PROYECTO DE APLICACIÓN:

1. Introducción a la Ciberseguridad

La ciberseguridad es el conjunto de prácticas, procesos y tecnologías diseñadas para proteger los sistemas, redes y datos contra ataques cibernéticos. En un entorno digitalizado como el actual, las amenazas cibernéticas son cada vez más sofisticadas, lo que hace que la ciberseguridad sea esencial para cualquier organización. Los elementos clave de la ciberseguridad incluyen la protección de la confidencialidad, integridad y disponibilidad de la información (conocido como el triángulo CIA), además de garantizar la autenticidad y no repudio de las comunicaciones digitales. Por lo tanto, TechCo, al manejar una amplia gama de datos sensibles, tanto propios como de sus clientes debe garantizar el cumplimiento de los siguientes objetivos:

- **Protección de datos**: Garantizar que la información de los clientes y la propia de TechCo esté protegida contra accesos no autorizados.
- **Protección de la infraestructura**: Asegurar que los sistemas, servidores y redes de TechCo estén a salvo de ataques que puedan comprometer su funcionamiento.
- **Cumplimiento normativo**: Asegurar que TechCo cumpla con todas las normativas y regulaciones aplicables en su industria y región.
- **Resiliencia operativa**: Desarrollar y mantener la capacidad de TechCo para responder y recuperarse rápidamente de incidentes de seguridad.

2. Amenazas Cibernéticas

Las principales amenazas cibernéticas son:

- **Malware**: Software malicioso diseñado para dañar, interrumpir o tomar control de sistemas. Esto incluye virus, troyanos y spyware. Para TechCo, un ataque de malware podría significar la pérdida de datos críticos o el compromiso de la seguridad de sus clientes.
- **Ransomware**: Un tipo de malware que cifra los datos del usuario y exige un rescate para su liberación. Un ataque de ransomware puede paralizar las operaciones de TechCo y dañar su reputación.

- **Phishing**: Técnica utilizada por los atacantes para engañar a los usuarios para que revelen información sensible, como credenciales de acceso. Los empleados de TechCo podrían ser blanco de estos ataques, comprometiendo la seguridad interna.

TechCo debe asegurar que su infraestructura de red esté protegida contra estas amenazas. Esto implica implementar arquitecturas de red seguras, utilizar protocolos de seguridad como SSL/TLS, desplegar firewalls para filtrar tráfico no autorizado y emplear VPNs para proteger la comunicación remota.

Integridad, Confidencialidad y Disponibilidad

- **Integridad**: Asegurar que los datos no sean alterados o manipulados sin autorización. Esto es crucial para mantener la fiabilidad de los sistemas de TechCo.
- **Confidencialidad**: Proteger la información sensible contra el acceso no autorizado. TechCo debe implementar controles de acceso estrictos y cifrado de datos.
- **Disponibilidad**: Garantizar que los sistemas y datos estén disponibles cuando se necesiten. Esto requiere planes de recuperación ante desastres y redundancias en la infraestructura.

3. Criptografía

La criptografía es el arte de convertir la información en un formato ininteligible para cualquier persona que no tenga la clave adecuada. Los procesos de cifrado y descifrado son fundamentales para proteger la confidencialidad de los datos.

Algoritmos de Cifrado

- **AES (Advanced Encryption Standard)**: Un algoritmo de cifrado simétrico utilizado ampliamente por su eficiencia y seguridad.
- **RSA (Rivest-Shamir-Adleman)**: Un algoritmo de cifrado asimétrico que se utiliza para el cifrado de datos y firmas digitales.
- **ECC (Elliptic Curve Cryptography)**: Un algoritmo de cifrado asimétrico que ofrece una mayor seguridad con claves más pequeñas en comparación con RSA.

Comparación entre Criptografía Simétrica y Asimétrica

La Criptografía de Clave Simétrica utiliza la misma clave para cifrar y descifrar. Es rápido y eficiente, pero la distribución segura de la clave es un desafío; mientras que la de Clave Asimétrica Utiliza un par de claves (pública y privada). Es más seguro para la transmisión de claves, pero más lento en términos de procesamiento.

4. Políticas y Estándares de Seguridad

TechCo debe cumplir con regulaciones como el GDPR, que exige la protección de los datos personales de los ciudadanos de la UE. También debe considerar leyes locales de privacidad según su ubicación geográfica. Los Frameworks de seguridad más comunes son: el ISO 27001 que es un estándar internacional para la gestión de la seguridad de la información y el NIST Cybersecurity Framework que proporciona un enfoque basado en cinco funciones clave: Identificar, Proteger, Detectar, Responder y Recuperar. TechCo debe implementar y cumplir con estándares de seguridad específicos según su industria.

5. Gestión de Riesgos y Continuidad del Negocio

TechCo debe realizar un análisis exhaustivo de riesgos para identificar las amenazas y vulnerabilidades específicas de su entorno. Esto incluye evaluar la probabilidad e impacto de diferentes escenarios de amenaza. En caso de un incidente de seguridad, TechCo debe tener un plan de respuesta bien definido que incluya la identificación del incidente, la contención, erradicación y recuperación, además de la comunicación interna y externa adecuada. Finalmente TechCo debe desarrollar planes de continuidad del negocio que aseguren la disponibilidad de sus servicios, incluso en situaciones de interrupción. Esto incluye la planificación para desastres naturales, fallos tecnológicos y ataques cibernéticos.

6. Mejores Prácticas

TechCo debería seguir las mejores prácticas publicadas por instituciones como el NIST y el CIS, que incluyen: Implementación de controles de acceso estrictos, monitoreo continuo y gestión de parches, la realización de pruebas de penetración periódicas y una capacitación continua del personal en ciberseguridad.

Referencias:

ManageEngine. (s/f). *¿Qué son y cómo implementar los Controles de CIS?* Manageengine.com. Recuperado el 27 de agosto de 2024, de https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

El empresario, U. G. de A. P. (s/f). *Gestión de riesgos*. Incibe.es. Recuperado el 27 de agosto de 2024, de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

¿Qué es el cifrado? Definición de cifrado de datos. (2023, julio 14). Ibm.com. https://www.ibm.com/es-es/topics/encryption

Ciberseguridad: amenanzas principales y emergentes. (s/f). Temas | Parlamento Europeo. Recuperado el 27 de agosto de 2024, de https://www.europarl.europa.eu/topics/es/article/20220120STO21428/ciberseguridad-amenanzas-principales-y-emergentes