MEMORANDO DE PARTES INTERESADAS

PARA: Gerente de TI, partes interesadas
DE: Trinidad Angel Gabriel
FECHA: 05/12/2024
ASUNTO: Hallazgos y recomendaciones de la auditoría interna de TI

Estimados colegas,

Revise la siguiente información sobre el alcance, los objetivos, los hallazgos críticos, el resumen y las recomendaciones de la auditoría interna de Botium Toys.

Alcance:

- Los siguientes sistemas están dentro del alcance: contabilidad, detección de puntos finales, firewalls, sistema de detección de intrusiones, herramienta SIEM. Los sistemas serán evaluados para:
    - Usuario actual permisos
    - Controles implementados actualmente
    - Procedimientos y protocolos actuales
- Asegúrese de que los permisos, controles, procedimientos y protocolos de usuario actuales estén alineados con los requisitos de cumplimiento de PCI DSS y GDPR.
- Asegúrese de que la tecnología actual tenga en cuenta tanto el acceso al hardware como al sistema.

Objetivos:

- Adhiérase al NIST CSF.
- Establecer un mejor proceso para sus sistemas para garantizar que cumplan.
- Fortalecer los controles del sistema.
- Adáptese al concepto de permisos mínimos cuando se trata de gestión de credenciales de usuario.
- Establecer sus políticas y procedimientos, que incluyen sus manuales.
- Asegúrese de que cumplan con los requisitos de cumplimiento.

Hallazgos críticos (debe abordarse de inmediato):

- Es necesario desarrollar e implementar múltiples controles para cumplir con los objetivos de la auditoría, incluyendo:
    - Control de privilegios mínimos y separación de funciones
    - Planes de recuperación de desastres
    - Políticas de contraseñas, control de acceso y gestión de cuentas, incluida la implementación de un sistema de gestión de contraseñas.
    - Cifrado (para transacciones seguras en sitios web)
    - identificación
    - Copias de seguridad
    - software audiovisual
    - circuito cerrado de televisión
    - Cabellos
    - Monitoreo, mantenimiento e intervención manuales para sistemas heredados
    - Sistemas de detección y prevención de incendios.
- Es necesario desarrollar e implementar políticas para cumplir con los requisitos de PCI DSS y GDPR.
- Es necesario desarrollar e implementar políticas para alinearse con las pautas SOC1 y SOC2 relacionadas con las políticas de acceso de los usuarios y la seguridad general de los datos.

Recomendaciones (debe abordarse, pero no es una necesidad inmediata):

- Cuando sea posible, se deben implementar los siguientes controles:
    - Caja fuerte con control de tiempo
    - Iluminación adecuada
    - Gabinetes con cerradura
    - Señalización que indica proveedor de servicios de alarma

Resumen/Recomendaciones: Se recomienda abordar de inmediato los hallazgos críticos relacionados con el cumplimiento de PCI DSS y GDPR, ya que Botium Toys acepta pagos en línea de clientes de todo el mundo, incluida la UE. Además, dado que uno de los objetivos de la auditoría es adaptarse al concepto de permisos mínimos, se deben utilizar las directrices SOC1 y SOC2 relacionadas con las políticas de acceso de los usuarios y la seguridad general de los datos para desarrollar políticas y procedimientos adecuados. Tener planes de recuperación ante desastres y copias de seguridad también es fundamental porque respaldan la continuidad del negocio en caso de un incidente. La integración de un software IDS y AV en los sistemas actuales respaldará nuestra capacidad para identificar y mitigar riesgos potenciales y podría ayudar con la detección de intrusiones, ya que los sistemas heredados existentes requieren monitoreo e intervención manuales. Para proteger aún más los activos alojados en la única ubicación física de Botium Toys, se deben utilizar cerraduras y CCTV para proteger los activos físicos (incluido el equipo) y para monitorear e investigar posibles amenazas. Si bien no es necesario de inmediato, usar encriptación y tener una caja fuerte con tiempo controlado, iluminación adecuada, gabinetes con cerradura, sistemas de detección y prevención de incendios y señalización que indique el servicio de alarma. El proveedor mejorará aún más la postura de seguridad de Botium Toys.