Memorándum para las partes interesadas

Completa cada sección del memorándum para las partes interesadas a fin de comunicarles los resultados de la auditoría y tus recomendaciones:

- Alcance
- Objetivos
- Hallazgos críticos (que deben abordarse de inmediato)
- Hallazgos (que deben abordarse, aunque no de inmediato)
- Resumen/recomendaciones

A: Gerente/a de TI, partes interesadas
DE: Luis Oviedo
FECHA: 06/09/2024
ASUNTO: Hallazgos y recomendaciones de la autoría interna de TI

Estimados/as compañeros/as:

La siguiente información incluye el ámbito, los objetivos, los hallazgos críticos, un 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 en cuanto a:
○ Permisos de usuario actuales
○ Controles implementados actualmente
○ Procedimientos y protocolos actuales
● Asegurar que los permisos de usuario actuales, controles, procedimientos y protocolos vigentes estén alineados con los requisitos de cumplimiento de PCI DSS y GDPR.
● Asegurar que la tecnología actual, tanto de hardware como de acceso al sistema, esté contabilizada.

Objetivos:
● Adherirse al CSF de NIST.
● Establecer un mejor proceso para sus sistemas para asegurar el cumplimiento.
● Fortalecer los controles del sistema.

● Adaptarse al concepto de mínimos privilegios en la gestión de credenciales de usuario.
● Establecer sus políticas y procedimientos, incluyendo sus manuales operativos.
● Asegurar el cumplimiento de los requisitos normativos.

Hallazgos críticos (que deben abordarse de inmediato):
● Se deben desarrollar e implementar múltiples controles para cumplir con los objetivos de la auditoría, incluyendo:
○ Control de Mínimos Privilegios y Separación de Funciones
○ Planes de recuperación ante desastres
○ Políticas de contraseñas, control de acceso y gestión de cuentas, incluyendo la implementación de un sistema de gestión de contraseñas
○ Cifrado (para transacciones seguras en sitios web)
○ Sistema de detección de intrusiones (IDS)
○ Copias de seguridad
○ Software antivirus (AV)
○ CCTV
○ Cerraduras
○ Monitoreo manual, mantenimiento e intervención 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 la orientación de SOC1 y SOC2 relacionada con políticas de acceso de usuarios y seguridad general de los datos.

Hallazgos (que deben abordarse, aunque no de inmediato):
● Los siguientes controles deben implementarse cuando sea posible:
○ Caja fuerte con control de tiempo ○ Iluminación adecuada
○ Gabinetes con cerradura
○ Señalización que indique el proveedor de servicios de alarmas

Resumen/recomendaciones:
Se recomienda que los hallazgos críticos relacionados con el cumplimiento de PCI DSS y GDPR se aborden de manera inmediata, ya que Botium Toys acepta pagos en línea de clientes en todo el mundo, incluida la UE. Además, dado que uno de los objetivos de la auditoría es adaptarse al concepto de mínimos privilegios, se debe utilizar la orientación de SOC1 y SOC2 relacionada con políticas de acceso de usuarios y seguridad general de datos para desarrollar políticas y procedimientos adecuados. Contar con planes de recuperación ante desastres y copias de seguridad también es fundamental, ya que apoyan la continuidad del negocio en caso de un incidente. Integrar un IDS y software antivirus 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 manual e intervención. Para asegurar aún más los activos ubicados en la única ubicación física de Botium Toys, se deben usar cerraduras y CCTV para asegurar activos físicos (incluido el equipo) y para monitorear e investigar posibles amenazas. Aunque no es necesario de inmediato, el uso de cifrado y la implementación de una caja fuerte con control de tiempo, iluminación adecuada, gabinetes con cerradura, sistemas de detección y prevención de incendios, y señalización que indique el proveedor de servicios de alarmas mejorarán aún más la postura de seguridad de Botium Toys.