Case Study

Comprehensive audit and pentesting for enhanced banking security and compliance

Client: A global banking institution with branches worldwide

Challenge

The bank aimed to verify the resilience of its core banking system (CBS) and identify weaknesses that could compromise data confidentiality or regulatory compliance. **Key challenges included:**

Compliance alignment: The client needed to validate adherence to all regulations and security standards required in the banking industry.

Vulnerability detection: Both internal and customer-facing systems required thorough penetration testing to identify potential risks.

Human factor assessment: The client requested an evaluation of staff awareness and susceptibility to social engineering threats.

Data confidentiality: Sensitive customer data such as credentials, financial information, and banking secret needed additional protection layers.

Solution

ZONE3000 performed a comprehensive cybersecurity audit for the bank's local branch to assess system resilience, identify vulnerabilities, and ensure compliance with financial and security standards. **Key steps included:**

Penetration testing

Simulated real-world attacks on internal and client-facing systems to identify exploitable vulnerabilities.

Social engineering testing

Evaluated staff awareness and readiness through controlled phishing and insider attack simulations.

Configuration and access review

Assessed firewall settings, encryption methods, and access management to ensure proper protection of sensitive data.

Remediation plan

Delivered a detailed report with prioritized recommendations for both the bank's security department and the developers of the core banking software.

Results

The cybersecurity audit brought measurable improvements in system security and compliance readiness:

Detected and fixed vulnerabilities

Identified flaws in data exchange between the core banking system (CBS) and the database that could expose sensitive customer information.

Improved data protection

The client's IT security team strengthened encryption, access control, and internal data-handling policies.

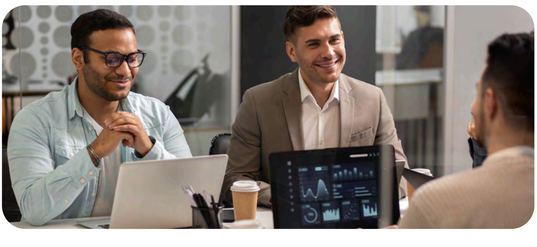
Increased security awareness

Based on weaknesses revealed in the social engineering tests, the client conducted targeted awareness and training among employees.

System-wide benefit

The findings shared with the CBS developer resulted in a software update that enhanced data security for multiple banks using the same system.

The project helped the bank reinforce its cybersecurity posture, prevent data leaks, and raise overall security standards across the banking network, demonstrating ZONE3000's expertise in delivering high-impact cybersecurity solutions.



Roman Dzvinka
Chief Revenue Officer

+380 67 505 72 96

roman.dzvinka@zone3000.net