Botium Toys: Informe de evaluación de riesgos, objetivos y alcance

Alcance y objetivos de la auditoría.

Alcance: El alcance de esta auditoría se define como todo el programa de seguridad de Botium Toys. Esto incluye sus activos, como equipos y dispositivos de los empleados, su red interna y sus sistemas.

Objetivos: Evalúe los activos existentes y complete la lista de verificación de cumplimiento y controles para determinar qué controles y mejores prácticas de cumplimiento deben implementarse para mejorar la postura de seguridad de Botium Toys.

Activos corrientes

Los activos gestionados por el Departamento de TI incluyen:

- Equipo local para necesidades comerciales en la oficina
- Equipos de los empleados: dispositivos de usuario final (computadoras de escritorio/portátiles, teléfonos inteligentes), estaciones de trabajo remotas, auriculares, cables, teclados, ratones, estaciones de acoplamiento, cámaras de vigilancia, etc.
- Productos de escaparate disponibles para la venta minorista en el sitio y en línea; almacenado en el almacén contiguo de la empresa
- Gestión de sistemas, software y servicios: contabilidad, telecomunicaciones, bases de datos, seguridad, comercio electrónico y gestión de inventarios.
- acceso a Internet
- Red interna
- Retención y almacenamiento de datos
- Mantenimiento de sistemas heredados: sistemas al final de su vida útil que requieren monitoreo humano

Evaluación de riesgos

Descripción del riesgo

Actualmente, existe una gestión inadecuada de los activos. Además, Botium Toys no cuenta con todos los controles adecuados y es posible que no cumpla totalmente con las regulaciones y estándares estadounidenses e internacionales.

Controlar las mejores prácticas

La primera de las cinco funciones del NIST CSF es Identificar. Botium Toys necesitará dedicar recursos a identificar activos para poder gestionarlos adecuadamente. Además, necesitarán clasificar los activos existentes y determinar el impacto de la pérdida de los activos existentes, incluidos los sistemas, en la continuidad del negocio.

Puntuación de riesgo

En una escala del 1 al 10, la puntuación de riesgo es 8, que es bastante alta. Esto se debe a la falta de controles y de cumplimiento de las mejores prácticas de cumplimiento.

Comentarios adicionales

El impacto potencial de la pérdida de un activo se califica como medio, porque el departamento de TI no sabe qué activos estarían en riesgo. El riesgo para los activos o las multas de los órganos rectores es alto porque Botium Toys no cuenta con todos los controles necesarios y no cumple plenamente con las mejores prácticas relacionadas con el cumplimiento de las regulaciones que mantienen la privacidad y seguridad de los datos críticos. Detalles específicos:

- Actualmente, todos los empleados de Botium Toys tienen acceso a datos almacenados internamente y pueden acceder a los datos de los titulares de tarjetas y a la PII/SPII de los clientes.
- Actualmente, el cifrado no se utiliza para garantizar la confidencialidad de la información de la tarjeta de crédito de los clientes que se acepta, procesa, transmite y almacena localmente en la base de datos interna de la empresa.
- No se han implementado controles de acceso relacionados con privilegios mínimos y separación de funciones.
- El departamento de TI ha garantizado la disponibilidad y ha integrado controles para garantizar la integridad de los datos.
- El departamento de TI tiene un firewall que bloquea el tráfico según un conjunto de reglas de seguridad adecuadamente definidas.
- El departamento de TI instala y supervisa periódicamente el software antivirus.
- El departamento de TI no ha instalado un sistema de detección de intrusos (IDS).
- Actualmente no existen planes de recuperación ante desastres y la empresa no cuenta con copias de seguridad de datos críticos.
- El departamento de TI ha establecido un plan para notificar a la UE. clientes dentro de las 72 horas si hay una violación de seguridad. Además, se han desarrollado políticas, procedimientos y procesos de privacidad que se aplican entre los miembros del departamento de TI y otros empleados para documentar y mantener los datos adecuadamente.
- Aunque existe una política de contraseñas, sus requisitos son nominales y no están en línea con los requisitos mínimos actuales de complejidad de contraseñas (por ejemplo, al menos ocho caracteres, una combinación de letras y al menos un número; caracteres especiales).

- No existe un sistema centralizado de administración de contraseñas que haga cumplir los requisitos mínimos de la política de contraseñas, lo que a veces afecta la productividad cuando los empleados/proveedores envían un ticket al departamento de TI para recuperar o restablecer una contraseña.
- Si bien los sistemas heredados son monitoreados y mantenidos, no existe un cronograma regular para estas tareas y los métodos de intervención no están claros.
- La ubicación física de la tienda, que incluye las oficinas principales de Botium Toys, el frente de la tienda y el almacén de productos, cuenta con cerraduras suficientes, vigilancia por circuito cerrado de televisión (CCTV) actualizada, así como sistemas de detección y prevención de incendios en funcionamiento.