Stakeholder memorandum

TO: IT Manager, stakeholders
FROM: Nick Dailey
DATE: 23 June 2023
SUBJECT: Internal IT audit findings and recommendations

Dear Colleagues,

Please review the following information concerning the scope, goals, critical findings, and summary recommendations of the Botium Toys internal audit.

Scope:

- In-scope systems: accounting, end point detection, firewalls, intrusion detection system, SIEM tool.
- Evaluation areas: current user permissions, implemented controls, procedures and protocols.
- Alignment with PCI DSS and GDPR compliance requirements.
- Accounting for current technology in terms of hardware and system access.

Goals:

- Adherence to the NIST CSF.
- Establishment of a compliant process for systems.
- Strengthening of system controls.
- Implementation of the least privilege concept for user credential management.
- Development and implementation of policies, including playbooks.
- Meeting compliance requirements.

Critical findings (must be addressed immediately):

- Multiple controls need to be developed and implemented to meet the audit goals, including:
    - Control of Least Privilege and Separation of Duties
    - Disaster recovery plans
    - Password, access control, and account management policies, including the implementation of a password management system
    - Encryption (for secure website transactions)
    - IDS
    - Backups
    - AV software
    - CCTV
    - Locks
    - Manual monitoring, maintenance, and intervention for legacy systems
    - Fire detection and prevention systems
- Policies need to be developed and implemented to meet PCI DSS and GDPR compliance requirements.
- Policies need to be developed and implemented to align to SOC1 and SOC2 guidance related to user access policies and overall data safety.

Findings (should be addressed, but no immediate need):

- The following controls should be implemented when possible:
    - Time-controlled safe
    - Adequate lighting
    - Locking cabinets
    - Signage indicating alarm service provider

Summary/Recommendations: Promptly address critical findings related to PCI DSS and GDPR compliance, considering Botium Toys' acceptance of online payments worldwide. Adopt the concept of least permissions by incorporating SOC1 and SOC2 guidance for user access policies and overall data safety. Establish disaster recovery plans and backups for business continuity. Integrate IDS and AV software to identify and mitigate risks. Enhance physical security with locks, CCTV, and monitoring. Optional improvements include encryption, time-controlled safe, adequate lighting, locking cabinets, fire detection and prevention systems, and signage for alarm services.

Please ensure these recommendations are taken into account to strengthen the security posture of Botium Toys.

Sincerely,

Nick Dailey