Sebastian Mauricio González Rueda

Agosto 2024

Auditoria de seguridad interna

Escenario (empresa ficticia)

Botium Toys es una pequeña empresa estadounidense que desarrolla y vende juguetes. La empresa tiene una sola sede física. Sin embargo, su presencia en línea ha crecido, atrayendo a clientes de Estados Unidos y del extranjero. Su departamento de tecnología de la información (TI) está sometido a una presión cada vez mayor para dar soporte a su mercado en línea en todo el mundo.

La gerente del departamento de TI ha decidido que es necesario realizar una auditoría interna de TI. Expresa su preocupación por no tener un plan de acción consolidado para garantizar la continuidad del negocio y el cumplimiento de la normativa, a medida que la empresa crece. Cree que una auditoría interna puede ayudar a asegurar mejor la infraestructura de la empresa y ayudar a identificar y mitigar los posibles riesgos, amenazas o vulnerabilidades de los activos críticos. La gerente también está interesada en asegurarse de que cumplen con la normativa relacionada con la aceptación de pagos en línea y la realización de negocios en la Unión Europea (UE).

La gerente de TI comienza aplicando el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST), estableciendo un alcance y unos objetivos de auditoría y completando una evaluación de riesgos. El objetivo de la auditoría es proporcionar una visión general de los riesgos que la empresa podría experimentar debido al estado actual de su postura de seguridad. La gerente de TI quiere utilizar los resultados de la auditoría como prueba para obtener la aprobación para ampliar su departamento.

La auditoría interna de TI de Botium Toys analizará lo siguiente:

- Permisos de usuario actuales creados en los siguientes sistemas: contabilidad, detección de puntos de conexión, cortafuegos (firewalls), sistema de detección de intrusiones, herramienta de gestión de eventos e información de seguridad (SIEM).
- Controles actuales implementados en los siguientes sistemas: contabilidad, detección de puntos de conexión, cortafuegos (firewalls), sistema de detección de intrusiones, herramienta de gestión de eventos e información de seguridad (SIEM).
- Procedimientos y protocolos actuales establecidos para los siguientes sistemas: contabilidad, detección de puntos de conexión, cortafuegos (firewall), sistema de detección de intrusiones, herramienta de gestión de eventos e información de seguridad (SIEM).
- Comprueba si los permisos, controles, procedimientos y protocolos actuales de los usuarios y las usuarias están alineados con los requisitos de cumplimiento normativo necesarios.
- Verifica si la tecnología actual está debidamente registrada, tanto el hardware como el acceso al sistema.

Objetivos:

Los objetivos de la auditoría interna de TI de Botium Toys son los siguientes:

- Cumplir con el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST).
- Establecer un proceso más efectivo para garantizar el cumplimiento de los sistemas.
- Fortalecer los controles del sistema.
- Implementar el principio de mínimo privilegio en la gestión de credenciales o tarjetas de identificación de usuarios/as.
- Establecer políticas y procedimientos claros, que incluyan manuales de estrategia.
- Asegurarse el acatamiento de los requisitos de cumplimiento normativo.

Descripción del riesgo

Actualmente, existe una gestión insuficiente de los activos. Además, Botium Toys no ha implementado los controles adecuados y es posible que no cumpla con las regulaciones y los estándares estadounidenses e internacionales.

- Prácticas recomendadas de control

La primera de las cinco funciones del Marco de Ciberseguridad del NIST es la identificación. Botium Toys deberá asignar recursos para gestionar los activos. Además, tendrá que determinar el impacto de la pérdida de los activos existentes, incluidos los sistemas, en la continuidad del negocio.

- Puntuación de riesgo

En una escala de 1 a 10, la puntuación de riesgo es de 8, lo cual es bastante alto. Esto se debe a la falta de controles y cumplimiento de las regulaciones y los estándares necesarios.

- Comentarios adicionales

El impacto potencial por la pérdida de un activo se califica como medio, debido a que el departamento de TI no sabe qué activos se perderían. La probabilidad de pérdida de un activo o de multas por parte de órganos reguladores es alta, ya que Botium Toys no tiene todos los controles necesarios implementados y no cumple con las normativas y estándares requeridos para mantener la privacidad de los datos de los clientes.

Listado De Evaluación De Controles

Activos actuales

Entre los activos administrados por el departamento de TI se encuentran los siguientes:

1. Equipos en las instalaciones para las necesidades comerciales en la oficina.
2. Equipos del personal: dispositivos de usuario final (computadoras de escritorio/portátiles, teléfonos inteligentes), estaciones de trabajo remotas, auriculares, cables, teclados, mouse, estaciones de acoplamiento, cámaras de vigilancia, etc.
3. Gestión de sistemas, software y servicios: contabilidad, telecomunicaciones, bases de datos, seguridad, comercio electrónico y gestión de inventario.
4. Acceso a Internet.
5. Red interna.
6. Gestión de acceso a proveedores.
7. Servicios de alojamiento del centro de datos.
8. Retención y almacenamiento de datos.
9. Lectores de tarjetas de identificación.
10. Mantenimiento de sistemas heredados: sistemas obsoletos que requieren supervisión humana.

Controles administrativos			
Nombre de control	**Tipo de control y explicación**	**Se tiene que implementar (X)**	**Prioridad**
Principio de mínimo privilegio	Preventivo. Reducir el riesgo asegurándose de que proveedores y el personal no autorizado solo tengan acceso a los activos/datos que necesitan para realizar su trabajo.	**X**	ALTA
Planes de recuperación ante incidentes	Correctivo. Garantizar la continuidad del negocio, asegurando que los sistemas puedan ejecutarse en caso de incidentes, que no haya pérdida de productividad por tiempo de inactividad ni impacto en los componentes del sistema, que incluyen entorno de la sala de computadoras (aire acondicionado, fuentes de alimentación, etc.), hardware (servidores, equipos de empleados), conectividad (red interna, inalámbrica), aplicaciones (correo electrónico, datos electrónicos), así como datos y restauración.	**X**	ALTA
Políticas de contraseñas	Preventivo. Establecer requisitos de seguridad de contraseñas para reducir la probabilidad de comprometer la cuenta debido a técnicas de ataque por fuerza bruta o diccionario.	**X**	MEDIA
Políticas de control de acceso	Preventivo. Aumentar la confidencialidad e integridad de los datos.	**X**	ALTA

Controles administrativos			
Políticas de gestión de cuentas	Preventivo. Reducir la superficie expuesta a ataques y limita el impacto general de ex empleados/as disconformes.	**X**	ALTA
Separación de funciones	Preventivo. Garantizar que nadie tenga tanto acceso que pueda abusar del sistema para obtener beneficios personales.	**X**	ALTA

Controles técnicos			
Nombre de control	**Tipo de control y explicación**	**Se tiene que implementar (X)**	**Prioridad**
Cortafuegos (firewall)	Preventivo. Ya hay instalados firewalls para filtrar el tráfico no deseado/malicioso que ingresa a la red interna.		N/A
Sistema de detección de intrusiones (IDS)	De detección. Permitir al equipo de TI identificar posibles intrusiones (por ejemplo, tráfico anómalo) rápidamente.	**X**	ALTA/MEDIA
Cifrado	Disuasivo. Garantizar que la información y los datos confidenciales sean más seguros (por ejemplo, transacciones de pago en el sitio web).	**X**	MEDIA

Copias de seguridad	Correctivo. Permitir la continuidad del negocio y mantener la productividad en caso de incidentes, al mantener los sistemas funcionando.	X	BAJA
Gestión de contraseñas	Correctivo. Recuperar y restablecer contraseñas, bloqueo de notificaciones.	X	MEDIA
Software de antivirus (AV)	Correctivo. Detectar amenazas conocidas y aislarlas.	X	MEDIA
Monitoreo manual, mantenimiento e intervención	Preventivo/correctivo. Necesario para que los sistemas heredados identifiquen y mitiguen posibles amenazas, riesgos y vulnerabilidades.	X	ALTA

Controles físicos			
Nombre de control	**Tipo de control y explicación**	**Se tiene que implementar (X)**	**Prioridad**
Caja fuerte con control de tiempo	Disuasivo. Reducir la superficie expuesta a ataque y el impacto de las amenazas físicas.		N/A
Iluminación adecuada	Disuasivo. Limitar los lugares “ocultos” para disuadir las amenazas.		N/A
Vigilancia del circuito cerrado de televisión (CCTV)	Preventivo/De detección. Reducir el riesgo de ciertos eventos y ver qué sucedió, después del incidente al llevar a cabo una investigación.	X	BAJA

Cerradura de gabinetes (para equipos de red)	Preventivo. Aumentar la integridad al evitar que personas no autorizadas accedan físicamente o modifiquen el equipo de infraestructura de la red.	X	BAJA
Carteles que indican el nombre de la empresa proveedora del servicio de alarmas	Disuasivo. Reducir la probabilidad de éxito de ciertos tipos de amenazas al dar la apariencia de que un ataque exitoso es poco probable.	X	BAJA
Cerraduras	Preventivo. Lograr que los activos físicos y digitales estén más seguros.	X	BAJA
Detección y prevención de incendios (alarma de incendios, sistema de rociadores, entre otros)	De detección/Preventivo. Detectar incendios en la ubicación física de la juguetería para evitar daños en el inventario, servidores, entre otros.	X	BAJA

Lista de control de cumplimiento normativo

_____ La Comisión Federal de Regulación de Energía, Corporación de Confiabilidad Eléctrica América del Norte (FERC-NERC)

La normativa FERC-NERC se aplica a organizaciones que trabajan con electricidad o que están involucradas con la red eléctrica de los Estados Unidos y América del Norte. Las empresas tienen la obligación de prepararse, mitigar y reportar cualquier incidente de seguridad potencial que pueda afectar negativamente a la red eléctrica. También están legalmente obligadas a cumplir con los Estándares de Confiabilidad de Protección de Infraestructura Crítica (CIP) definidos por la FERC.

Explicación: N/A

___X__ Reglamento General de Protección de Datos (RGPD)

El RGPD es una regulación general de datos de la Unión Europea (UE) que protege el procesamiento de los datos de sus residentes y su derecho a la privacidad dentro y fuera del territorio. Además, si se produce una filtración y los datos de una persona se ven comprometidos, esto debe ser informado en un plazo de 72 horas posteriores al incidente.

Explicación: debe cumplir con el RGPD para proteger los datos personales de sus clientes y más que la empresa esta creciendo alrededor del mundo, cumplir con los derechos de privacidad, evitar sanciones económicas y salvaguardar su reputación. Dado que el comercio digital y los servicios en línea son cada vez más relevantes y la empresa recopila información de sus clientes, garantizar la protección de los datos se convierte en una prioridad para la empresa.

__X___ Estándares de seguridad de datos del sector de las tarjetas de pago (PCI DSS)

PCI DSS es un estándar de seguridad internacional destinado a garantizar que las organizaciones que almacenan, aceptan, procesan y transmiten información de tarjetas de crédito lo hagan en un entorno seguro.

Explicación: cumplir con la PCI DSS no solo es una obligación para aceptar pagos con tarjeta, sino también una forma de proteger a sus clientes, evitar sanciones y asegurar la continuidad del negocio. Implementar este estándar mejora la seguridad de las transacciones y la confianza de los consumidores, lo que es clave en el competitivo mundo del comercio online.

_____ Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA)

La HIPAA es una ley federal de los Estados Unidos establecida en 1996 para proteger la información médica de las personas. Esta ley prohíbe que la información de un/a paciente sea compartida sin su consentimiento. Las organizaciones tienen la obligación legal de informar a los/las pacientes en caso de que esta información se filtre.

Explicación: N/A

__X___ Controles de Sistemas y Organizaciones (SOC tipo 1, SOC tipo 2)

El SOC1 y el SOC2 se enfocan en las políticas de acceso de los usuarios y las usuarias de una organización en los diferentes niveles. Se utilizan para evaluar el cumplimiento financiero de una organización, así como los niveles de riesgo asociados. También abordan aspectos críticos como la confidencialidad, privacidad, integridad, disponibilidad, seguridad y protección general de los datos. Es importante destacar que cualquier falla en el control de estos aspectos puede resultar en posibles fraudes.

Explicación: Estas certificaciones no solo aseguran que la información de los clientes esté protegida, sino que también mejoran la reputación de la empresa, proporcionan transparencia a los socios comerciales y ayudan a gestionar mejor los riesgos. SOC Tipo 1 garantiza que los controles están diseñados adecuadamente, mientras que SOC Tipo 2 demuestra que esos controles funcionan de manera efectiva a lo largo del tiempo.

Memorándum para las partes interesadas

A: Gerente/a de TI, partes interesadas

DE: Sebastian Mauricio Gonzalez Rueda
FECHA: Agosto 25, 2024
ASUNTO: Hallazgos y recomendaciones de la autoría interna de TI

Estimados compañeros:

A continuación, se presenta un resumen de los resultados de la auditoría interna de seguridad de TI de Botium Toys, junto con recomendaciones clave para garantizar la mejora continua de la infraestructura tecnológica y el cumplimiento normativo de la empresa.

Alcance:

La auditoría interna de TI tuvo como objetivo evaluar la situación actual de los permisos de usuario, controles, procedimientos y protocolos en los sistemas críticos de la empresa, incluyendo contabilidad, detección de puntos de conexión, cortafuegos, sistema de detección de intrusiones y la herramienta de gestión de eventos e información de seguridad (SIEM). También se revisó el cumplimiento con normativas clave como el RGPD y PCI DSS.

Objetivos:

1. Cumplir con el Marco de Ciberseguridad (CSF) del NIST.
2. Establecer un proceso efectivo de cumplimiento de sistemas.
3. Fortalecer los controles de seguridad, especialmente en la gestión de acceso.
4. Implementar el principio de mínimo privilegio en la gestión de usuarios.
5. Asegurar el cumplimiento normativo y evitar sanciones.

Hallazgos críticos (que deben abordarse de inmediato):

- **Gestión de activos insuficiente**: No se tiene un control claro sobre los activos críticos, lo que pone en riesgo la continuidad del negocio.
- **Falta de controles de acceso estrictos**: La ausencia de una política clara de gestión de cuentas y separación de funciones puede facilitar accesos no autorizados y potenciales abusos.
- **Cumplimiento normativo insuficiente**: La empresa no cumple totalmente con las normativas PCI DSS y SOC, lo que aumenta el riesgo de fraudes y sanciones regulatorias.

Hallazgos (que deben abordarse, aunque no de inmediato):

- **Cifrado y copias de seguridad**: Si bien se han implementado algunas medidas de seguridad, el cifrado de datos sensibles y las copias de seguridad no están completamente optimizados para garantizar la máxima protección.
- **Monitoreo y sistemas de detección de intrusiones (IDS)**: Aunque se cuenta con sistemas IDS, su uso debe optimizarse para identificar amenazas potenciales con mayor rapidez.
- **Controles físicos de bajo impacto**: Elementos como la vigilancia por circuito cerrado de televisión y el sistema de alarmas requieren mejoras en su cobertura y efectividad.

Resumen/recomendaciones:

Para mejorar la postura de seguridad de la empresa y mitigar los riesgos identificados, recomiendo lo siguiente:

- **Priorizar la gestión de activos** para garantizar que todos los sistemas y dispositivos estén adecuadamente identificados y protegidos.
- Implementar de inmediato un **control de acceso basado en roles** y el **principio de mínimo privilegio**, limitando el acceso a los datos según las necesidades específicas de cada usuario.
- **Asegurar el cumplimiento normativo** con PCI DSS y SOC tipo 2, implementando medidas de seguridad adicionales en los sistemas que manejan datos financieros y personales de clientes.
- **Fortalecer las políticas de cifrado y copias de seguridad**, garantizando que todos los datos confidenciales estén adecuadamente protegidos tanto en tránsito como en almacenamiento.
- Mejorar los **sistemas de detección y respuesta ante intrusiones**, asegurando una vigilancia constante y respuesta rápida ante incidentes de seguridad.