Amenazas en Ciberseguridad. TOP 10

Descripción

El Top 10 DE LAS AMENAZAS EN CIBERSEGURIDAD

Debido a la transformación digital, muchas empresas están implantando aplicaciones web. Debido a esto, es importante conocer las medidas de seguridad que se pueden implementar, tanto si desarrollamos una nueva aplicación o usamos una que esté ya en funcionando. Casi todas las vulnerabilidades pueden ser aplicadas sin importar el tamaño de la empresa. Para ello te vamos a explicar como son las 10 amenazas en Ciberseguridad más comunes.

El 'Proyecto abierto de seguridad en aplicaciones web' (*Open Web Application Security Project*, OWASP por su acrónimo) es una comunidad que, a través de sus colaboradores, los cuales les ceden datos de más de 500.000 aplicaciones web, emite un documento llamado OWASP Top 10 que recopila las 10 vulnerabilidades web más usuales que se han identificado hasta 2021.

Analizamos las primeras 5 vulnerabilidades. Pero antes debes saber que una vulnerabilidad es una debilidad que puede poner en peligro toda una red y por eso deben existir los expertos en **ciberseguridad** para aliviar las amenazas y sus correspondientes tipos de **vulnerabilidades.**

La **vulnerabilidad** es la incapacidad de resistencia cuando se presenta un fenómeno amenazante, o la incapacidad para reponerse después de que ha ocurrido un desastre. Por ejemplo, un teléfono móvil sin contraseña es más vulnerable al robo de datos en caso de extravío. Este caso parece muy obvio, pero existen muchos tipos de vulnerabilidades que debes conocer para prevenir o reforzar esas amenazas.

¿Cuáles son esas vulnerabilidades y cómo me pueden afectar?

1. Pérdida del control de acceso (*Broken Access Control*)

El control de acceso permite cumplir una política de permisos y roles, es decir, que un usuario pueda acceder a determinados lugares. Estas limitaciones impiden que los usuarios puedan actuar fuera de los permisos que poseen y a su vez, llevar un control de los usuarios que acceden a cada recurso en el sistema.

La vulnerabilidad *Broken Access Control* permite que un usuario sin privilegios pueda acceder a un recurso al que no tendría que acceder, constituyendo una brecha en el aspecto de la Confidencialidad en un sistema.

IMPACTO:

- Un ciberdelicuente podría actuar en el sistema con permisos de usuario o administrador, pudiendo alterar la configuración del sistema.
- Acceso a registros, directorios o archivos confidenciales para su posterior posible divulgación, lo que constituiría una vulneración de la confidencialidad de los datos, con todas las implicaciones

que eso supone. (perdida de prestigio, competitividad, exposición de datos de carácter personal con las correspondientes sanciones, etc.

2. Fallos criptográficos (*Cryptographic Failures*)

La criptografía ayuda a mantener la confidencialidad de los datos en un sistema mediante el encriptado de la información y su cifrado mediante algoritmos criptográficos.

Los datos sensibles que deben estar cifrados son

- Credenciales de acceso
- Datos bancarios
- Información confidencial de la empresa, proyectos, estrategias, diseños etc..

Además de que la ley lo exija, el que un ciberdelincuente se pueda hacer con estos datos sensibles puede resultar crítico para la empresa.

Es por esto que, para proteger la confidencialidad de estos datos, hemos de aplicarles un cifrado con algoritmos y protocolos estándares y robustos.

IMPACTO:

Exposición de datos sensibles a un ciberdelincuente (datos personales, críticos o estratégicos para la empresa; credenciales…).

3. Inyección (*Injection*)

Esto sucede cuando un ciberdelincuente puede enviar datos dañinos a un intérprete. Muy común en formularios web mal diseñados.

El antídoto para este tipo de ataques, es tener APIs seguras y controles de verificación a la hora de introducir los datos.

IMPACTO:

Exposición y posible modificación de datos sensibles por parte de un ciberdelincuente.

- Bajo ciertas circunstancias podría permitir al ciberdelincuente tomar el control del servidor.

4. Diseño inseguro (*Insecure Desing*)

Una de las mayores vulnerabilidades de las aplicaciones web vienen dadas por sus errores de diseño. Normalmente, esto ocurre cuando no se ha tomado en cuenta la seguridad a la hora de diseñar el producto.

Este año se ha incluido esta nueva categoría debido a la gran cantidad de aplicaciones que no cumplen los estándares mínimos de seguridad.

IMPACTO:

- Exposición y posible modificación de datos por un ciberdelincuente.
- Acceso al servidor/aplicación por parte de un ciberdelincuente con permisos de administrador o usuario.

5. Phishing

El Phishing es una técnica de engaño cibernético utilizada por los delincuentes informáticos para obtener información confidencial, como nombres de usuario, contraseñas, información bancaria y otra información personal sensible. Estos delincuentes envían correos electrónicos o mensajes de texto falsificados que parecen ser de una fuente confiable, como un banco o un sitio web de comercio electrónico, y solicitan que el destinatario revele su información personal o haga clic en un enlace que lleva a un sitio web falso.

IMPACTO:

1. Robo de identidad: Los delincuentes pueden usar la información obtenida para acceder a cuentas bancarias, tarjetas de crédito y otros tipos de cuentas en línea, y utilizarlas para cometer fraudes y robos financieros.
2. Instalación de malware: Al hacer clic en un enlace falso en un correo electrónico de phishing, es posible que el destinatario descargue malware en su computadora o dispositivo móvil.
3. Pérdida de dinero: Si los delincuentes tienen acceso a cuentas bancarias o tarjetas de crédito, pueden transferir dinero y causar pérdidas financieras significativas.
4. Daño a la reputación: La información personal obtenida a través del phishing puede ser utilizada para cometer fraudes y otros delitos, lo que puede dañar la reputación y la credibilidad de la víctima.

6. Ataques de malware:

Estos incluyen virus, troyanos, spyware y otros tipos de software malicioso que pueden infectar un dispositivo y permitir a los atacantes acceder a información confidencial.

Los ataques de malware son una forma común y efectiva utilizada por los delincuentes cibernéticos para acceder a sistemas y dispositivos y causar daño o robar información. Algunos de los tipos de ataques de malware incluyen:

1. Virus: Es un tipo de malware que se propaga a través de archivos y programas infectados y puede dañar el sistema operativo, los archivos y los programas.
2. Gusanos: Son similares a los virus, pero se propagan a través de redes y pueden replicarse a sí

mismos sin la necesidad de un archivo o programa infectado.
3. Adware: Es un tipo de malware que muestra anuncios no deseados en el dispositivo de la víctima y puede rastrear y recopilar información sobre la navegación en línea de la víctima.
4. Spyware: Es un tipo de malware que se instala en el dispositivo de la víctima sin su conocimiento y puede rastrear y recopilar información confidencial, como nombres de usuario y contraseñas.
5. Ransomware: Es un tipo de malware que cifra los archivos y solicita un rescate a cambio de la descifratura. Estos ataques pueden ser particularmente graves y costosos para las organizaciones y los individuos afectados.
6. Trojano: Es un tipo de malware que se disfraza como un archivo o programa legítimo pero tiene una función maliciosa oculta, como el acceso remoto no autorizado a un dispositivo.

7. Ataques DDoS (Denegación de servicio distribuido)

Un ataque DDoS (Denegación de servicio distribuido) es una técnica utilizada por los atacantes para hacer que un servicio en línea o una red se vuelva inaccesible para los usuarios legítimos. Esto se logra enviando una cantidad masiva de solicitudes falsas al servidor o red, lo que los sobrecarga y hace que se vuelvan inaccesibles.

En un ataque DDoS, los atacantes emplean una red de dispositivos comprometidos, conocidos como bots o zombies, para enviar una cantidad masiva de solicitudes al objetivo. Estos dispositivos pueden ser computadoras, servidores o dispositivos IoT que han sido comprometidos sin el conocimiento de sus propietarios.

IMPACTO:

Las consecuencias de un ataque DDoS pueden ser graves, especialmente para las organizaciones que dependen de sus servicios en línea para operar. Los ataques DDoS pueden interrumpir los servicios y causar pérdidas financieras directas, así como dañar la reputación de la organización. Además, los ataques DDoS a menudo son utilizados como una táctica de distracción para ocultar otros ataques más graves, como la exfiltración de datos o la introducción de malware.

Por lo tanto, es importante tomar medidas para protegerse contra los ataques DDoS, como utilizar soluciones de mitigación DDoS, monitorear el tráfico de red y tener planes de respaldo en caso de un ataque. Además, es fundamental estar al tanto de las últimas técnicas y tendencias en ataques DDoS para estar preparado y responder adecuadamente.

8. Robos de identidad

El robo de identidad es un delito cibernético en el que un atacante obtiene y utiliza información confidencial de una persona sin su autorización con el fin de cometer fraude o realizar actividades ilegales en su nombre.

Esta información puede incluir nombres completos, fechas de nacimiento, números de seguro social, información financiera y de tarjetas de crédito, direcciones de correo electrónico y contraseñas. Esta información puede ser obtenida a través de phishing, ataques de malware, robo de documentosfísicos, o simplemente a través de la recopilación de datos públicos.

IMPACTO:

Las consecuencias del robo de identidad pueden ser graves y duraderas. Los delincuentes pueden utilizar la información robada para cometer fraude y obtener préstamos o créditos a nombre de la víctima. También pueden usar la información para cometer fraude con tarjetas de crédito y otros servicios financieros. Además, el robo de identidad puede dañar la reputación de la víctima y ser costoso y tardado para resolver.

Por lo tanto, es importante tomar medidas para proteger la información personal y ser consciente de las señales de robo de identidad. Estas medidas incluyen el uso de contraseñas seguras y únicas, la monitorización de las transacciones financieras y la verificación periódica de los informes de crédito. También es importante estar atento a los correos electrónicos y llamadas sospechosas y no compartir información confidencial con terceros no confiables.

9. Ransomware

El ransomware es un tipo de malware que cifra los archivos del usuario y los hace inaccesibles hasta que se paga un rescate. Los atacantes suelen exigir un pago en criptomonedas, como Bitcoin, para proporcionar la clave de descifrado necesaria para recuperar los archivos.

El ransomware se propaga a través de correos electrónicos de phishing, descargas de software infectado y vulnerabilidades de seguridad explotadas. Una vez instalado en un sistema, el ransomware comienza a cifrar los archivos y muestra una demanda de rescate que incluye instrucciones sobre cómo realizar el pago.

IMPACTO

Las consecuencias de un ataque de ransomware pueden ser graves, especialmente para las organizaciones. Los archivos cifrados pueden ser irrecuperables si no se posee una copia de seguridad o si los atacantes no proporcionan la clave de descifrado. Además, los ataques de ransomware pueden interrumpir los servicios y causar pérdidas financieras directas, así como dañar la reputación de la organización.

Por lo tanto, es importante tomar medidas para protegerse contra los ataques de ransomware, como mantener actualizados los sistemas y software, utilizar soluciones de seguridad y realizar copias de seguridad regulares. También es importante estar atento a las señales de un posible ataque de ransomware, como correos electrónicos sospechosos y comportamientos inusuales en los archivos y sistemas. En caso de un ataque de ransomware, es importante no pagar el rescate y contactar a expertos en seguridad cibernética para obtener ayuda.

10. Ataques de supuesto “dilema del prisionero”

Los ataques de “dilema del prisionero” en ciberseguridad se refieren a situaciones en las que dos o más partes compiten o colaboran en una acción que puede tener consecuencias negativas para ambas. Este término se aplica a menudo a la seguridad cibernética porque muchos ataques requieren la cooperación de varias partes para tener éxito.

En un ataque de “dilema del prisionero”, cada parte trata de obtener una ventaja sobre la otra, a menudo a costa de la seguridad de todas las partes involucradas. Por ejemplo, un atacante puede tratar de comprometer un sistema para obtener acceso a información confidencial, mientras que la organización trata de proteger sus datos y mantener su seguridad.

IMPACTO

Las consecuencias de un ataque de “dilema del prisionero” pueden ser graves y amplias, ya que cualquiera de las partes involucradas puede sufrir daños significativos a su seguridad, privacidad y reputación. Además, los ataques de “dilema del prisionero” pueden tener un impacto en la economía y la sociedad en general, especialmente si se trata de información confidencial o crítica.

Por lo tanto, es importante para las organizaciones y los usuarios individuales tomar medidas para protegerse contra los ataques de “dilema del prisionero”, como mantener actualizados los sistemas y software, utilizar soluciones de seguridad, y estar atentos a las señales de posibles ataques. También es importante colaborar con otros actores en la industria y la sociedad para establecer normas y prácticas de seguridad sólidas y efectivas que reduzcan la probabilidad de ataques de “dilema del prisionero”.

Es importante que los usuarios tomen medidas para protegerse contra estas amenazas en ciberseguridad, como utilizar contraseñas seguras, mantener software y sistemas actualizados y ser cautelosos con los correos electrónicos y sitios web sospechosos. Al estar informados sobre estas amenazas y tomar medidas para protegerse, los usuarios pueden minimizar el riesgo de sufrir un ataque y mantener sus información y sistemas seguros.