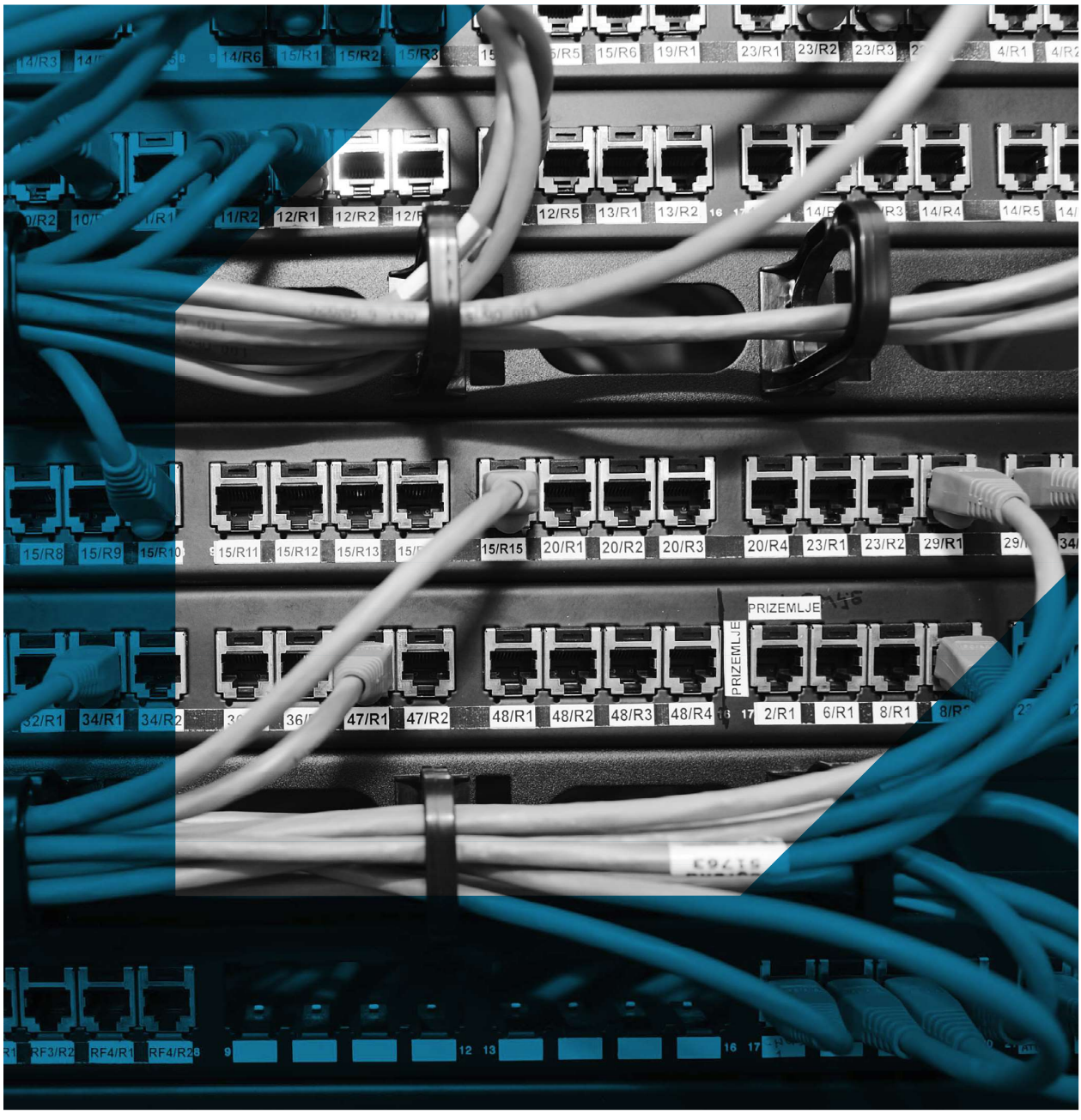
SWISS FTS
Forensic Technology
Solutions

EIN FALL AUS DER PRAXIS – INFORMATION GOVERNANCE

SABOTAGEANGRIFF AUF DIE SERVERINFRASTRUKTUR EINES INDUSTRIEUNTERNEHMENS



Cyberangriffe auf Unternehmen häufen sich. Da immer mehr Prozesse digitalisiert und Systeme miteinander vernetzt werden, sind IT Security und Governance wichtige Bestandteile, um Datensicherheit und -schutz zu gewährleisten. Dies dient dazu, mögliche wirtschaftliche Schäden zu verhindern, zum Beispiel durch Datenverlust und -diebstahl.

Industriekonzerne sind immer öfter das Ziel von Cyberangriffen. Um dieser Bedrohung entgegenzuwirken, sollten präventive Massnahmen geplant und implementiert werden, da grosse Finanz- und Reputationsschäden entstehen können.

DIE AUSGANGSLAGE

Cyberangriffe werden aus unterschiedlichen Beweggründen ausgeführt. Neben wirtschaftlichen Interessen können Hacker auch persönliche oder ideelle Motive haben. Angreifer verfügen oft über technische Kenntnisse, die ihnen den Zugriff über externe oder interne Wege auf die Server eines Unternehmens ermöglichen. Es kommt auch vor, dass durch Unwissen oder Unachtsamkeit von Mitarbeitern Tür und Tor für Angriffe offen gelassen werden.

Im vorliegenden Fall hat ein ehemaliger Mitarbeiter eines Industriekonzerns einen persönlich motivierten Sabotageangriff auf die Serverinfrastruktur durchgeführt. Betroffen waren über 200 Serversysteme. Neben der systematischen und weitreichenden Löschung kritischer Unternehmensdaten, hat dieser Angriff zu einem teilweisen Betriebsstillstand geführt, infolgedessen spürbare wirtschaftliche Schäden entstanden sind. Um dem Angreifer auf die Spur zu kommen, wurden zehn Systeme sichergestellt und einer forensischen Analyse unterzogen.

DER SWISS FTS-ANSATZ

Kommt es zu einem Cyberangriff, kann das schwerwiegende Folgen für ein Unternehmen haben. Neben der Sicherstellung von Beweismitteln und Spuren sollten im vorliegenden Fall die Verantwortlichen gefunden, sowie die Sicherheitslücken aufgedeckt und beseitigt werden. Da die Server des Unternehmens kompromittiert waren, galt es weitere Schäden durch schnelles Handeln zu verhindern. Spuren durften trotz immensem Zeitdruck keinesfalls vernichtet werden. Dies gelang nur dank eingeübten standardisierten Prozessen.

Eine detaillierte Lageanalyse stellte den ersten Schritt der Intervention dar. Dabei identifizierte Swiss FTS die kritischen Systeme und priorisierte sie für die forensische Sicherstellung und Analyse. Die sichergestellten Systeme wurden anschliessend in einem mehrstufigen Prozess aufbereitet, wobei unsere Experten auch gelöschte Dateien und Logs wiederherstellen konnten. Eine gründliche Datenauswertung und Analyse ermöglichten uns, den Eintrittspfad des Hackers zu ermitteln. Während der Analyse stiessen unsere Forensik-Experten auf verschiedenste Verbindungsdaten, wie zum Bespiel die IP-Adressen der Computer, von denen der Angriff ausging. Anhand der sichergestellten Beweise und Indizien konnten internationale zivil- und strafrechtliche Schritte eingeleitet werden. ■

WICHTIGE ASPEKTE

ZUGRIFFSRECHTE TRENNEN

Die Zugriffsrechte einzelner Administratoren und Zugriffsberechtigter müssen beschränkt, kontrolliert und getrennt werden.

ZUGRIFFE AUFZEICHNEN

Alle Zugriffe auf kritische Systeme sollten aufgezeichnet und als präventive Routinemassnahme regelmässig auditiert werden.

STANDARDS FESTLEGEN

Standardisierte Prozesse zum Audit und zur Deaktivierung von Zugriffsrechten bei Austritt von Mitarbeitern sind unverzichtbar.

ÜBER SWISS FTS
Gegründet: 2010
Fachgebiete: IT Forensik, eDiscovery, Information Governance
www.swiss-fts.com

SWISS FTS
Forensic Technology Solutions

SWISS FTS AG
Europa-Strasse 19 | 8152 Glattbrugg | Schweiz
Telefon +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