Evaluación de controles

Activos actuales

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

- Equipos en las instalaciones para las necesidades comerciales en la oficina.
- 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.
- Gestión de sistemas, software y servicios: contabilidad, telecomunicaciones, bases de datos, seguridad, comercio electrónico y gestión de inventario.
- Acceso a Internet.
- Red interna.
- Gestión de acceso a proveedores.
- Servicios de alojamiento del centro de datos.
- Retención y almacenamiento de datos.
- Lectores de tarjetas de identificación.
- 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

Controles administrativos			
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	ALTA
Políticas de control de acceso	Preventivo. Aumentar la confidencialidad e integridad de los datos.	X	ALTA
Políticas de gestión de cuentas	Preventivo. Reducir la superficie expuesta a ataques y limita el impacto general de ex empleados/as disconformes.	X	MEDIA
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.	NO	NO APLICA
Sistema de detección de intrusiones (IDS)	De detección. Permitir al equipo de TI identificar posibles intrusiones (por ejemplo, tráfico anómalo) rápidamente.	X	ALTO
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	ALTA
Gestión de contraseñas	Correctivo. Recuperar y restablecer contraseñas, bloqueo de notificaciones.	X	ALTA
Software de antivirus (AV)	Correctivo. Detectar amenazas conocidas y aislarlas.	X	ALTA
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.	X	BAJA
Iluminación adecuada	Disuasivo. Limitar los lugares “ocultos” para disuadir las amenazas.	X	MEDIA
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	MEDIA
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	MEDIA
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	BAJO
Cerraduras	Preventivo. Lograr que los activos físicos y digitales estén más seguros.	X	ALTA
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	ALTA

Lista de control de cumplimiento normativo

Para revisar las regulaciones y estándares de cumplimiento normativo, lee el documento sobre controles, marcos y 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: No aplica

__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: Botium Toys tiene que cumplir con el RGPD porque trabaja con datos de las personas de todo el mundo, incluida la UE.

___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: Botium Toys tiene que cumplir con los estándares PCI DSS para proteger la información de los titulares de tarjetas de crédito, ya que guarda y procesa esta información de manera presencial y en línea.

_____ **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: No aplica

__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: Botium Toys necesita garantizar la seguridad financiera y de datos, reducir riesgos operacionales, cumplir con normativas de seguridad, y fortalecer la confianza de clientes y terceros.

Memorándum para las partes interesadas

A: Gerente/a de TI, partes interesadas
DE: Vicente Alfredo García Nava
FECHA: 02/10/2024
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 incluidos: contabilidad, detección de puntos finales, firewalls, sistema de detección de intrusiones, herramienta SIEM. Los sistemas se evaluarán en cuanto a:
    - Permisos de usuario actuales
    - Controles implementados actuales
    - Procedimientos y protocolos actuales
- Asegurarse de que los permisos de usuario, controles, procedimientos y protocolos actuales estén implementados conforme a los requisitos de cumplimiento de PCI DSS y GDPR.
- Asegurarse de que la tecnología actual se tenga en cuenta tanto para el acceso al hardware como al sistema.

Objetivos:

- Cumplir con el CSF del NIST.
- Establecer un mejor proceso para sus sistemas a fin de garantizar que cumplan con las normas.
- Reforzar los controles del sistema.
- Adaptarse al concepto de permisos mínimos en lo que respecta a la gestión de credenciales de usuario.
- Establecer sus políticas y procedimientos, incluidos sus manuales de estrategias.
- Asegurarse de que cumplen con los requisitos de cumplimiento.

Hallazgos críticos (que deben abordarse de inmediato):

- Se deben desarrollar e implementar múltiples controles para cumplir con los objetivos de la auditoría, entre ellos:
    - Control de privilegios mínimos y separación de funciones
    - Planes de recuperación ante desastres
    - Políticas de contraseñas, control de acceso y administración de cuentas, incluida la implementación de un sistema de administración de contraseñas
    - Cifrado (para transacciones seguras en sitios web)
    - IDS
    - Copias de seguridad
    - Software de AV
    - CCTV
    - Cerraduras
    - Monitoreo, mantenimiento e intervención manuales para sistemas heredados
    - Sistemas de detección y prevención de incendios
- Se deben desarrollar e implementar políticas para cumplir con los requisitos de cumplimiento de PCI DSS y GDPR.
- Se deben 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.

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

- Se deben implementar los siguientes controles cuando sea posible:
    - Caja fuerte con control de tiempo
    - Iluminación adecuada
    - Armarios con cerradura
    - Señalización que indique el proveedor del servicio de alarma

Resumen/recomendaciones:

Se recomienda que los hallazgos críticos relacionados con el cumplimiento de PCI DSS y GDPR se aborden de inmediato, ya que Botium Toys acepta pagos en línea de clientes de todas partes del mundo, incluida la Unión Europea. Además, dado que uno de los objetivos de la auditoría es adaptarse al concepto de permisos mínimos, se deben utilizar las pautas 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 de desastres y copias de seguridad también es fundamental porque respaldan la continuidad del negocio en caso de un incidente. La integración de un software de detección de intrusiones y antivirus en los sistemas actuales respaldará la capacidad de identificar y mitigar riesgos potenciales, y podría ayudar con la detección de intrusos, ya que los sistemas heredados existentes requieren monitoreo e intervención manuales. Para proteger aún más los activos alojados en la ubicación física única de Botium Toys, se deben usar cerraduras y CCTV para proteger los activos físicos (incluido el equipo) y para monitorear e investigar las amenazas potenciales. Por último, no es necesario de inmediato, pero el uso de cifrado y tener 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 alarma mejorarán aún más la postura de seguridad de la empresa.