Case Study

Comprehensive security audit and compliance support after a data breach

Client: A multinational pharmaceutical company headquartered in Europe, operating more than 50 branches worldwide.

Challenge

The company produces lifesaving medicines and operates under strict data-protection regulations. After a security breach, it needed urgent assistance to contain the incident, verify system resilience, and ensure compliance with GxP and ISO 27001 standards. **Key challenges included:**

Incident detection, response, and recovery: The client needed to investigate the breach and implement measures to prevent its recurrence.

System vulnerability assessment: The client needed a full ERP security and infrastructure audit, including servers, routers, etc., to verify data protection and business continuity.

Compliance requirements: The company aimed to confirm alignment with GxP and ISO 27001 standards.

Human factor evaluation: Management wanted to test how employee behavior and awareness could contribute to security risks.

Solution

ZONE3000 conducted a comprehensive cybersecurity audit combining penetration testing, social engineering, and compliance consulting. **Key steps included:**

Social engineering campaign

ZONE3000 ran a phishing test across 50 branches to identify weak password practices and low cybersecurity awareness, and provided a report with targeted training steps.

External penetration testing

Black-box testing identified potential external entry points and allowed immediate protective actions to prevent repeated breaches.

Compliance audit

A two-stage assessment addressed both GxP and ISO 27001 requirements, including a custom infrastructure test adapted to the client's systems and industry standards.

Internal penetration testing

On-site testing revealed critical vulnerabilities within the ERP system, corporate Wi-Fi, email infrastructure, and servers that could expose sensitive information and disrupt core operations.

Remediation guidance

ZONE3000 provided a prioritized set of actions to mitigate risks and enhance system defenses in cooperation with the client's IT team and developers.

Results

The project helped the client restore security control and improve compliance posture:

Vulnerabilities addressed

ZONE3000 guided the client's IT team in fixing all identified weak spots.

Improved cybersecurity awareness

Campaign findings were used to update internal training programs and reduce human-factor risks.

Regulatory alignment

The company successfully strengthened its information-security controls and passed GxP and ISO 27001 certification audits.

The collaboration with ZONE3000 enabled the client to reinforce data integrity, prevent future breaches, and ensure uninterrupted operations in one of the most regulated industries worldwide.

Roman Dzvinka
Chief Revenue Officer

+380 67 505 72 96

roman.dzvinka@zone3000.net