To : IT Manager & Stakeholders

From : Ammiroul Amin

Date : 23/8/2023 Subject : Internal IT audit findings and recommendations

Dear IT Manager and Stakeholders,

I'd like to share the key findings and recommendations from our recent internal IT audit at Botium Toys.

Scope:

We audited the following systems:

* Accounting
* Endpoint detection
* Firewalls
* Intrusion detection system
* Security information and event management (SIEM) tool

We evaluated these systems for:

* Current user permissions
* Implemented controls
* Procedures and protocols
* Alignment with GDPR, PCI DSS, and compliance requirements
* Technology and asset accountability

Goals:

Our goals were to:

* Follow the NIST CSF framework
* Establish a compliant process
* Strengthen system controls
* Implement the principle of least privilege
* Develop policies, including playbooks

Critical Findings (Immediate Action Required):

We identified several critical issues that must be addressed immediately:

* Implement the Principle of Least Privilege and Separation of Duties
* Develop disaster recovery plans
* Implement password, access control, and account management policies
* Enhance the Intrusion Detection System (IDS)
* Implement encryption for secure transactions and sensitive data storage
* Establish robust backup procedures
* Implement a password management system
* Deploy antivirus (AV) software
* Address manual monitoring for legacy systems
* Enhance closed-circuit television (CCTV) surveillance
* Improve physical security with locks, locking cabinets, and fire detection/prevention

Policy Development (To Meet Compliance Requirements):

We recommend developing and implementing policies to meet PCI DSS, GDPR, SOC1, and SOC2 compliance requirements.These policies should focus on user access and overall data safety.

Non-Critical Findings (Address After Critical Issues):

After addressing critical issues, consider the following physical controls:

* Time-controlled safe
* Adequate lighting
* Signage indicating alarm service provider for restricted areas

Summary and Recommendations: We strongly recommend addressing critical compliance issues with PCI DSS and GDPR swiftly, as Botium Toys handles online payments from global customers, including the EU. To achieve the goal of least permissions, follow SOC1 and SOC2 guidance for user access policies and data safety procedures.

Having disaster recovery plans and backups is essential for business continuity in case of incidents. Integrating an IDS and AV software will enhance risk detection and intrusion prevention, especially for legacy systems needing manual monitoring.

To secure physical assets at Botium Toys' location, use locks and CCTV. Consider encryption, a time-controlled safe, adequate lighting, locking cabinets, fire prevention, and alarm signage for further security, though these can be addressed gradually.

Your attention to these recommendations will significantly improve Botium Toys' security and compliance posture.

Best regards,

Ammiroul Amin