Mohannad Darwish 4Geeks

Cybersecurity Incident & Vulnerability Remediation

Overview

The following will summarize the results of a comprehensive internal security audit and protection plan.

This review was conducted in 3 focused phases:

- **Phase 1:** Hack Identification and Correction
- **Phase 2:** System Hardening & Vulnerability Mitigation
- **Phase 3:** Long-Term Security Governance & Resilience Strategy

Discoveries

These vulnerabilities increased the company’s exposure to data loss, unauthorized access, and business disruption:

- Unauthorized Access
- Sensitive Access Gaps
- Outdated Configurations
- Exposed Files
- Open, Unused Services

Remediations

- **Blocked the Intrusion**: Access methods used by the attacker were shut down immediately.
- **Secured All Passwords & Accounts**: Every user was audited, strong passwords were applied, and some accounts were disabled.
- **Fixed FTP & Database Security**: Disabled anonymous access and removed unsafe settings.

Remediations cont.

- **Protected WordPress & Web Directories**: Web admin account replaced; public file listings blocked.
- **Closed Unnecessary Doors**: Unused ports were shut down and confirmed sealed.
- **Verified Patch Coverage**: The Apache server was verified to be safe based on Debian's security policy.

Preventing Future Incidents

- Weak access points are removed and strong password rules have been put in place.
- Introduced key-based login for secure remote access
- Established log tracking and account activity monitoring
- Separated user roles and limited access only to what's needed

Long-Term Plan

- Implemented a formal Incident Response Plan, following NIST SP 800-61
- Established an Information Security Management System (ISMS) aligned with ISO 27001:
    - Clear IT security policies
    - Risk evaluations and access controls
    - Automated backups and recovery protocols
    - Data loss prevention (DLP) systems

Summary

- The server has been stabilized and hardened
- Tools are now in place to detect and react to future threats
- Internal processes now follow industry best practices (NIST, ISO 27001)

Recommendations

- Begin monthly audits and vulnerability scans
- Enable two-factor authentication for all high-risk accounts
- Adopt centralized logging and alerting tools
- Expand protection to include employee security awareness training
- Schedule annual security reviews and simulated incident drills