Stakeholder Memorandum

to: IT Manager, stakeholders
from: Andres Rincon Sanchez
date: 23/07/2024
subject: Internal IT audit findings and recommendations

Dear Colleagues, please find below the details regarding the scope, objectives, key findings, summary, and recommendations from the Botium Toys internal audit.

Scope:

- The audit covers the following systems: accounting, endpoint detection, firewalls, intrusion detection systems, and the SIEM tool. The evaluation will focus on:
    - Current user permissions
    - Implemented controls
    - Existing procedures and protocols
- Ensure alignment of user permissions, controls, procedures, and protocols with PCI DSS and GDPR compliance requirements.
- Ensure all technology, including hardware and system access, is accounted for.

Goals:

- Comply with the NIST Cybersecurity Framework (CSF).
- Establish a more robust process to ensure system compliance.
- Strengthen system controls.
- Adopt the principle of least privilege in user credential management.
- Develop policies and procedures, including playbooks.
- Ensure compliance with regulatory requirements.

Critical Findings (Immediate Attention Required):

- Several controls need to be developed and implemented to achieve audit goals, such as:
    - Control of Least Privilege and Separation of Duties
    - Disaster recovery plans
    - Policies for password management, access control, and account management, including a password management system
    - Encryption for secure website transactions
    - Intrusion Detection Systems (IDS)
    - Backup solutions

    - Antivirus (AV) software
    - Closed-circuit television (CCTV)
    - Physical locks
    - Manual monitoring, maintenance, and intervention for legacy systems
    - Fire detection and prevention systems
- Policies must be created and implemented to meet PCI DSS and GDPR compliance requirements.
- Policies should be aligned with SOC1 and SOC2 guidance on user access policies and overall data safety.

Findings (To Be Addressed Later):

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

Summary/Recommendations: It is recommended that the critical findings related to PCI DSS and GDPR compliance be addressed promptly, as Botium Toys accepts online payments from customers worldwide, including the EU. Additionally, to align with the audit goal of adopting the least privilege principle, policies and procedures should be developed following SOC1 and SOC2 guidelines related to user access and data safety. Having disaster recovery plans and backups is crucial for maintaining business continuity in case of an incident. Implementing an IDS and AV software will help identify and mitigate potential risks, particularly since legacy systems require manual monitoring and intervention. To secure assets at Botium Toys' physical location, it is advisable to use locks and CCTV for asset protection and threat monitoring. While not immediately necessary, adding encryption, a time-controlled safe, adequate lighting, locking cabinets, fire detection and prevention systems, and signage for the alarm service provider will enhance Botium Toys' security measures.