servers. In addition to systematic and extensive deletion of critical corporate data (which could fortunately be recovered) this attack had a drastic impact on business operations, and consequentially caused considerable financial damage. In an effort to track down the attacker ten workstations and servers were forensically acquired and analyzed.

THE SWISS FTS APPROACH

A cyber-attack may have serious consequences. In addition to securing evidence, the attacker had to be identified and located, and the security flaw needed to be discovered and eliminated.

Since a number of workstations and servers were compromised, a rapid response was required to avoid further damage. However, it was critical that no evidence was destroyed in the process. This could only be accomplished by adhering to standardized processes. A detailed assessment of the situation is key for a successful intervention.

Thereby critical systems are identified and prioritized for forensic acquisition. The acquired systems where then prepared in a multi-level process, where deleted files and logs were recovered. They were then thoroughly analyzed to determine the attacker's access point, and tracing its steps led to the IP address of the computer used for the attack. Using the evidence obtained by our forensics experts, both civil and criminal proceedings were initiated. ■

IMPORTANT ASPECTS

DIVIDING ACCESS RIGHTS

Access rights of administrators and people with authorized access have to be restricted, controlled and segregated.

RECORDING ACCESSES

Accesses, especially to critical systems should be monitored and regularly audited as a preventive measure.

DEFINING STANDARDS

Standardized procedures for auditing access rights, and disabling them when employees leave the company, are required.

ABOUT SWISS FTS
Founded: 2010
Specialties: IT Forensics, eDiscovery, Information Governance
www.swiss-fts.com

SWISS FTS
Forensic Technology Solutions

SWISS FTS AG
Europa-Strasse 19 | 8152 Glattbrugg | Switzerland
Phone +41 43 266 78 50 | info@swiss-fts.com

SWISS FTS (SINGAPORE) PTE LTD
50 Raffles Place | Level 30, Singapore Land Tower
Singapore 048623
Phone +65 6950 1370 | singapore@swiss-fts.com