A: Gerente/a de TI, partes interesadas

DE: Jorge Daniel Bellerate  
FECHA: 05 de Octubre del 2023

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:**

●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 las usuarias y los usuarios están alineados con los requisitos de cumplimiento normativo necesarios.

**Objetivos:**

Nuestros objetivos incluyen cumplir con el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST), establecer un proceso más eficiente para garantizar el cumplimiento de los sistemas, reforzar los controles del sistema, implementar el principio de mínimo privilegio en la gestión de credenciales o tarjetas de identificación de usuarios, establecer políticas y procedimientos bien definidos que incluyan manuales de estrategia, y asegurar el cumplimiento de los requisitos normativos

**Hallazgos críticos** (que deben abordarse de inmediato):

En el ámbito de los **controles administrativos**, implementamos diversos principios y políticas para garantizar la seguridad de nuestros activos y datos:

**Principio de Mínimo Privilegio**: Adoptamos un enfoque preventivo para reducir el riesgo al garantizar que proveedores y personal no autorizado solo tengan acceso a los recursos y datos necesarios para llevar a cabo sus responsabilidades, evitando así posibles brechas de seguridad.

**Planes de Recuperación Ante Incidentes**: Aseguramos que nuestros sistemas sean capaces de funcionar en caso de incidentes, minimizando la pérdida de productividad debido al tiempo de inactividad. Esto abarca desde la infraestructura de la sala de servidores hasta la conectividad y las aplicaciones, garantizando la continuidad operativa.

**Políticas de Contraseñas**: Mediante políticas de contraseñas sólidas, prevenimos ataques por fuerza bruta o diccionario, aumentando la seguridad de las cuentas y reduciendo el riesgo de comprometerlas.

**Políticas de Control de Acceso**: Fortalecemos la confidencialidad e integridad de los datos mediante políticas de control de acceso, asegurando que solo las personas autorizadas tengan acceso a la información relevante.

**Políticas de Gestión de Cuentas:** Para reducir la exposición a riesgos y limitar el impacto de ex empleados/as insatisfechos, implementamos políticas de gestión de cuentas efectivas que incluyen la desactivación o eliminación de cuentas de manera oportuna.

**Separación de Funciones:** Garantizamos que ninguna persona tenga un nivel de acceso que permita un posible abuso del sistema con fines personales, previniendo posibles conflictos de intereses y asegurando la integridad de nuestras operaciones."

**Estas políticas y principios administrativos son fundamentales para mantener la seguridad y el cumplimiento normativo en nuestra organización.**

Dentro de nuestros **controles técnicos**, implementamos una serie de medidas para salvaguardar la seguridad de nuestros sistemas y datos:

**Sistema de Detección de Intrusiones (IDS):** Con un enfoque en la detección, este sistema permite a nuestro equipo de TI identificar rápidamente posibles intrusiones, como tráfico anómalo, para tomar medidas inmediatas.

**Cifrado:** Utilizamos cifrado como una medida disuasiva para garantizar que la información y los datos confidenciales estén protegidos, especialmente en transacciones de pago en nuestro sitio web.

**Copias de Seguridad:** Como un enfoque correctivo, realizamos copias de seguridad regulares para asegurar la continuidad del negocio y mantener la productividad en caso de incidentes, lo que permite que nuestros sistemas sigan funcionando sin interrupciones.

**Gestión de Contraseñas**: En un contexto correctivo, nuestra política de gestión de contraseñas nos permite recuperar y restablecer contraseñas cuando sea necesario y bloquear notificaciones no autorizadas.

**Software de Antivirus (AV):** Como medida correctiva, utilizamos software de antivirus para detectar y aislar amenazas conocidas, protegiendo nuestros sistemas contra posibles ataques.

**Monitoreo Manual, Mantenimiento e Intervención**: Adoptamos un enfoque preventivo y correctivo a través del monitoreo y mantenimiento manual de sistemas heredados. Esto nos permite identificar y mitigar posibles amenazas, riesgos y vulnerabilidades para mantener la integridad de nuestros sistemas."

**Estos controles técnicos desempeñan un papel fundamental en nuestra estrategia de seguridad cibernética y son esenciales para mantener la integridad y la disponibilidad de nuestros sistemas y datos.**

En nuestra estrategia de seguridad, implementamos una variedad de **controles físicos** para proteger nuestros activos y garantizar un ambiente seguro:

Prioridad Alta:

Vigilancia del Circuito Cerrado de Televisión (CCTV): Este control de alta prioridad nos permite reducir el riesgo de eventos no deseados y llevar a cabo investigaciones posteriores a incidentes. Proporciona una visión detallada de lo que sucede en nuestras instalaciones.

Cerraduras: Como medida preventiva de alta prioridad, se implementan para asegurar que nuestros activos físicos y digitales estén protegidos.

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

**Otros Controles Físicos**:

Caja Fuerte con Control de Tiempo: Un enfoque disuasivo que limita la superficie expuesta a ataques y reduce el impacto de las amenazas físicas.

Iluminación Adecuada: Esta medida disuasiva garantiza que no haya lugares "ocultos" que puedan utilizarse para actividades maliciosas.

Cerradura de Gabinetes (para Equipos de Red): Enfoque preventivo para aumentar la integridad de nuestra infraestructura de red al evitar el acceso no autorizado o la modificación de los equipos.

Carteles que Indican el Nombre de la Empresa Proveedora del Servicio de Alarmas: Una medida disuasiva que reduce la probabilidad de éxito de ciertas amenazas, creando la apariencia de que un ataque exitoso es improbable.

Detección y Prevención de Incendios: Este control de detección y prevención incluye alarmas de incendios y sistemas de rociadores para detectar y prevenir incendios en nuestras instalaciones, protegiendo así nuestro inventario y servidores.

Estos controles físicos desempeñan un papel crucial en nuestra estrategia global de seguridad, garantizando un ambiente seguro y la protección de nuestros activos.

**Resumen/recomendaciones:**

Hemos implementado una variedad de controles físicos, administrativos y técnicos para garantizar la seguridad y la integridad de nuestros activos y datos. Desde principios como el "Mínimo Privilegio" y políticas de contraseñas sólidas hasta medidas técnicas como el cifrado y la vigilancia de CCTV, nuestro enfoque es integral y busca minimizar los riesgos asociados a amenazas cibernéticas y físicas.

Recomendaciones:

Continuar manteniendo una cultura de seguridad sólida, educando a nuestro personal sobre la importancia de cumplir con las políticas y prácticas de seguridad.

Evaluar regularmente la efectividad de nuestros controles y realizar auditorías de seguridad para identificar posibles vulnerabilidades y áreas de mejora.

Priorizar la implementación de sistemas de vigilancia de CCTV, especialmente en áreas críticas, para mejorar la capacidad de detectar y responder a incidentes.

Reforzar las políticas de control de acceso y gestión de cuentas para limitar el acceso no autorizado y garantizar una rápida respuesta a las solicitudes de recuperación de contraseñas.

Continuar educando a los empleados sobre la importancia de la seguridad física, incluyendo la necesidad de mantener cerraduras y tarjetas de identificación seguras.

Asegurarse de que los planes de recuperación ante incidentes estén actualizados y probados regularmente para garantizar una rápida recuperación en caso de interrupciones.

Periódicamente, revisar y actualizar nuestras políticas de seguridad en función de las tendencias y amenazas emergentes en el ámbito de la ciberseguridad y la seguridad física.

Estas recomendaciones fortalecerán aún más nuestra postura de seguridad y nos ayudarán a mantener un entorno protegido y resiliente.