TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE TLAXIACO

INVESTIGACION.

SEGURIDAD Y VIRTUALIZACION

CARRERA:

INGENIERIA EN SISTEMAS COMPUTACIONALES

GRUPO: 7US

PRESENTA:

RUFINO MENDOZA VAZQUEZ - 21620198

ANA MICHEL LEÓN LEÓN - 21620112

ROSA SALAZAR DOROTEO - 18620216

FERNANDA RUIZ HERAS - 21520151

DOCENTE

ING. EDWARD OSORIO SALINA

Tlaxiaco, Oax., 30 de Agosto del 2024.

"Educación, ciencia y tecnología, progreso día con día"®

Contenido

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial: la información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo. La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información.

Precisamente la reducción o eliminación de riesgos asociado a una cierta información es el objeto de la seguridad de la información y la seguridad informática. Más concretamente, la seguridad de la información tiene como objeto los sistemas el acceso, uso, divulgación, interrupción o destrucción no autorizada de información

Conceptos:

1. Contraseña

Una contraseña es una secuencia de caracteres que se utiliza para autenticar la identidad de un usuario y permitirle acceso a un sistema, aplicación, o servicio. Las contraseñas son una forma básica de seguridad y deben ser lo suficientemente complejas para prevenir su adivinación o ataques de fuerza bruta. Generalmente, las contraseñas deben combinar letras, números y caracteres especiales para incrementar su robustez. (Julián Pérez Porto, 2018)

2. Certificado digital

Un certificado digital es un documento electrónico emitido por una autoridad de certificación (CA) que vincula la identidad de una persona, organización, o dispositivo con una clave pública. El certificado incluye información como el nombre del propietario, la clave pública, la entidad emisora y la fecha de

expiración. Los certificados digitales son fundamentales para asegurar la comunicación en redes, especialmente en protocolos como HTTPS, donde garantizan que el intercambio de información sea seguro y provenga de una fuente confiable. (Fernandez, 2024)

3. Firma digital

Una firma digital es un mecanismo criptográfico que se utiliza para verificar la autenticidad e integridad de un mensaje, documento o archivo digital. Se basa en criptografía de clave pública y permite al receptor comprobar que el contenido no ha sido alterado y que proviene del remitente legítimo. La firma digital funciona mediante la creación de un hash (resumen criptográfico) del documento que se cifra con la clave privada del firmante. El receptor puede descifrarla usando la clave pública correspondiente y comparar el hash para validar la firma.

4. Cifrado simétrico

El cifrado simétrico es un método de cifrado donde la misma clave se utiliza tanto para cifrar como para descifrar la información. Es rápido y eficiente, lo que lo hace ideal para el cifrado de grandes volúmenes de datos. Sin embargo, la seguridad de este método depende del secreto de la clave, ya que, si un tercero obtiene la clave, puede descifrar la información. Ejemplos de algoritmos de cifrado simétrico son AES (Advanced Encryption Standard) y DES (Data Encryption Standard).

5. Cifrado asimétrico

El cifrado asimétrico utiliza un par de claves relacionadas: una clave pública y una clave privada. La clave pública se utiliza para cifrar los datos, y la clave privada, que debe mantenerse en secreto, se utiliza para descifrarlos. Este método permite a los usuarios intercambiar información de forma segura sin necesidad de compartir una clave secreta. El cifrado asimétrico es fundamental en protocolos de seguridad como SSL/TLS y es usado en firmas digitales. Un ejemplo común de cifrado asimétrico es el algoritmo RSA.

6. Hash

Un hash es el resultado de aplicar una función hash a un conjunto de datos. Una función hash toma una entrada (o "mensaje") y produce una cadena de caracteres de longitud fija que representa de manera única los datos originales. Los hashes son determinísticos, es decir, la misma entrada siempre producirá el mismo hash. Sin embargo, cualquier pequeño cambio en la entrada generará un hash completamente diferente. Los hashes se utilizan en varias áreas de la informática, como en la verificación de la integridad de datos, en el almacenamiento seguro de contraseñas, y en firmas digitales. Ejemplos de funciones hash incluyen SHA-256 y MD5.

7. Encriptación

La encriptación es el proceso de convertir información legible (texto claro) en un formato codificado (texto cifrado) que solo puede ser leído o decodificado por alguien que tenga la clave de descifrado correspondiente. Este proceso protege la confidencialidad de los datos, asegurando que solo las personas autorizadas puedan acceder a la información. Existen dos tipos principales de encriptación: simétrica y asimétrica. (cloudflare, s.f.)

Algoritmos de cifrado:

AES (Advanced Encryption Standard)

AES es un estándar de cifrado simétrico que fue establecido por el Instituto Nacional de Estándares y Tecnología (NIST) de los EE.UU. en 2001. AES se basa en el algoritmo Rijndael, desarrollado por los criptógrafos. Se utiliza ampliamente en aplicaciones de software y hardware para asegurar datos confidenciales.

Características:

Longitud de clave: AES soporta tres tamaños de clave: 128, 192 y 256 bits. Cuanto más larga sea la clave, más segura será la encriptación, pero también requerirá más recursos de procesamiento.

Bloque de datos: AES opera en bloques de 128 bits, lo que significa que los datos se procesan en bloques de este tamaño.

2. RSA (Rivest-Shamir-Adleman)

RSA es un algoritmo de cifrado asimétrico que fue inventado en 1977 por Ron Rivest, Adi Shamir, y Leonard Adleman. Es uno de los primeros algoritmos de cifrado de clave pública y sigue siendo uno de los más utilizados hoy en día.

Características:

Clave pública y privada: RSA utiliza un par de claves: una clave pública para cifrar los datos y una clave privada para descifrarlos. La seguridad del algoritmo se basa en la dificultad de factorizar números grandes en sus factores primos.

Longitud de clave: Las longitudes de clave comunes en RSA son 2048 o 4096 bits. Una clave más larga ofrece mayor seguridad, pero también requiere más poder de procesamiento. (Gitlan, 2024)

SHA-256 (Secure Hash Algorithm 256-bit)

SHA-256 es parte de la familia de funciones hash SHA-2, desarrollada por la Agencia de Seguridad Nacional de EE.UU. (NSA) y publicada por NIST en 2001. Es una función hash criptográfica que produce un valor hash de 256 bits (32 bytes) a partir de una entrada de cualquier longitud.

Características:

Determinismo: La misma entrada siempre produce el mismo hash.

Longitud fija del hash: Independientemente del tamaño de la entrada, el hash resultante tiene siempre 256 bits.

Estándares de cifrado:

1. SSL (Secure Sockets Layer)

Descripción: SSL es un protocolo criptográfico diseñado para proporcionar seguridad en las comunicaciones a través de redes como Internet. Fue desarrollado por Netscape Communications en 1994 y es el precursor de TLS (Transport Layer Security). SSL permite la autenticación del servidor (y opcionalmente del cliente) y el establecimiento de una conexión cifrada entre dos puntos.

Características:

Autenticación: SSL permite que un cliente verifique la identidad de un servidor mediante el uso de certificados digitales, garantizando que la comunicación se realiza con la entidad correcta.

Cifrado: Después de la autenticación, SSL negocia una clave de sesión entre el cliente y el servidor, que se utiliza para cifrar la comunicación. Esto protege los datos transmitidos contra la interceptación y el espionaje.

2. TLS (Transport Layer Security)

Descripción: TLS es el sucesor de SSL y fue desarrollado por la IETF (Internet Engineering Task Force) como un estándar más seguro y eficiente para la seguridad en las comunicaciones a través de redes. La primera versión de TLS fue publicada en 1999 como un reemplazo directo de SSL, y desde entonces se han lanzado varias versiones mejoradas para abordar vulnerabilidades y actualizar los estándares de seguridad.

Características:

Autenticación: Como SSL, TLS permite la autenticación de servidores y, opcionalmente, de clientes, utilizando certificados digitales emitidos por una Autoridad de Certificación (CA).

Cifrado: TLS utiliza algoritmos de cifrado modernos y seguros, como AES, para cifrar los datos transmitidos entre el cliente y el servidor, protegiendo la confidencialidad de la información.

Protocolos de seguridad:

1. HTTPS

HTTPS es la versión segura del protocolo HTTP, que se utiliza para la comunicación en la web. A través de HTTPS, los datos transmitidos entre el navegador web del usuario y el servidor se cifran utilizando SSL/TLS (Secure Sockets Layer/Transport Layer Security). Esto garantiza que la información intercambiada, como contraseñas, números de tarjetas de crédito y otros datos sensibles, esté protegida contra interceptaciones y manipulaciones por parte de terceros.

Características:

Cifrado: La principal característica de HTTPS es el cifrado de los datos transmitidos, lo que impide que actores malintencionados puedan leer o alterar la información mientras se transmite.

Autenticación: HTTPS asegura que el servidor con el que el usuario se está comunicando es legítimo y no un impostor, gracias a los certificados digitales emitidos por autoridades de certificación (CA).

2. SFTP

SFTP es un protocolo de red que permite la transferencia segura de archivos entre un cliente y un servidor. Funciona sobre el protocolo SSH (Secure Shell), proporcionando un canal seguro para la transferencia de datos y la gestión de archivos en una red. A diferencia de FTP, que transmite datos en texto plano, SFTP cifra tanto los comandos como los datos, asegurando que no puedan ser interceptados o alterados durante la transmisión.

Características:

Cifrado: SFTP utiliza cifrado para proteger los datos durante la transferencia, asegurando que la información no pueda ser leída ni modificada por terceros.

Autenticación: SFTP soporta múltiples métodos de autenticación, incluyendo contraseñas y claves públicas, lo que añade una capa adicional de seguridad.

Integridad de datos: El protocolo asegura que los datos transferidos no sean alterados durante el tránsito.

3. SSH (Secure Shell)

SSH es un protocolo de red utilizado para acceder de manera segura a un dispositivo remoto, generalmente un servidor, sobre una red no segura. SSH permite ejecutar comandos, transferir archivos y administrar remotamente sistemas de manera segura. Fue desarrollado como una alternativa segura a protocolos como Telnet y rlogin, que transmiten la información en texto plano, lo que los hace vulnerables a intercepciones.

Características:

Cifrado: SSH cifra todo el tráfico entre el cliente y el servidor, incluyendo las credenciales de acceso, lo que impide la interceptación por parte de atacantes.

Autenticación: SSH soporta autenticación mediante contraseñas, claves públicas, y otros métodos, lo que lo hace versátil y seguro.

Conclusión:

La seguridad de la información no se limita a la protección contra amenazas externas, sino que también debe abordar riesgos internos. Las políticas y prácticas de seguridad deben ser integrales, abarcando desde la encriptación de datos y el uso de contraseñas seguras hasta la implementación de controles de acceso. Las amenazas están en constante evolución, con ciberdelincuentes que desarrollan técnicas más sofisticadas para vulnerar sistemas y redes. Los riesgos incluyen ataques de malware, phishing, y la exposición de datos sensibles. La seguridad debe ser dinámica, adaptándose a nuevas amenazas y vulnerabilidades a medida que surgen, y así poder ofrecer seguridad a los usuarios.

BIBLIOGRAFIA:

cloudflare. (s.f.). Obtenido de https://www.cloudflare.com/es-es/learning/ssl/what-is-encryption/

Fernandez, Y. (22 de Marzo de 2024). *xataka*. Obtenido de https://www.xataka.com/basics/certificado-digital-que-que-tipos-hay-como-solicitarlo-activarlo

Gitlan, D. (2 de febrero de 2024). *SSL Dragon*. Obtenido de https://www.ssldragon.com/es/blog/rsa-aes-cifrado/

Julián Pérez Porto, M. M. (13 de diciembre de 2018). *Definición.DE*. Obtenido de https://definicion.de/contrasena/