mFIN-CERT.tg

The five most common cybersecurity mistakes observed in microfinance institutions

By Maklawe HADATOKI
Cybersecurity Analyst & Lead CTI departement

CTI investigations help identify recurring trends in incidents and exposures affecting financial organizations. In the microfinance sector, several weaknesses repeatedly facilitate account compromise or exploitation of exposed infrastructure.

Mistake 1: Failing to Monitor Compromised Credentials
An organization may have effective security controls while remaining unaware that a user account appears in a leaked dataset originating from a compromised workstation. Monitoring compromised data makes it possible to identify high-risk accounts quickly and trigger password resets or investigations.

Mistake 2: Reusing Passwords
Reusing the same password across multiple services significantly increases the impact of a leak. A credential recovered from one platform can be tested against another. Using unique passwords, a password manager and multi-factor authentication substantially reduces this risk.

Mistake 3: Neglecting Internet-Exposed Assets
Domains, subdomains, administrative interfaces, management services and exposed software components must be inventoried and monitored. Uncontrolled exposure facilitates reconnaissance and can allow attackers to identify vulnerable or misconfigured components.

Mistake 4: Treating Phishing as Merely a User Problem
Phishing should be treated as both a technical and operational risk. Modern campaigns are often customized and can rely on public information or data from previous compromises. Protection should combine awareness, filtering, MFA, message analysis and detection of anomalous authentication activity.

Mistake 5: Failing to Integrate CTI into Security Operations
Occasional intelligence monitoring is not enough. Intelligence from credential leaks, malicious infrastructure and ongoing campaigns must be integrated into SOC and incident-management processes.
CTI becomes truly useful when it leads to action: blocking, investigation, credential reset, notification, takedown or strengthening of a security control.

The five mistakes are different but closely connected. An institution can reduce its exposure by combining asset visibility, compromise monitoring, MFA, identity management, awareness and integration of CTI into security operations.