Stakeholder

TO: IT Manager, Stakeholders of Botium Toys
FROM: Mohammed Noori
DATE: Aug 20, 2023
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please review the following information regarding the Botium Toys internal audit scope, goals, critical ndings, summary and recommendations.

Scope:

- The following systems are in scope: accounting, end point detection, rewalls, intrusion detection system, SIEM tool. The systems will be evaluated for:
    - Current user permissions
    - Current implemented controls

    - Current procedures and protocols

● Ensure current user permissions, controls, procedures, and protocols in place align with PCI DSS and GDPR compliance requirements.

● Ensure current technology is accounted for both hardware and system access.

Goals:

● Adhere to the NIST CSF.

● Establish a beer process for their systems to ensure they are compliant.

● Fortify system controls.

● Adapt to the concept of least permissions when it comes to user credential management.

● Establish their policies and procedures, which includes their playbooks.

- Ensure they are meeting compliance requirements.

- Multiple controls need to be developed and implemented to meet the audit goals, including:

    - Control of Least Privilege and Separation of Duties

    - Disaster recovery plan

    - Password, access control, and account management policies, including the implementation of a password management system

    - Encryption (for secure website transactions)

    - IDS

    - Backups

    - AV soware

- 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: Botium Toys needs to follow the recommendations above to be in compliance with the law and security measures. First, it is needed to implement the PCI DSS and GDPR for online payments and worldwide customers. Another compliance that should be implemented is the SOC1 and SOC2, these will provide access policies and data safety. Second, having disaster recovery plans and backups should be a priority to support business continuity in case of a natural disaster or any malicious aacks. Third, mitigating potential risks by identifying it in the systems, they should be using IDS and AV soware to help them with intrusion detection, monitoring and intervention. Four, technical and physical security should be equally important by adapting CCTV's, locks, and any equipment that could help investigate potential threats. As per the priority of control implementations, there is a high critical need to improve security immediately. However, there are few implementations that can be worked on in the future, such as time-controlled safe, locking cabinets, adequate lighting, among others in the list aached. Please review documents aached for detailed information. These recommendations will help Botium Toy's to be in compliance with international and domestic regulations and maintain a safe environment for internal and external personnel, and customers.