Botium Toys: Alcance, objetivos y evaluación de riesgos

Informe

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 los equipos y dispositivos de los empleados, su red interna y sus sistemas. Deberá revisar los activos de Botium Toys y los controles y prácticas de cumplimiento implementados.

Objetivos: Evaluar los activos existentes y completar la lista de verificación de controles y cumplimiento para determinar qué controles y prácticas recomendadas de cumplimiento deben implementarse para mejorar la seguridad de Botium Toys.

Activos actuales

Los activos gestionados por el Departamento de TI incluyen:

● Equipos locales para las necesidades comerciales de la oficina

● Equipos de los empleados: dispositivos de usuario final (computadoras de escritorio/portátiles, teléfonos inteligentes), estaciones de trabajo remotas, auriculares, cables, teclados, ratones, bases de conexión, cámaras de vigilancia, etc.

● Productos de tienda disponibles para la venta minorista en las instalaciones 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 inventario.

● Acceso a internet.

● Red interna.

● Retención y almacenamiento de datos.

● Mantenimiento de sistemas heredados: sistemas al final de su vida útil que requieren supervisión humana.

Evaluación de riesgos

Descripción del riesgo

Actualmente, la gestión de activos es inadecuada. Además, Botium Toys no cuenta con todos los controles adecuados y podría no cumplir plenamente con las regulaciones y estándares estadounidenses e internacionales.

Mejores prácticas de control

La primera de las cinco funciones del CSF del NIST es Identificar. Botium Toys deberá dedicar recursos a identificar los activos para poder gestionarlos adecuadamente.

Además, deberá clasificar los activos existentes y determinar el impacto de la pérdida de estos, incluidos los sistemas, en la continuidad del negocio.

Puntuación de riesgo

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

Comentarios adicionales

El impacto potencial de la pérdida de un activo se califica como medio, ya que el departamento de TI desconoce qué activos estarían en riesgo. El riesgo para los activos o las multas de los organismos gubernamentales es alto porque Botium Toys no cuenta con todos los controles necesarios ni se adhiere plenamente a las mejores prácticas relacionadas con las regulaciones de cumplimiento que mantienen la privacidad y seguridad de los datos críticos. Revise los siguientes puntos para obtener detalles específicos:

● Actualmente, todos los empleados de Botium Toys tienen acceso a los datos almacenados internamente y podrían acceder a los datos de los titulares de tarjetas y a la información personal identificable (PII)/información personal identificable (SPII) de los clientes.

● Actualmente no se utiliza cifrado para garantizar la confidencialidad de la información de las tarjetas 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 el mínimo privilegio y la 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 cuenta con un firewall que bloquea el tráfico según un conjunto de reglas de seguridad adecuadamente definidas.

● El departamento de TI instala y supervisa periódicamente un software antivirus.

* El departamento de TI no ha instalado un sistema de detección de intrusiones (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 los clientes de la UE en un plazo de 72 horas en caso de una vulneración 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 adecuadamente los datos.

● Aunque existe una política de contraseñas, sus requisitos son nominales y no se ajustan a 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 gestión de contraseñas que aplique los requisitos mínimos de la política de contraseñas, lo que a veces afecta la productividad cuando los empleados o proveedores envían una solicitud al departamento de TI para recuperar o restablecer una contraseña.

● Si bien los sistemas heredados se monitorean y mantienen, 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, la fachada y el almacén de productos, cuenta con cerraduras suficientes, circuito cerrado de televisión (CCTV) actualizado y sistemas de detección y prevención de incendios en funcionamiento.