Comprehensive Security Strategy & Technical Implementation – FinTrade AG

By Patrice Bertin

1. Company Overview

FinTrade AG is a financial services company based in Bonn, Germany, with approximately 250 employees.
The infrastructure includes:
- External Client Portal: portal.fintrade.de
- Internal Web Application: intranet.fintrade.local
- PostgreSQL Core Database: db1.fintrade.local
- Windows Active Directory (fintrade.local)
- ~20 Windows Servers, ~80 Client Machines

The organization is pursuing compliance with ISO 27001, NIS2, and GDPR.

2. Detailed Risk Assessment

Step-by-step process used for assessing the risks of the client portal:

1. Define Scope:
  - Scope: External client portal, backend APIs, and database server.
  - Tools: Excel and architecture documentation.
  - Stakeholders: CISO, IT Operations, Development Team.

2. Asset Identification:
  - Commands:
    <<sudo lshw -short > asset-inventory.txt>>
    <<Get-ADComputer -Filter | Export-Csv ad-assets.csv>>
  - Outcome:
    - portal.fintrade.de (Web Server)
    - db1.fintrade.local (Database)
    - Windows AD and internal workstations

3. Identify Threats & Vulnerabilities:
  - Tools:
    - Nessus for vulnerability scanning:
      nessuscli scan run --targets portal.fintrade.de --policy "Advanced"

- Threat sources: OWASP Top 10, MITRE ATT&CK
- Findings:
  - CVE-2021-41773: Apache Path Traversal (High Risk)

4. Risk Analysis:
- CIA Evaluation:
  - Confidentiality: High (financial data)
  - Integrity: High (transaction integrity)
  - Availability: High (client access)
- Impact Score: 5, Likelihood: 4 → Risk = 20 (High)

5. Risk Treatment:
- Control mapping: ISO 27001 A.12.6.1
- Mitigations:
  - Upgrade Apache to 2.4.52
  - Apply WAF using ModSecurity

6. Recording:
- Risk Register:

ID	Asset	Risk	Score	Owner	Status
R1	Web01	RCE via Apache	20	DevOps	Open

7. Reporting:
- Tools: Excel Risk Matrix and PDF reports to ISMS team

3. Internal Vulnerability Assessment

1. Tools:
- Nessus for internal network scanning
- Credentialed scan with domain account

2. Execution:
- Command:

<< nessuscli scan run --policy "Internal Audit" --targets 192.168.10.0/24>>

3. Findings:
- Example: MS17-010 (EternalBlue) on WIN-SRV-DC01

4. Remediation:

- Patch: WSUS + PowerShell:
  <<Install-WindowsUpdate -KB4013389>>

5. Retesting confirms mitigation of critical issues.

4. Penetration Testing

Penetration Testing Methodologies:

- White Box: Full access (used to validate defenses)
- Grey Box: Limited user credentials (simulate insider)
- Black Box: No access, external attacker simulation
- Blue Team: Defensive monitoring (Wazuh, SIEM)
- Red Team: Offensive exploitation (manual + automated)
- Purple Team: Cooperative engagements for tuning detection

Execution:

1. Reconnaissance:
  - Tool: Nmap
    <<nmap -sS -A -T4 portal.fintrade.de>>

2. Vulnerability Discovery:
  - Tool: Nikto
    <<nikto -h https://portal.fintrade.de>>
  - Result: CVE-2021-41773

3. Exploitation:
  - Command:
    <<curl -v --path-as-is https://portal.fintrade.de/cgi-bin/.%2e/.%2e/.%2e/etc/passwd>>
  - Output confirms access to `/etc/passwd`

4. Post-Exploitation:
  - Burp Suite:
    SQL Injection payload: `admin' OR '1'='1 --`
  - Result: Login bypassed; admin access granted

5. Reporting:

Vulnerability	CVE	Proof	Risk	Fix
Path Traversal	CVE-2021-41773	/etc/passwd	High	Apache Patch
SQLi	N/A	Login bypass	Input Sanitization	WAF

5. Security Concepts & Architecture

1. Business Process: "Client Onboarding"
2. Data Flow: Client → Web Portal → API → DB
3. Controls:
  - MFA via SSO
  - Data encryption in transit (TLS 1.3) and at rest (AES-256)
  - Logging and SIEM integration

4. Architecture Diagram:
  - Web portal behind Cloudflare WAF
  - Backend hosted in private subnet
  - PostgreSQL with TLS & encryption

The security concept for FinTrade AG is structured to ensure end-to-end protection of sensitive data and compliance with regulations.
This includes technical, organizational, and process-level controls:
- Identity & Access Management (IAM): Role-based access control (RBAC) enforced via Active Directory and Azure AD.
- Data Classification: Implemented via Microsoft Purview and tagging policies.
- Endpoint Protection: Using Microsoft Defender for Endpoint with EDR and automated response.
- Backup Strategy: Daily encrypted backups with offsite storage using Veeam and AWS S3.
- Secure Software Development Lifecycle (SSDLC): Integrated SAST, DAST, and dependency checks (OWASP Dependency-Check).
- Security Governance: Regular internal audits, patch cycles, and compliance reviews tied to ISO 27001 controls.

The comprehensive security concept for FinTrade AG aligns with ISO 27001, NIS2, and GDPR. It integrates proactive defense, detection, response, and recovery elements to protect business processes, sensitive data, and infrastructure integrity.

1. Identity and Access Management (IAM):
  - Centralized authentication via Active Directory Federation Services (ADFS).

- Role-Based Access Control (RBAC) linked to business units.
- MFA enforced via Azure Conditional Access policies.

2. Data Protection Strategy:
- Data classification using Microsoft Purview (Confidential, Internal, Public).
- Endpoint Data Loss Prevention (DLP) enforced through Microsoft Purview policies.
- All backups encrypted using AES-256 and stored redundantly in AWS S3.

3. Secure Network Architecture:
- Segmented VLANs (Production, DMZ, Development, Management).
- Firewall-enforced east-west traffic control.
- VPN gateway with IPsec and Duo MFA for remote workers.

4. SSDLC:
- GitHub Actions pipelines integrate:
  - OWASP Dependency-Check
  - SonarQube static code analysis
  - OWASP ZAP dynamic analysis during CI/CD.

6. Attack Prevention Measures

1. WAF:
- Tool: ModSecurity + OWASP CRS
- Commands:
  <<sudo apt install libapache2-mod-security2>>
  <<sudo a2enmod security2>>

2. Rate Limiting:
- Tool: NGINX
- Config:
  ```
  limit_req_zone $binary_remote_addr zone=mylimit:10m rate=5r/s;
  location /api/ {
    limit_req zone=mylimit burst=10;
  }
  ```

3. Code Analysis:
- Tool: SonarQube
  ```
  sonar-scanner -Dsonar.projectKey=FinTradePortal -Dsonar.sources=src -
  ```

Dsonar.host.url=http://localhost:9000
```

4. Log Monitoring:
  - Tool: Wazuh
  - Alerts triggered for brute-force attempts, SQLi, path traversal, abnormal login times.

## 7. Security Architecture Diagram

The following diagram represents the security architecture:

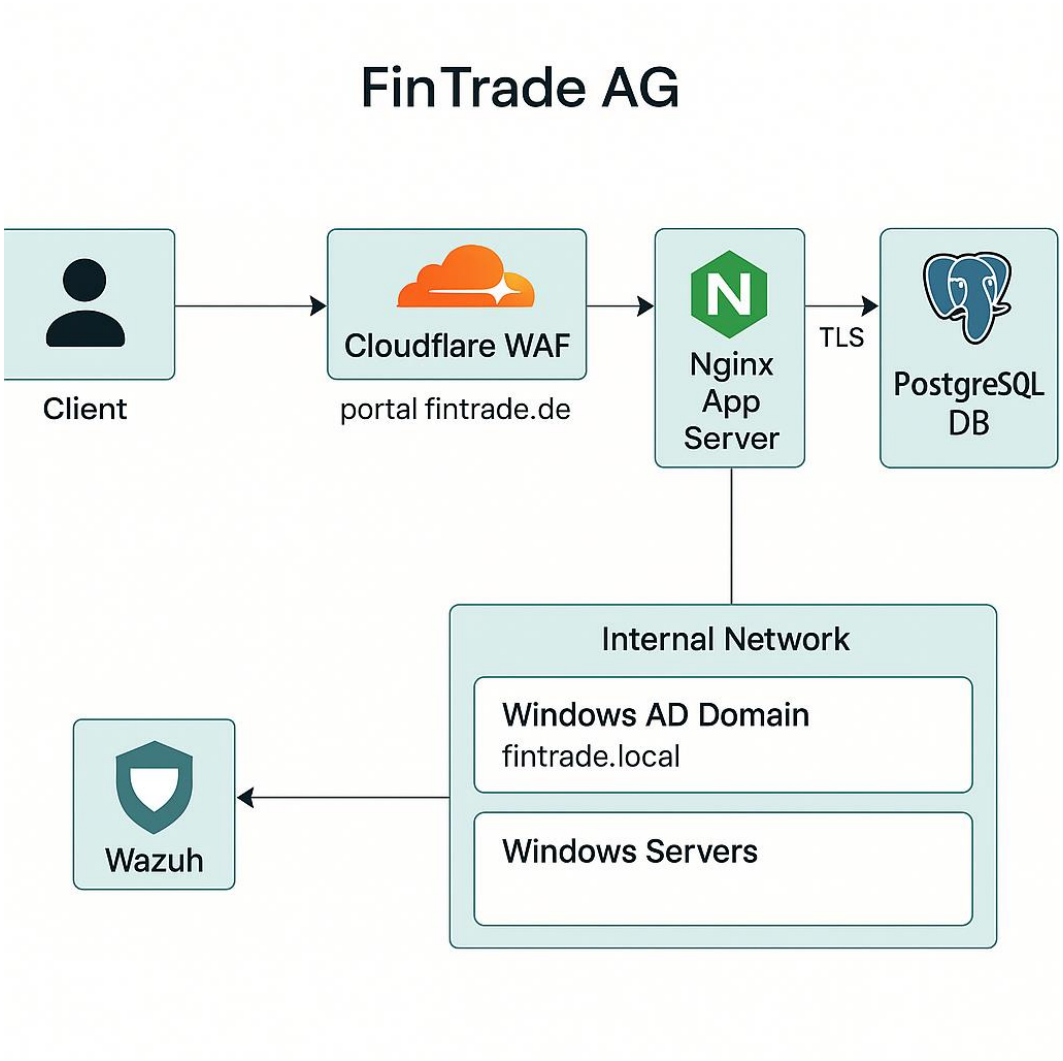


*Fig.1: Security Architecture Fintrade*
```

8. Implementation of Attack Prevention Measures (Expanded)

Prevention mechanisms are layered across multiple domains:

1. Network Layer:
  - Firewall: pfSense with geo-blocking and IDS/IPS enabled (Snort).
  - VPN: Enforced IPsec VPN for remote access with MFA.

2. Application Layer:
  - OWASP Secure Headers:
    - Strict-Transport-Security
    - X-Content-Type-Options
    - X-Frame-Options
  - Rate Limiting: `limit_conn_zone` and `limit_req` in NGINX to deter brute-force.
  - CAPTCHA enforcement after 3 failed logins.

3. Data Layer:
  - At-rest encryption using LUKS for Linux and BitLocker for Windows
  - Data masking in staging/testing environments

4. Monitoring & Detection:
  - Real-time alerts in Wazuh for:
    - Unusual login patterns
    - Port scans
    - SQL injection attempts
  - Use of Graylog to correlate log events and detect advanced persistent threats.

5. Staff Training:
  - Quarterly phishing simulations (e.g., GoPhish campaigns)
  - Mandatory security awareness training via KnowBe4

The security architecture implements layered attack prevention across all operational domains using enterprise-grade tooling and hardened configurations.

1. Perimeter & Firewall Rules:
  - pfSense Firewall configured with:
    - Geo-blocking to deny access from non-EU IPs
    - Allow TCP 443/80 to web servers only
    - Deny all inbound to internal subnets (RFC1918)
    - IDS/IPS rules from Emerging Threats and Snort community lists

- Example pfSense Firewall Rule Set:

Rule #	Source	Destination	Protocol	Action	Description
1	Any (Geo-EU)	WAN address	TCP 443	Allow	HTTPS Access to Portal
2	Any	Internal RFC1918	ANY	Block	Block Inbound Internal
3	Internal Net	Any	TCP/UDP	Allow	Outbound User Traffic

2. SIEM - Splunk Enterprise:
  - All system, firewall, and application logs forwarded to Splunk Heavy Forwarders.
  - Use cases implemented:
    - Detection of brute force attempts
    - SQL injection attempt alerts
    - Suspicious administrative privilege escalations

  - Example Splunk query:
    ```
    index=firewall sourcetype=pfSense "Blocked" | stats count by src_ip, dest_port
    ```

3. Endpoint Security:
  - Cisco Secure Endpoint (formerly AMP for Endpoints):
    - Advanced malware detection
    - File trajectory tracking
    - Exploit prevention (behavior-based)

4. Email Security:
  - Cisco Secure Email Gateway (ESA):
    - SPF, DKIM, DMARC enforcement
    - URL rewrite + sandboxing
    - Attachment detonation (Cisco Threat Grid)

5. WAF and DDoS Protection:
  - Cloudflare WAF active with OWASP CRS 3.3 rules
  - Rate limiting enabled per session
  - CAPTCHA challenge enforced after 5 login failures

6. Secure Software Development:
  - SAST via SonarQube in CI/CD pipelines:
    ```
    sonar-scanner -Dsonar.projectKey=FinTradePortal -Dsonar.sources=src -Dsonar.host.url=http://localhost:9000
    ```

- DAST via OWASP ZAP nightly scans:
  ```
  zap-cli quick-scan --self-contained --start-options '-config api.disablekey=true' https://portal.fintrade.de
  ```

7. Monitoring & Incident Response:
   - Real-time alerts and correlation in Splunk Enterprise
   - Cisco SecureX for unified response between XDR, firewall, and email

8. Training & Awareness:
   - KnowBe4 phishing simulation every quarter
   - Role-specific security workshops for developers and support teams