TO: IT Manager, stakeholders

FROM: Bartosz

DATE: 04.07.2023

SUBJECT: Internal IT audit findings and recommendations

Dear Colleagues,

Please review the following information regarding the Botium Toys internal audit scope,

goals, critical findings, summary and recommendations.

Scope:

- System that are in scope: accounting, end point detection, firewalls, IDS, SIEM tool. They are useful for:
    - Current user permissions
    - Current implemented controls
    - Current procedures and protocols
- Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements such as GDPR, PCI DSS, Soc type 1 and Soc type 2.
- Ensure current technology is accounted for both hardware and system access.

Goals:

- To adhere to the National Institute of Standards and Technology Cybersecurity
- Framework (NIST CSF)
- Establish a better process for their systems to ensure they are compliant
- Fortify system controls
- Implement 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

Critical findings (must be addressed immediately:

Several findings has been discovered and have to be covered diligently.

- Least Privilege
- Disaster recovery (business continuity)
- Firewall
- IDS
- Encryption (for website payment transactions)
- Antivirus Software
- Locking cabinets (these for network gear)
- Signage indicating alarm service provider
- Fire detection and prevention (for people's safety and for server's safety)

Policies need to be created to meet requirements for GDPR, PCI DSS, SOC type 1, SOC type 2

Findings (doesn't have to be addressed immediately):

- Plans
- Password policies
- Access control policies
- Backups
- Manual monitoring
- Time-controlled safe
- Closed-circuit television surveillance
- Locks

Summary/Recommendations: Several findings needs to be taken care of immediately. Most of them are Technical Controls. Our organization also has to adhere to compliance with GDPR as we also serve people in EU, PCI DSS as we accept credit card payment method and SOC type 1 and 2 as we deal with privacy information of our clients. We need to ensure Least Privilege to reduce risk connected to non-authorized staff logging in to our systems. Disaster recovery plans also have to be made because we need to have business continuity in case of attack. Firewall is a basic defensive tool to protect our network from malicious traffic. Intrusion Detection System (IDS) will allow our IT team to identify possible intrusions. Encryption is crucial to remain integrity and confidentiality of our customers information. We also need some physical controls such as Locking cabinets, signage indicating alarm service provider, fire detection and prevention. The things that are not necessary are: password policies, access control policies, backups, manual monitoring, time-controlled safe, CCTV, locks.