Ciberseguridad en Empresa

Equipo de TI y Servicios en la Nube

¡Bienvenidos al curso de Ciberseguridad!

Protégete y protege la información de la empresa.

Índice

- Definición de ciberseguridad
- Políticas de Ciberseguridad de TechSecure
- Ciberseguridad en la Nube
- Protección de Infraestructura
- Seguridad en el Desarrollo Web
- Respuestas ante Incidentes de Ciberseguridad
- Dudas o Extras

Importancia de la Ciberseguridad

- La ciberseguridad es una prioridad crítica para todas las organizaciones.
- Los ciberataques no solo amenazan los datos sensibles, sino que también comprometen la reputación empresarial.
- La protección de la información es responsabilidad de todos. Al estar comprometidos con las mejores prácticas, ayudamos a mantener la seguridad de la empresa y de nuestros clientes.

Políticas de Ciberseguridad de TechSecure

- **Proteger la confidencialidad, integridad y disponibilidad de la información:** Aseguramos que los datos sean accesibles solo para las personas autorizadas, precisos y siempre disponibles cuando se necesiten.
- **Prevenir, detectar y responder a amenazas cibernéticas**: Implementamos medidas para minimizar el riesgo de ataques, detectar amenazas a tiempo y dar respuestas rápidas y eficaces.
- **Establecer una base de cumplimiento legal y normativo**: Cumplimos con todas las leyes, regulaciones y estándares de la industria relacionados con la protección de datos.
- **Promover una cultura de ciberseguridad**: Fomentamos el compromiso de todos los empleados para integrar prácticas seguras en su día a día.
- **Fortalecer la resiliencia organizacional**: Creamos una infraestructura sólida que permite a la empresa recuperarse rápidamente de cualquier incidente cibernético.
- **Optimizar la gestión de riesgos**: Implementamos un enfoque proactivo para identificar, evaluar y mitigar riesgos antes de que se materialicen.

Ciberseguridad en la Nube

Principios de seguridad en plataformas como AWS, Azure, Google Cloud:

Las plataformas en la nube públicas como AWS, Azure y Google Cloud proporcionan herramientas de seguridad integradas, pero es fundamental comprender los principios básicos de seguridad en estas plataformas. Esto incluye la gestión de identidades, cifrado, y la protección de datos.

Asegurar la configuración de las instancias, controlar accesos, utilizar la gestión de identidades (IAM) para gestionar permisos y aplicar el cifrado tanto en reposo como en tránsito.

Ciberseguridad en la Nube

Gestión de identidades y accesos (IAM):

Explicación: IAM permite gestionar quién tiene acceso a los recursos de la nube y qué acciones pueden realizar. Implementar IAM correctamente es crucial para garantizar que solo los usuarios autorizados puedan acceder a los servicios.

Utilizar roles y permisos mínimos, aplicar el principio de "menos privilegios" y habilitar la autenticación multifactor (MFA).

Ciberseguridad en la Nube

Seguridad en bases de datos y almacenamiento en la nube:

La seguridad de las bases de datos y el almacenamiento en la nube es fundamental, ya que los datos son uno de los activos más importantes de la empresa. Las plataformas en la nube ofrecen características para cifrado y monitoreo de accesos a las bases de datos.

Usar cifrado de datos, realizar auditorías de acceso y mantener un control estricto sobre las configuraciones de las bases de datos.

Protección de Infraestructura

Configuración segura de servidores, redes y dispositivos:

La infraestructura debe configurarse de manera segura desde el inicio para evitar vulnerabilidades que puedan ser explotadas. Esto incluye servidores, redes y dispositivos de red.

Aplicar configuraciones seguras en los servidores (por ejemplo, deshabilitar servicios innecesarios), proteger las redes mediante firewalls y asegurar los dispositivos mediante autenticación fuerte.

Protección de Infraestructura

Firewalls, redes privadas virtuales (VPN), segmentación de redes:

Los firewalls ayudan a controlar el tráfico de red no deseado, mientras que las VPNs permiten conexiones seguras y cifradas a través de redes no confiables. La segmentación de redes ayuda a reducir la superficie de ataque.

Implementar firewalls de próxima generación, usar VPNs para conexiones externas y dividir la red en segmentos para limitar el acceso entre diferentes áreas de la red.

Protección de Infraestructura

Control de accesos y autenticación de múltiples factores:

Es fundamental controlar quién tiene acceso a la red y los sistemas mediante la autenticación multifactor (MFA), lo que proporciona una capa adicional de seguridad más allá de las contraseñas.

Utilizar MFA en todos los puntos de acceso sensibles y configurar sistemas de control de acceso adecuados para cada nivel de privilegio.

Seguridad en el Desarrollo Web

Seguridad en el desarrollo: buenas prácticas de codificación segura (OWASP):

La seguridad debe ser una prioridad desde la fase de desarrollo de aplicaciones web. El proyecto OWASP (Open Web Application Security Project) proporciona directrices y estándares para la codificación segura.

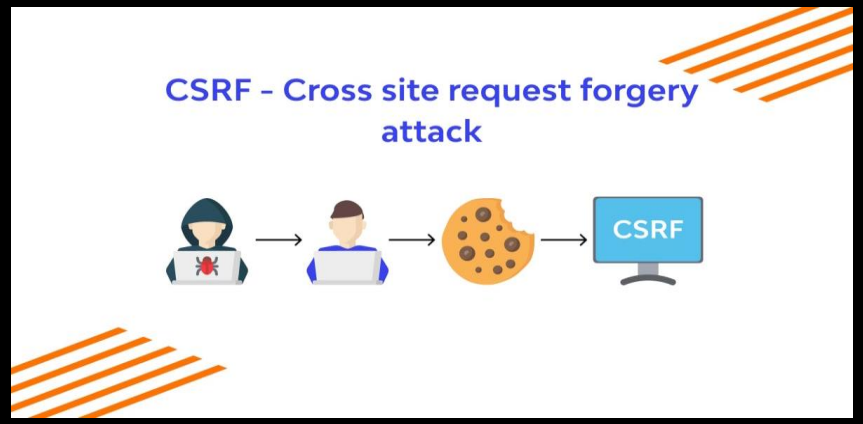
Aplicar las mejores prácticas para prevenir vulnerabilidades como las que se listan en el OWASP Top 10, como inyecciones SQL y XSS.

Seguridad en el Desarrollo Web

Protección contra vulnerabilidades comunes: inyecciones SQL, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF):

Las vulnerabilidades como las inyecciones SQL, XSS y CSRF son comunes en las aplicaciones web y pueden ser explotadas por atacantes para obtener acceso no autorizado o modificar datos sensibles.

Validar y sanear todas las entradas de usuarios, utilizar parámetros preparados en las consultas SQL, y aplicar técnicas de protección como tokens CSRF para evitar ataques.



Seguridad en el Desarrollo Web

Monitoreo y parches de seguridad en aplicaciones web:

Las aplicaciones web deben ser monitoreadas de manera continua para detectar posibles vulnerabilidades o ataques en tiempo real. Además, los parches de seguridad deben aplicarse regularmente para corregir fallos de seguridad conocidos.

Utilizar herramientas de monitoreo y aplicar actualizaciones de seguridad de manera proactiva para reducir riesgos.

Respuestas ante Incidentes de Ciberseguridad

Identificación, notificación y respuesta ante un ataque cibernético:

Detectar los primeros signos de un ataque cibernético es crucial para mitigar los daños. Contar con un proceso claro de notificación y respuesta asegura una reacción rápida y eficiente.

Implementar sistemas de detección de intrusiones, notificar a los responsables de TI inmediatamente y seguir un protocolo de respuesta ante incidentes.

Respuestas ante Incidentes de Ciberseguridad

Protocolos de recuperación ante desastres:

Los protocolos de recuperación ante desastres son esenciales para asegurar la disponibilidad continua de los servicios en caso de un incidente grave. Esto incluye planes detallados de restauración de datos y servicios.

Tener copias de seguridad regulares, realizar pruebas de recuperación y documentar un plan claro de contingencia.

Respuestas ante Incidentes de Ciberseguridad

Plan de contingencia para la restauración de servicios en la nube:

Los servicios en la nube deben contar con planes de contingencia para restaurar la disponibilidad de los mismos en caso de fallos o ataques.

Implementar estrategias de alta disponibilidad y redundancia, así como crear procedimientos de restauración rápida ante incidentes que afecten a los servicios en la nube.

Recursos y Soporte

Si tienes alguna pregunta o necesitas más información, estamos aquí para ayudarte.

- **Soporte de TI:** juanma.herrera.mer@gmail.com
- **Documentos adicionales: Accede a guías y recursos de ciberseguridad aquí: Enlace a la intranet de seguridad**

¡Gracias por vuestra atención!

Espero que os haya resultado y ameno y útil