Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Ryan Sterling-Noel
DATE: 28/06/2023
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:

- Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
- Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.
- Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
- Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
- 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):

Least Privilege - Preventative; reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs

Disaster recovery plans - Corrective; business continuity to ensure systems are able to run in the event of an incident/there is limited to no loss of productivity downtime/impact to system components, including: computer room environment (air conditioning, power supply, etc.); hardware (servers, employee equipment); connectivity (internal network, wireless); applications (email, electronic data); data and restoration

Password policies - Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques

Access control policies - Preventative; increase confidentiality and integrity of data

Account management policies - Preventative; reduce attack surface and limit overall impact from disgruntled/former employees

Separation of duties - Preventative; ensure no one has so much access that they can abuse the system for personal gain

Firewall - Preventative; firewalls are already in place to filter unwanted/malicious traffic from entering internal network
Intrusion Detection System (IDS) - Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly

Encryption - Deterrent; makes confidential information/data more secure (e.g., website payment transactions)

Backups - Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan

Password management system - Corrective; password recovery, reset, lock out notifications

Antivirus (AV) software - Corrective; detect and quarantine known threats

Fire detection and prevention (fire alarm, sprinkler system, etc.) - Detective/Preventative; detect fire in the toy store’s physical location to prevent

Manual monitoring, maintenance, and intervention - Preventative/corrective; required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities

Closed-circuit television (CCTV) surveillance - Preventative/detective; can reduce risk of certain events; can be used after event for investigation

Locks - Preventative; physical and digital assets are more secure

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

Time-controlled safe - Deterrent; reduce attack surface/impact of physical threats

Adequate lighting - Deterrent; limit “hiding” places to deter threats

Signage indicating alarm service provider - Deterrent; makes the likelihood of a successful attack seem low

Locking cabinets (for network gear) - Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear

Summary/Recommendations:

Above are the areas in which your security posture needs to be improved upon that were addressed in the scope of the audit that went ahead. The critical findings must be rectified as soon as possible in order to guarantee safety within the company and the goings ahead with customer interactions. Compliance with PCI DSS and GDPR must be promptly addressed since Botium Toys accepts online payments from customers worldwide, including the E.U. Additionally, since one of the goals of the audit is to adapt to the concept of least permissions, SOC1 and SOC2 guidance related to user access policies and overall data safety should be used to develop appropriate policies and procedures. Certain critical findings such as Least Privilages, IDS, Encryption and CCTV could vastly improve your security in order to carry out day to day activities and reduce the chance of a breakdown in business. Failure to implement these recommendations can and will result in huge financial loss and the reputation of the company being put in jeopardy, which could in turn mean the end of the company. Other findings such as signage indicating alarm service provider should be looked into, as it can deter potential attackers from making a move on your assets. Making these improvements will help you to further improve the security posture of Botium Toys and will achieve the security goals that were initially put in place.