IFCT0109. SEGURIDAD INFORMÁTICA

MF0490_3 GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

ANEXO

DESCRIPCIÓN DE LOS CONCEPTOS BÁSICOS DE LA CIBERSEGURIDAD

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. **DESCRIPCIÓN DE AMENAZAS, ATAQUES Y MITIGACIONES BÁSICOS DE CIBERSEGURIDAD**
2. DESCRIPCIÓN DE LOS CONCEPTOS DE CRIPTOGRAFÍA
3. DESCRIPCIÓN DE LA AUTENTICACIÓN Y LA AUTORIZACIÓN EN CIBERSEGURIDAD
4. DESCRIBIR LAS AMENAZAS DE RED Y LAS MITIGACIONES
5. DESCRIPCIÓN DE LAS AMENAZAS BASADAS EN DISPOSITIVOS Y LOS CONTROLES DE SEGURIDAD
6. DESCRIPCIÓN DE AMENAZAS BASADAS EN APLICACIONES Y CÓMO PROTEGERSE FRENTE A ELLAS

Descripción de los conceptos básicos de la ciberseguridad

Conocer los aspectos fundamentales de la ciberseguridad es un primer paso para protegerse contra las ciberamenazas. En esta ruta de aprendizaje, aprenderá los conceptos de la ciberseguridad y formas de protegerse usted mismo y su negocio frente a los ciberataques.

DESCRIPCIÓN DE AMENAZAS, ATAQUES Y MITIGACIONES BÁSICOS DE CIBERSEGURIDAD

Introducción

En la actualidad, **estamos inundados de informes de ciberataques y sus ramificaciones**. Escuchamos hablar de ataques a cadenas de suministro globales que tienen consecuencias económicas importantes. Casi de forma rutinaria, observamos que los ciberdelincuentes han robado la información personal de millones de consumidores a través de plataformas que se usan a diario. A veces, incluso se habla de servicios sanitarios y gubernamentales vitales que sufren bloqueos y extorsiones a cambio de un rescate.

Los ciberataques evolucionan continuamente. **La ciberseguridad es un campo importante, grande y en crecimiento** en un mundo en el que las empresas y las instituciones compiten por trasladar y mantener sus negocios en línea.

A lo largo de este módulo, conocerá los conceptos básicos sobre la ciberseguridad.
Al término de este módulo, sabrá hacer lo siguiente:

- *Describir el panorama básico de amenazas*
- *Describir los diferentes tipos de malware*
- *Describir estrategias básicas de mitigación.*

Describir qué es la ciberseguridad

Las personas, las organizaciones y los gobiernos son víctimas habituales de los ciberataques. Constantemente escuchamos referencias a conceptos como ciberseguridad, ciberataques, ciberdelincuentes, etc.

Todo esto puede parecer abrumador y difícil de entender. Para protegerse a sí mismo y a los usuarios que le rodean, deberá tener una comprensión básica de estos conceptos.

¿Qué es un ciberataque?

Un ciberataque se define normalmente como un intento de obtener acceso no autorizado a un equipo o sistema informático para causar daños. Pero solo pensar en equipos o sistemas informáticos, en el sentido tradicional, es una limitación. La realidad es que **un ciberataque puede producirse en casi cualquier dispositivo digital** moderno. **El impacto puede abarcar desde molestias a un individuo hasta una alteración económica y social en todo el mundo**.

Un atacante puede usar personas, equipos, teléfonos, aplicaciones, mensajes y procesos del sistema para llevar a cabo un ataque. Los individuos, las organizaciones, las instituciones y los gobiernos pueden ser víctimas de un ataque.

Describir qué es la ciberseguridad

Estos atacantes podrían hacer lo siguiente:

- *Bloquear datos y procesos y exigir un rescate.*
- *Quitar información vital para causar daños graves.*
- *Robar información.*
- *Exponer públicamente información privada.*
- *Detener la ejecución de procesos y sistemas empresariales vitales para provocar interrupciones y errores de funcionamiento.*

Con los ciberataques en constante evolución, es importante recordar que los atacantes no necesitan solo un equipo para llevar a cabo un ataque. Además, la naturaleza y el ámbito de los ataques pueden variar significativamente.

Cualquier dispositivo o entidad conectado digitalmente se puede usar como parte de un ataque o estar sujeto a un ataque.

Describir qué es la ciberseguridad

¿Qué es un ciberdelincuente?

Un ciberdelincuente es cualquier persona que lleva a cabo un ciberataque. Los ciberdelincuentes **pueden ser:**

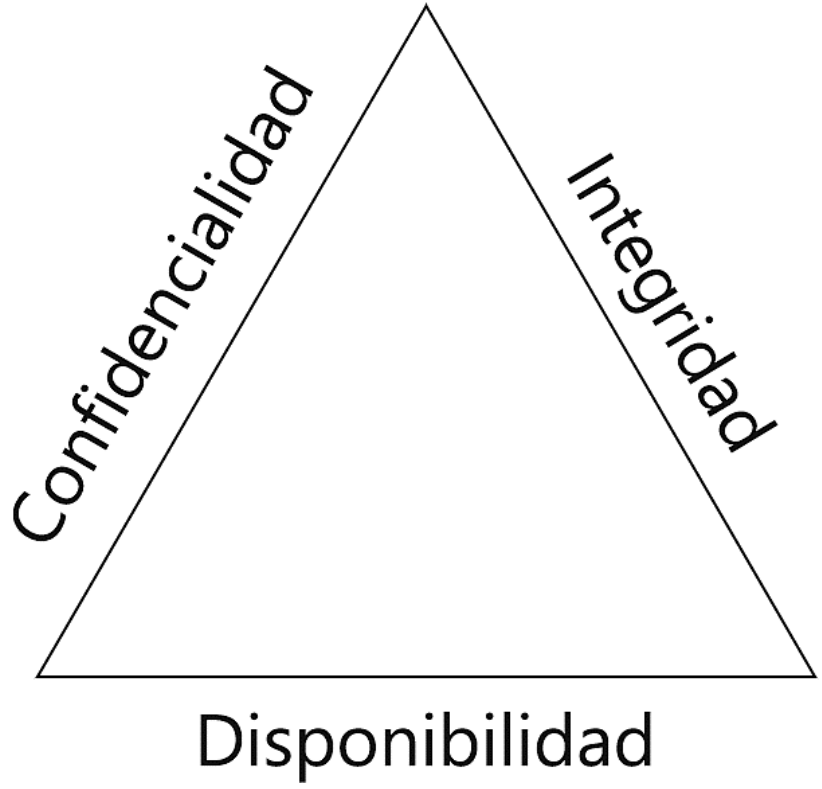
- *Una sola persona o un grupo de personas.*
- *Una organización para contratación.*
- *Una entidad gubernamental.*

Los ciberdelincuentes se pueden encontrar en cualquier lugar, incluso dentro de una organización o institución, para causar daños desde dentro.

Describir qué es la ciberseguridad

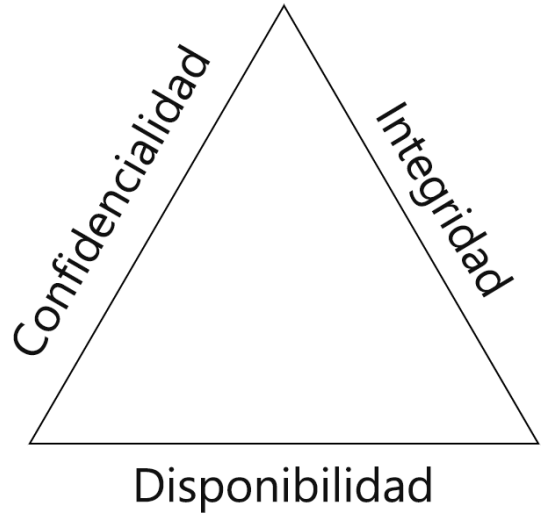
¿Qué es la ciberseguridad?

La ciberseguridad hace referencia a tecnologías, procesos y aprendizaje que ayudan a proteger los sistemas, las redes, los programas y los datos frente a ciberataques, daños y accesos no autorizados. La ciberseguridad le *permite lograr los siguientes objetivos*:



Describir qué es la ciberseguridad

¿Qué es la ciberseguridad?



- ***Confidencialidad****: la información solo debe ser visible para las personas correctas.*
- ***Integridad****: la información solo deben cambiarla las personas o los procesos adecuados.*
- ***Disponibilidad****: la información debe ser visible y accesible siempre que sea necesario.*

Esto se conoce normalmente como **el modelo de *confidencialidad, integridad y disponibilidad* (CIA)** en el contexto de la ciberseguridad.

En el resto de este módulo, conocerá los tipos de ataques que usan los ciberdelincuentes para perturbar estos objetivos y causar daños. También verá algunas estrategias básicas de mitigación de amenazas.

Describir el panorama de amenazas

Ya ha obtenido información sobre los ciberataques, los ciberdelincuentes y la ciberseguridad. Pero también deberá conocer los recursos que los ciberdelincuentes pueden usar para llevar a cabo ataques y lograr sus objetivos. Para ello, aprenderá conceptos como el panorama de amenazas, los vectores de ataque, las infracciones de seguridad, etc.

¿Qué es el panorama de amenazas?

Independientemente de si una organización es grande o pequeña, **el panorama digital completo con el que interactúa representa un punto de entrada para un ciberataque.** Estas pueden incluir:

- *Cuentas de correo*
- *Cuentas de redes sociales*
- *Dispositivos móviles*
- *La infraestructura tecnológica de la organización*
- *Servicios en la nube*
- *Personas*

Colectivamente**, se conoce como el panorama de amenazas**. Observe que el panorama de amenazas puede abarcar más que solo equipos y teléfonos móviles. Puede incluir cualquier elemento cuya titularidad o administración recaiga o no en una organización. Como aprenderá a continuación, los delincuentes usarán cualquier recurso que puedan para montar y llevar a cabo un ataque.

Describir el panorama de amenazas

¿Qué son los vectores de ataque?

Un vector de ataque es un punto de entrada o una ruta para que un atacante obtenga acceso a un sistema.

El correo electrónico quizá sea el vector de ataque más común.

Los ciberdelincuentes enviarán correos electrónicos aparentemente legítimos que provocarán que los usuarios realicen alguna acción. Esto puede incluir la descarga de un archivo o la selección de un vínculo que pondrá en peligro su dispositivo.

Otro vector de ataque común es **a través de redes inalámbricas**. Los agentes malintencionados suelen aprovechar las redes inalámbricas no seguras en aeropuertos o cafeterías, en busca de vulnerabilidades en los dispositivos de los usuarios que acceden a la red inalámbrica**.**

Describir el panorama de amenazas

¿Qué son los vectores de ataque?

La supervisión de cuentas de redes sociales o incluso el acceso a dispositivos que no están seguros son otras rutas de uso común para los ciberataques.

Sin embargo, debe saber que los atacantes no solo se basan en estos vectores**. Pueden usar una variedad de vectores de ataque** menos obvios.

Estos son algunos ejemplos:

- **Medios extraíbles**. Un atacante puede usar medios como unidades USB, cables inteligentes, tarjetas de almacenamiento y mucho más para poner en peligro un dispositivo. Por ejemplo, los atacantes pueden cargar código malintencionado en dispositivos USB que posteriormente se proporcionan a los usuarios como un obsequio gratuito o se dejan en espacios públicos para que alguien los encuentre. Cuando se conectan, se provoca el daño.

Describir el panorama de amenazas

¿Qué son los vectores de ataque?

- **Explorador**. Los atacantes pueden usar sitios web malintencionados o extensiones del navegador para que los usuarios descarguen software malintencionado en sus dispositivos o cambien la configuración del explorador de un usuario. A continuación, el dispositivo puede verse comprometido, lo que proporciona un punto de entrada al sistema o a la red más amplios.
- **Servicios en la nube**. Las organizaciones dependen cada vez más de los servicios en la nube para el negocio y los procesos diarios. Los atacantes pueden poner en peligro servicios o recursos mal protegidos en la nube. Por ejemplo, un atacante podría poner en peligro una cuenta en un servicio en la nube y obtener el control de todos los recursos o servicios accesibles para esa cuenta. También podrían obtener acceso a otra cuenta incluso con más permisos.

Describir el panorama de amenazas

¿Qué son los vectores de ataque?

- **Agentes internos**. Los empleados de una organización pueden actuar como un vector de ataque en un ciberataque, ya sea intencionadamente o no. Un empleado podría convertirse en la víctima de un ciberdelincuente que lo suplanta como una persona de autoridad para obtener acceso no autorizado a un sistema. Se trata de una forma de ataque de ingeniería social. En este escenario, el empleado actúa como un vector de ataque involuntario. Sin embargo, en algunos casos, un empleado con acceso autorizado puede usarlo para robar intencionadamente o causar daños.

Describir el panorama de amenazas

¿Qué son las infracciones de seguridad?

Cualquier ataque que da lugar a que alguien obtenga acceso no autorizado a dispositivos, servicios o redes se considera una infracción de seguridad. Imagine una infracción de seguridad como similar a un allanamiento en el que un intruso (atacante) logra entrar en un edificio (un dispositivo, una aplicación o una red).

Las infracciones de seguridad tienen diferentes formas, entre las que se incluyen las siguientes:

- **Ataques de ingeniería social**
- **Ataques del explorador**
- **Ataques a contraseñas**

Describir el panorama de amenazas

¿Qué son las infracciones de seguridad?

Ataques de ingeniería social

Es habitual pensar que las infracciones de seguridad aprovechan algún error o vulnerabilidad en un servicio tecnológico o en parte de un equipo. Del mismo modo, podría pensar que las infracciones de seguridad solo se producen debido a vulnerabilidades en la tecnología. Pero ese no es el caso. Los atacantes pueden usar ataques de ingeniería social para aprovecharse de los usuarios o manipularlos con la intención de concederles acceso no autorizado a un sistema.

En la ingeniería social, los ataques de suplantación se producen cuando un usuario no autorizado (el atacante) **pretende ganarse la confianza de un usuario autorizado al hacerse pasar por una persona de autoridad para acceder a un sistema a partir de alguna actividad fraudulenta**. Por ejemplo, un ciberdelincuente podría hacerse pasar por un ingeniero de soporte técnico para conseguir que un usuario revele su contraseña para acceder a los sistemas de una organización.

Describir el panorama de amenazas

¿Qué son las infracciones de seguridad?

Ataques del explorador

Ya sea en un escritorio, portátil o teléfono, **los exploradores son una herramienta de acceso importante para Internet. Las vulnerabilidades de seguridad de un explorador pueden tener un impacto significativo** debido a su generalización. Por ejemplo, suponga que un usuario está trabajando en un proyecto importante con una fecha límite inminente. Quiere averiguar cómo resolver un problema determinado para su proyecto. Encuentra un sitio web que cree que proporcionará una solución.

El sitio web pide al usuario que realice algunos cambios en la configuración del explorador para poder instalar un complemento. El usuario sigue las instrucciones del sitio web. Aunque no lo sabe, el explorador ahora está en peligro. Se trata de un ataque modificador del explorador, uno de los muchos tipos diferentes que usan los ciberdelincuentes. Un atacante ahora puede usar el explorador para robar información, supervisar el comportamiento del usuario o poner en peligro un dispositivo.

Describir el panorama de amenazas

¿Qué son las infracciones de seguridad?

Ataques a contraseñas

Un ataque de contraseña es cuando alguien intenta usar la autenticación de una cuenta protegida con contraseña para obtener acceso no autorizado a un dispositivo o sistema. Los atacantes suelen usar **software para acelerar el proceso de descifrar y adivinar contraseñas**. Por ejemplo, suponga que un atacante ha descubierto de algún modo el nombre de usuario de alguien para su cuenta profesional.

A continuación, el atacante intenta una gran cantidad de combinaciones de contraseñas posibles para acceder a la cuenta del usuario. La contraseña solo tiene que ser correcta una vez para que el atacante obtenga acceso. Esto se conoce como un ataque por fuerza bruta y es una de las muchas maneras en que un ciberdelincuente puede usar ataques de contraseña.

Describir el panorama de amenazas

¿Qué son las infracciones de datos?

Una infracción de datos es cuando un atacante logra acceder a los datos o controlarlos. Con el ejemplo del intruso, esto sería similar a esa persona que obtenía acceso a documentos vitales e información dentro del edificio o que los robaba:

Cuando un atacante logra cometer una infracción de seguridad, su objetivo serán los datos, porque representan información vital.

Una seguridad deficiente de los datos puede provocar que un atacante obtenga acceso a los datos y los controle. Esto **puede provocar consecuencias graves para la víctima**, ya sea una persona, una organización o incluso un gobierno. Esto se debe a que los datos de la víctima podrían ser objeto de abusos de muchas maneras. Por ejemplo, se pueden retener como rescate o usarse para causar daños financieros o a la reputación.

Descripción de malware

¿Ha escuchado hablar de términos como malware, virus y gusanos, entre otros?

Pero, ¿qué significan? ¿Un gusano es un virus? ¿Qué hace el malware exactamente? Estos son solo algunos de los conceptos básicos que aprenderá en esta unidad.

¿Qué es el malware?

El malware procede de la combinación de las palabras malintencionado y software. Es un fragmento de software que usan los ciberdelincuentes para infectar los sistemas y llevar a cabo acciones dañinas. Esto podría incluir el robo de datos o la interrupción del uso y los procesos normales.

El malware tiene dos componentes principales:

- *Mecanismo de propagación*
- *Carga*

¿Qué es un mecanismo de propagación?

La propagación **es la forma en que el malware se propaga entre uno o varios sistemas**. Estos son algunos ejemplos de técnicas de propagación comunes:

Descripción de malware

Virus

La mayoría de nosotros ya estamos familiarizados con este término. Pero ¿qué significa realmente? En primer lugar, vamos a pensar en los virus en términos no técnicos. En biología, por ejemplo, un virus entra en el cuerpo humano y, una vez dentro, puede propagarse y causar daños. **Los virus basados en la tecnología dependen de alguna forma de acceso, específicamente una acción del usuario, para entrar en un sistema.** Por ejemplo, un usuario podría descargar un archivo o conectar un dispositivo USB que contiene el virus que contamina el sistema. Esto es una infracción de seguridad.

Descripción de malware

Gusano

A diferencia de un virus, **un gusano no necesita ninguna acción del usuario para propagarse por los sistemas.** En su lugar, **un gusano causa daños al encontrar sistemas vulnerables de los que se puede aprovechar. Una vez dentro, el gusano se puede propagar a otros sistemas conectados.** Por ejemplo, un gusano podría infectar un dispositivo al aprovechar una vulnerabilidad en una aplicación que se ejecuta en él. A continuación, el gusano se puede propagar por otros dispositivos en la misma red y otras redes conectadas.

Troyano

Un ataque de caballo de Troya debe su nombre a la historia clásica, donde los soldados se escondían dentro de un caballo de madera que se ofrecía como un regalo a los troyanos. Cuando los troyanos llevaron el caballo de madera a su ciudad, los soldados salieron de su escondite y atacaron. En el contexto de la ciberseguridad**, un troyano es un tipo de malware que pretende ser un componente de software original.** Cuando un usuario instala el programa, puede pretender que funcione como se anuncia, pero **el programa también realiza de forma secreta acciones malintencionadas, como robar información.**

Descripción de malware

¿Qué es una carga?

La carga es la acción que realiza un fragmento de malware en un dispositivo o sistema infectado. Estos son algunos tipos comunes de carga:

- El **ransomware** es una carga **que bloquea sistemas o datos hasta que la víctima paga un rescate**. Supongamos que hay una vulnerabilidad no identificada en una red de dispositivos conectados. Un ciberdelincuente puede aprovechar esto para acceder a todos los archivos de esta red y cifrarlos después. A continuación, el atacante exige un rescate a cambio de descifrar los archivos. Podría amenazar con quitar todos los archivos si el rescate no se ha pagado en una fecha límite establecida.
- El **spyware** es un tipo de carga que **espía un dispositivo o sistema**. Por ejemplo, el malware puede instalar software de examen de teclado en el dispositivo de un usuario, recopilar detalles de contraseñas y transmitirlos al atacante, y todo sin que el usuario lo sepa.

Descripción de malware

¿Qué es una carga?

- **Puertas traseras**: una puerta trasera es una carga que **permite a un ciberdelincuente aprovechar una vulnerabilidad en un sistema o dispositivo para eludir las medidas de seguridad existentes y causar daños**. Imagine que un ciberdelincuente se infiltra en una empresa de desarrollo de software y deja algún código que le permite realizar ataques. Esto se convierte en una puerta trasera que el ciberdelincuente podría usar para piratear la aplicación, el dispositivo en el que se ejecuta e incluso las redes y los sistemas de la organización y los clientes.
- La **red de robots (botnet)** es un tipo de carga que **une un equipo, un servidor u otro dispositivo a una red de dispositivos infectados de forma similar que se pueden controlar de forma remota para llevar a cabo alguna acción fraudulenta.** Una aplicación común de malware de red de robots (botnet) es la minería de datos de cifrado (a menudo denominada malware de minería de datos de cifrado). En este caso, el malware conecta un dispositivo a una red de robots (botnet) que consume la potencia informática del dispositivo para extraer o generar criptomonedas. Es posible que un usuario observe que su equipo se ejecuta más lentamente de lo normal y que empeora con los días.

Descripción de estrategias básicas de mitigación

Ha aprendido que hay muchos tipos diferentes de ciberataques. Pero **¿cómo puede a su organización frente a los ciberdelincuentes?** Hay varias maneras diferentes de mantener a raya a los ciberdelincuentes, desde la autenticación multifactor hasta la mejora de la seguridad del explorador y la información y capacitación de los usuarios.

¿Qué es una estrategia de mitigación?

Una estrategia de mitigación es una medida o colección de pasos que una organización realiza para evitar un ciberataque o defenderse de él. Esto se hace normalmente mediante la implementación de directivas y procesos tecnológicos y organizativos diseñados para protegerse frente a ataques. Estas son algunas de las muchas estrategias de mitigación diferentes disponibles para una organización:

- **Autenticación multifactor**
- **Seguridad del explorador**

Descripción de estrategias básicas de mitigación

Autenticación multifactor

Tradicionalmente, si la contraseña o el nombre de usuario de alguien están en peligro, esto permite que un ciberdelincuente pueda obtener el control de la cuenta. Pero se introdujo la autenticación multifactor para combatir esto.

La autenticación multifactor funciona exigiendo a un usuario que proporcione varias formas de identificación para comprobar que es quien dice ser. La forma más común de identificación que se usa para comprobar o autenticar a un usuario es una contraseña. Esto representa algo que el usuario sabe.

Otros dos métodos de autenticación proporcionan algo que el usuario es, como una huella digital o un escaneo de retina (una forma biométrica de autenticación) o proporcionan algo que el usuario tiene, como un teléfono, una clave de hardware u otro dispositivo de confianza. La autenticación multifactor emplea dos o más de estas formas de prueba para comprobar un usuario válido.

Por ejemplo, un banco podría exigir que un usuario proporcione códigos de seguridad enviados a su dispositivo móvil, además de su nombre de usuario y contraseña, para acceder a su cuenta en línea.

Descripción de estrategias básicas de mitigación

Seguridad del explorador

Todos dependemos de los exploradores para acceder a Internet para trabajar y llevar a cabo nuestras tareas diarias.

Como ha aprendido anteriormente, **los atacantes pueden poner en peligro los exploradores poco seguros. Un usuario puede descargar un archivo malintencionado o instalar un complemento malintencionado** que pueda poner en peligro el explorador, el dispositivo e incluso propagarse a los sistemas de una organización**.**

Las organizaciones pueden protegerse frente a estos tipos de ataques mediante la implementación de directivas de seguridad que:

- *Impiden la instalación de extensiones o complementos del navegador no autorizados.*
- *Solo permiten que los exploradores permitidos se instalen en dispositivos.*
- *Bloquean determinados sitios mediante filtros de contenido web.*
- *Mantienen actualizados los exploradores.*

Descripción de estrategias básicas de mitigación

Educación de los usuarios

Los ataques de ingeniería social se basan en las vulnerabilidades de las personas para causar daños. **Las organizaciones pueden defenderse contra los ataques de ingeniería social mediante la capacitación de su personal**.

Los usuarios deben aprender a reconocer contenido malintencionado que reciben o encuentran, y saber qué hacer cuando detectan algo sospechoso. Por ejemplo**, las organizaciones pueden enseñar a los usuarios a** :

- *Identificar elementos sospechosos en un mensaje.*
- *No responder nunca a solicitudes externas de información personal.*
- *Bloquear dispositivos cuando no están en uso.*
- *Almacene, comparta y quite datos solo según las directivas de la organización.*

Descripción de estrategias básicas de mitigación

Información sobre amenazas

El panorama de amenazas puede ser amplio. Las organizaciones pueden tener muchos vectores de ataque que son todos los posibles objetivos de los ciberdelincuentes.

Esto significa **que las organizaciones deben tomar tantas medidas como sea posible para supervisar, evitar, defenderse contra los ataques e incluso identificar posibles vulnerabilidades antes de que los ciberdelincuentes las usen para llevar a cabo ataques**. En resumen, **deben usar la inteligencia sobre amenazas.**

La inteligencia sobre amenazas **permite a una organización recopilar información sobre sistemas, detalles sobre vulnerabilidades, información sobre ataques, etc**.

En función del conocimiento que se tenga de esta información, la organización puede implementar directivas de seguridad, dispositivos, acceso de usuarios, etc., para defenderse contra los ciberataques. La colección de información para obtener conclusiones y responder a los ciberataques se conoce como inteligencia sobre amenazas.

Descripción de estrategias básicas de mitigación

Las organizaciones pueden usar soluciones tecnológicas para implementar inteligencia sobre amenazas en sus sistemas. A menudo se trata de soluciones inteligentes contra amenazas que pueden recopilar automáticamente información e incluso buscar ataques y vulnerabilidades y responder a ellos.

Estas son solo algunas de las estrategias de mitigación que las organizaciones pueden adoptar para protegerse frente a ciberataques. **Las estrategias de mitigación permiten a una organización adoptar un enfoque sólido en relación con la ciberseguridad. Esto protegerá en última instancia la confidencialidad, integridad y disponibilidad de la información.**

Resumen y recursos

En este módulo, ha aprendido conceptos como ciberataques, ciberseguridad, panorama de amenazas y malware. También ha visto cómo mitigar los ciberataques.

Ha aprendido **que los ciberdelincuentes usan ciberataques para obtener acceso o control no autorizados en dispositivos, sistemas y datos. A continuación, pueden poner en peligro la confidencialidad, integridad o disponibilidad de la información (el modelo CIA).**

Además, ha visto que **la ciberseguridad es la forma de proteger y mantener la confidencialidad, la integridad y la disponibilidad de la información.** Esto se debe a que la ciberseguridad le **permite implementar estrategias de mitigación que puede usar para protegerse frente a ciberataques**.

Ahora que ha completado este módulo, podrá realizar lo siguiente:

- *Describir el panorama básico de amenazas*
- *Describir los diferentes tipos de malware*
- *Describir estrategias básicas de mitigación*

CONTENIDOS

1. DESCRIPCIÓN DE AMENAZAS, ATAQUES Y MITIGACIONES BÁSICOS DE CIBERSEGURIDAD
2. **DESCRIPCIÓN DE LOS CONCEPTOS DE CRIPTOGRAFÍA**
3. DESCRIPCIÓN DE LA AUTENTICACIÓN Y LA AUTORIZACIÓN EN CIBERSEGURIDAD
4. DESCRIBIR LAS AMENAZAS DE RED Y LAS MITIGACIONES
5. DESCRIPCIÓN DE LAS AMENAZAS BASADAS EN DISPOSITIVOS Y LOS CONTROLES DE SEGURIDAD
6. DESCRIPCIÓN DE AMENAZAS BASADAS EN APLICACIONES Y CÓMO PROTEGERSE FRENTE A ELLAS

DESCRIPCIÓN DE LOS CONCEPTOS DE CRIPTOGRAFÍA

Introducción

Las palabras "criptografía" y "cifrado" pueden hacer pensar en espías y operaciones clandestinas, o en piratas informáticos sentados en habitaciones sin ventanas. Sin embargo, gran parte del mundo en línea moderno actual no sería posible sin estos dos conceptos.

La criptografía y el cifrado son los pilares de cualquier buena solución de ciberseguridad. Por ejemplo, ayudan a mantener los mensajes de correo electrónico a salvo de miradas indiscretas y protegen los pagos en línea.

A medida que continúe su recorrido por el mundo de la ciberseguridad, **verá cómo usamos la criptografía y el cifrado para protegernos en las actividades cotidianas.**

Después de completar este módulo, tendrá amplios conocimientos sobre lo siguiente:

- *Conceptos básicos de criptografía.*
- *Usos del cifrado en la ciberseguridad.*
- *Usos del hashing y la firma digital.*
- *Compatibilidad de los certificados digitales con una buena ciberseguridad.*

Descripción de la criptografía

El deseo de mantener cierta información en secreto nos ha acompañado desde que aprendimos a comunicarnos. A lo largo de la historia, hemos desarrollado nuevos métodos y formas de comunicarnos y, a su vez, ha crecido la necesidad de compartir secretos con amigos y aliados.

Definición de criptografía

El término "criptografía", derivado de la palabra griega "*kryptos*", que significa *oculto* o *secreto*, **hace referencia a la aplicación de una comunicación segura en cualquier forma entre un remitente y un destinatario**. Normalmente, **la criptografía se usa para ocultar el significado de un mensaje** escrito, pero también se puede aplicar a imágenes.

El primer uso conocido de la criptografía se remonta al antiguo Egipto y al uso de jeroglíficos complejos. Uno de los primeros cifrados utilizados para proteger las comunicaciones militares provino del emperador romano Julio César.

Estos dos ejemplos muestran claramente que la criptografía tiene muchos usos y no se limita al mundo digital. Sin embargo, desde esos humildes orígenes, hay una cosa que está clara: **la criptografía es ahora un requisito fundamental para ayudar a proteger nuestro planeta conectado digitalmente.**

Descripción de la criptografía

- Cada vez que se usa un explorador para acceder, por ejemplo, a una dirección HTTPS, a una tienda minorista en línea, a una cuenta bancaria o incluso a este sitio de Learn, **los elementos de criptografía preservan la seguridad y la confidencialidad de las interacciones.**
- Cada vez que conecta un dispositivo de forma inalámbrica a un enrutador para acceder a Internet, la criptografía ayuda a protegerlo.
- Se puede usar también para **proteger los archivos del almacenamiento externo o interno**.
- Los smartphones han cambiado la forma en que nos comunicamos, desde llamadas de vídeo y audio a mensajería de texto. La criptografía se usa para mantener la confidencialidad y la integridad de estas comunicaciones.

Descripción de la criptografía

Al igual que con todos los sistemas, la criptografía tiene sus propios términos y fraseología. **Dos de los términos más importantes son "texto no cifrado" y "texto cifrado".**

- El término **texto no cifrado** representa cualquier mensaje, incluidos los documentos, la música, las imágenes, las películas, los datos y los programas informáticos, que se encuentre a la espera de una transformación criptográfica.
- Una vez que el texto no cifrado se convierte en un mensaje secreto, se denomina **texto cifrado**. Este término representa los datos cifrados o protegidos.

Descripción de la criptografía

Como hemos visto en la unidad anterior, **la criptografía es el arte de ocultar el significado de un mensaje a todos los usuarios, menos al destinatario previsto**. Esto requiere que el mensaje de texto no cifrado se transforme en texto cifrado. El mecanismo que hace esto posible se denomina "cifrado".

Los métodos usados para cifrar un mensaje han evolucionado a lo largo de miles de años, desde el intercambio de una letra por otra hasta dispositivos mecánicos más elaborados, como la máquina Enigma.

El cifrado ahora tiene lugar en el mundo digital. Se usan equipos y matemáticas para combinar números primos altos aleatorios con el fin de crear claves que se emplean tanto en el cifrado simétrico como en el asimétrico.

Descripción de la criptografía

¿Qué es el cifrado?

El cifrado es el mecanismo por el que los mensajes de texto no cifrado se convierten en texto cifrado ilegible. El uso del cifrado mejora la *confidencialidad* de los datos que se comparten con el destinatario, ya sea un amigo, un compañero de trabajo o una empresa.

El descifrado es el mecanismo por el que el destinatario de un mensaje de texto cifrado puede volver a convertirlo en texto no cifrado legible.

Para facilitar los procesos de cifrado y descifrado, debe usar una clave de cifrado secreta. Esta clave es muy parecida a la que usaría para abrir el coche o la puerta de su casa. **Las claves de cifrado pueden ser de dos tipos:**

- *Claves simétricas*
- *Claves asimétricas*

Descripción de la criptografía

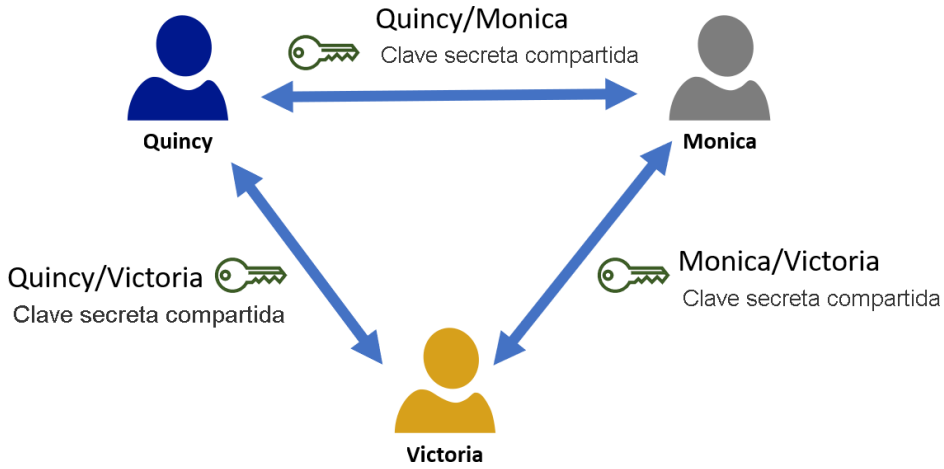
Claves simétricas

El cifrado de claves simétricas **se basa en la idea de usar la misma clave criptográfica tanto para el *cifrado* del mensaje de texto no cifrado como el *descifrado* del mensaje de texto cifrado**. Esto hace que el método de cifrado sea rápido y proporciona un grado de confidencialidad en cuanto a la seguridad del texto cifrado.

Con este método de cifrado, **la clave criptográfica se trata como un *secreto compartido* entre dos o más partes**. El secreto debe protegerse cuidadosamente para evitar que lo encuentre una persona con malas intenciones. Todas las partes deben tener la misma clave criptográfica para poder enviar mensajes seguros. **La distribución de la clave representa uno de los desafíos asociados al cifrado simétrico.**

Imagine un grupo u organización en el que cada individuo necesite la capacidad de comunicarse de forma segura con otra persona. Si el grupo consta de tres individuos, solo necesita tres claves.

Descripción del cifrado y sus usos en la ciberseguridad



Ahora, imaginemos el caso de una organización con solo 100 empleados en la que cada persona necesite comunicarse de forma segura con todas las demás. En este caso, es necesario crear, compartir y administrar de forma segura 4950 claves. Por último, imaginemos una organización gubernamental con 1000 empleados donde cada individuo necesite comunicarse de forma segura. Se necesitan 499.500 claves. Este crecimiento se puede expresar con la fórmula p x (p-1)/2, donde "p" es el número de personas que necesitan comunicarse.

A medida que crece el número de personas de la organización, el número de claves aumenta significativamente. Esto hace que la administración y la distribución seguras de las claves secretas, que se usan en el cifrado simétrico, sean difíciles y costosas.

Descripción del cifrado y sus usos en la ciberseguridad

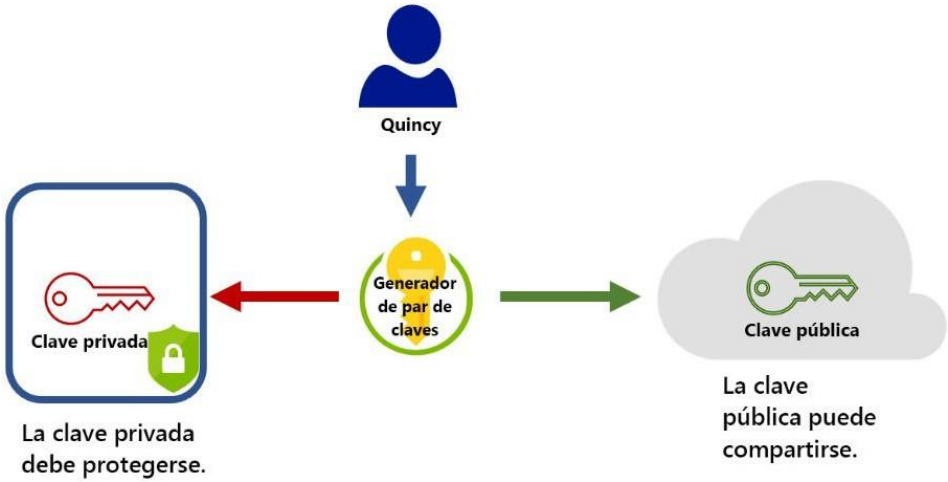
Cifrado asimétrico o de clave pública

El cifrado asimétrico **se desarrolló en los años 70**. Aborda la distribución y la proliferación seguras de claves asociadas al cifrado simétrico.

El cifrado asimétrico cambió la forma en la que se compartían las claves criptográficas. En lugar de una clave de cifrado, **una clave asimétrica se compone de dos elementos: una clave privada y una clave pública, que forman un par de claves. La clave pública, como su nombre sugiere, se puede compartir con cualquier persona**, por lo que ahorra a particulares y organizaciones tener que preocuparse por su distribución segura.

La clave privada debe protegerse. Solo la supervisará la persona que haya generado el par de claves y no se compartirá con nadie. **Un usuario que necesite cifrar un mensaje usará la clave pública y solo la persona que tenga la clave privada podrá descifrarlo**.

Descripción del cifrado y sus usos en la ciberseguridad



El cifrado asimétrico, con su uso de claves públicas y privadas, **elimina la molestia de tener que distribuir de forma segura las claves.**

Este concepto también aborda la proliferación de claves que vimos cuando hablamos del cifrado simétrico.

Piense en el ejemplo de la organización gubernamental de 1000 empleados en la que cada individuo debe poder comunicarse de forma segura.

Con el cifrado asimétrico, cada persona generará un par de claves, lo que dará como resultado 2000 claves. Con el cifrado simétrico, se habrían requerido 450.000 claves.

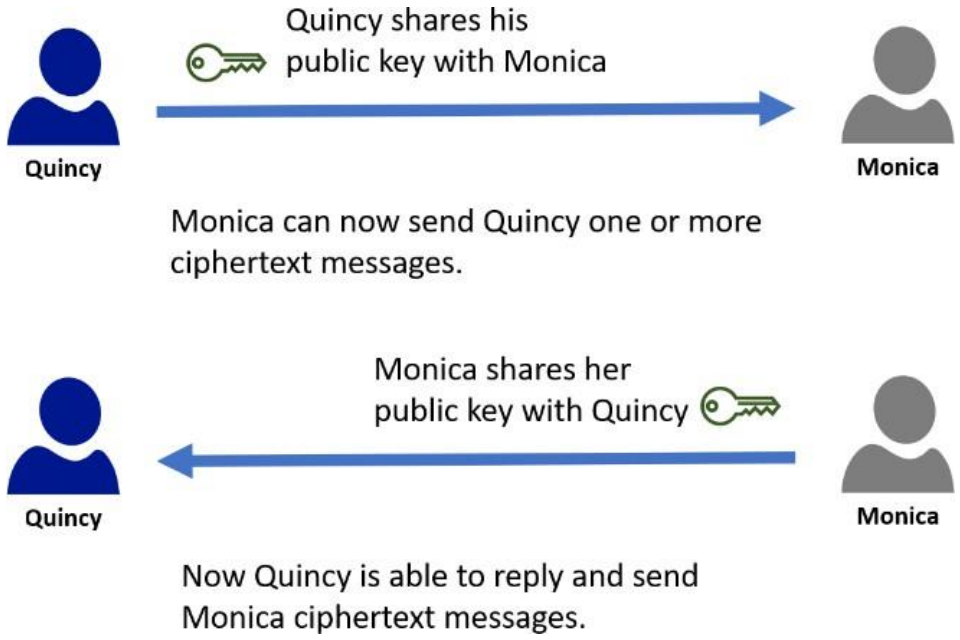
Descripción del cifrado y sus usos en la ciberseguridad

¿Cómo funciona el cifrado asimétrico?

Aunque los algoritmos y las matemáticas que respaldan el cifrado asimétrico son complejos, el principio de su funcionamiento es relativamente sencillo.

Supongamos que tenemos dos personas, Quincy y Mónica, que necesitan comunicarse de forma segura y privada. Mediante el uso de las herramientas de software disponibles, cada una de ellas crea su propio par de claves.

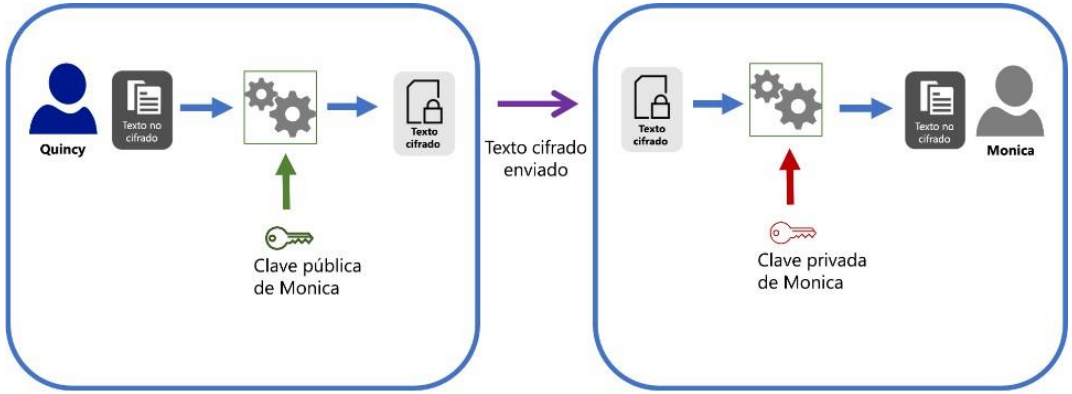
Lo primero que harán es compartir sus claves públicas la una con la otra. Dado que las claves públicas no son secretas, pueden intercambiarlas por correo electrónico.



Descripción del cifrado y sus usos en la ciberseguridad

¿Cómo funciona el cifrado asimétrico?

Cuando Quincy quiere enviar un mensaje protegido a Mónica**, usa su clave pública para cifrar el texto no cifrado y crear el texto cifrado.** A continuación, Quincy enviará el texto cifrado a Mónica por el medio que quiera; por ejemplo, por correo electrónico. Cuando Mónica reciba el texto cifrado, usará su **clave privada** para descifrarlo y lo volverá a convertir en texto no cifrado.



Quincy usa la clave pública de Monica para convertir su mensaje de texto sin formato en texto cifrado.

Mónica reciba el texto cifrado y usa su clave privada para volverlo a convertir en texto no cifrado.

Cuando Mónica quiera responder, usará la **clave pública** de Quincy para cifrar el mensaje antes de enviarlo. Luego, Quincy usará su **clave privada** para descifrarlo.

Supongamos que a Eve le interesa conocer los mensajes que están intercambiando Quincy y Mónica. Eve intercepta un mensaje de texto cifrado que Quincy ha enviado a Mónica. Además, Eve conoce la clave pública de Mónica.

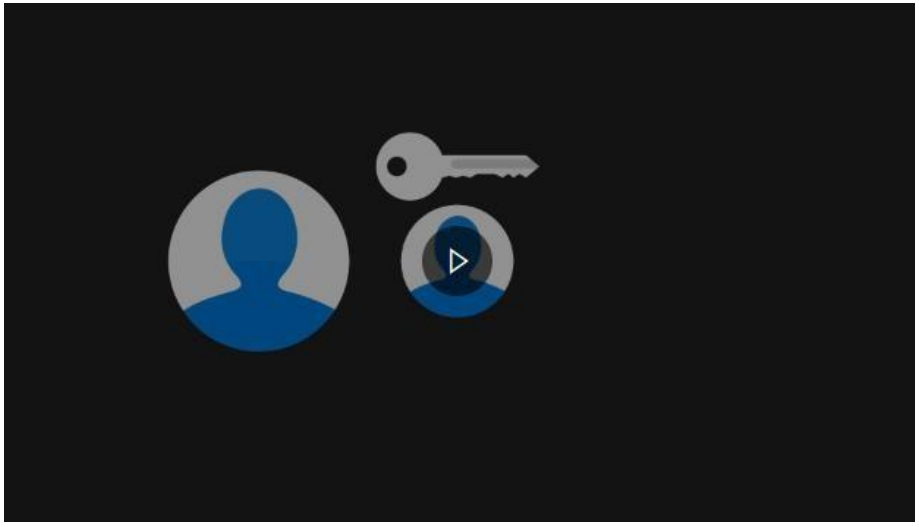
Descripción del cifrado y sus usos en la ciberseguridad

¿Cómo funciona el cifrado asimétrico?

Dado que no conoce la clave privada de Mónica, no tiene forma de descifrar el texto cifrado. Si Eve intenta descifrar el texto cifrado con la clave pública de Mónica, verá texto incomprensible.

Dada la naturaleza del cifrado asimétrico, incluso aunque se conozca la clave pública, es imposible detectar la clave privada.

En este vídeo de dos minutos, se muestra cómo funcionan el cifrado simétrico y el asimétrico y cómo estos protegen los documentos de la lectura por parte de personas no autorizadas.



Descripción del cifrado y sus usos en la ciberseguridad

Diferentes tipos de cifrados

Hay varios tipos de cifrado simétrico y asimétrico y se inventan nuevas versiones constantemente. Estos son algunos de los que puede encontrarse:

- **Data Encryption Standard (DES)** y **Triple DES**. Se trata de uno de los primeros estándares de cifrado simétricos que se usaron.
- **Advanced encryption standard (AES)**. AES reemplazó al cifrado DES y Triple DES, y se sigue usando mucho en la actualidad.
- **RSA**. Se trata de uno de los primeros estándares de cifrado asimétrico que se usaron y del que actualmente se siguen utilizando variaciones.

Descripción del cifrado y sus usos en la ciberseguridad

¿Dónde se usa el cifrado?

El cifrado se usa en todo el mundo y en casi todos los ámbitos de la vida, desde para hacer una llamada con el móvil hasta para usar la tarjeta de crédito para una compra en una tienda. El cifrado se usa aún más al navegar por Internet.

Exploración web

Es posible que se dé cuenta, pero cada vez que va a **un sitio web cuya dirección comienza por "https" o se muestra un icono de candado, se está usando el cifrado**. Si observa la barra de direcciones de esta página web, verá que comienza por "https://". Del mismo modo, cuando se conecte a su banco a través de la Web o realice una compra en línea en la que proporcione información confidencial, como un número de tarjeta de crédito, deberá asegurarse de que aparezca "https://" en la barra de direcciones.

Cifrado de dispositivos

Muchos sistemas operativos proporcionan **herramientas para habilitar el cifrado de unidades de disco duro y dispositivos portátiles.** Por ejemplo, **Windows BitLocker**, una característica del sistema operativo Windows, proporciona cifrado para el disco duro del equipo o las unidades portátiles que se puedan conectar en el puerto USB.

Descripción del cifrado y sus usos en la ciberseguridad

¿Dónde se usa el cifrado?

Aplicaciones de mensajería

Algunas de **las aplicaciones de mensajería conocidas y disponibles habitualmente cifran los mensajes.**

Comunicaciones móviles

independientemente de si usa **un smartphone u otro dispositivo de comunicaciones móviles, se usa el cifrado para registrarlo de forma segura en el mástil o la torre de telecomunicaciones que haya más cerca.** Esto garantiza que siempre tenga la mejor intensidad de señal.

Descripción del hashing y su aplicación en la firma digital

Hasta ahora, ha visto cómo se usa la criptografía, mediante el uso del cifrado, para proteger los mensajes de miradas indiscretas. La criptografía también se usa para comprobar que los datos, como los documentos y las imágenes, no se hayan alterado. Esto se realiza a través de un proceso denominado "hashing".

¿Qué es el hashing?

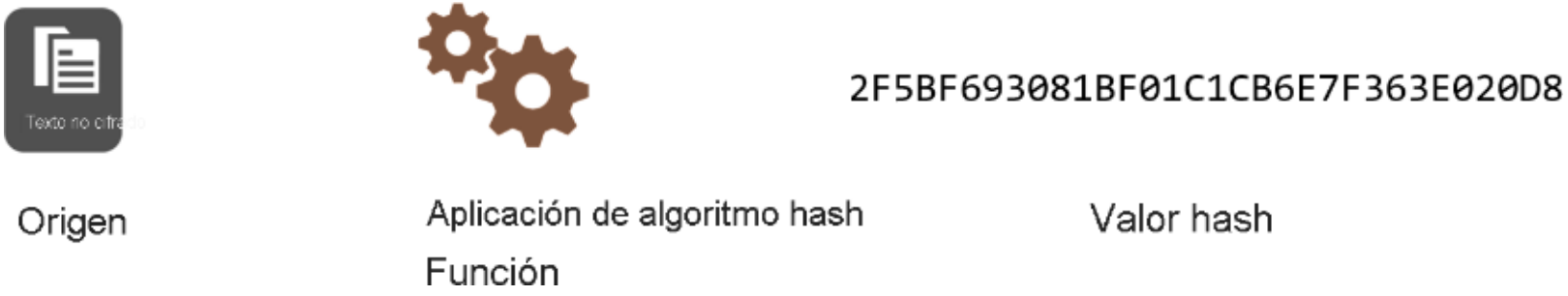
El hashing utiliza un algoritmo, también conocido como función hash para convertir el texto original en un valor de longitud fija único. Esto se denomina "valor hash". Cada vez que se aplica un algoritmo hash al mismo texto mediante el mismo algoritmo, se genera el mismo valor hash. Ese hash se puede usar como identificador único de los datos asociados.

El hashing es diferente del cifrado, ya que no usa claves, y el valor al que se aplica el algoritmo hash no puede descifrarse para convertirse en el valor original.

Descripción del hashing y su aplicación en la firma digital

Existen muchos tipos de funciones hash. Uno que es conocido y que puede que escuche en las conversaciones con profesionales de seguridad es el algoritmo hash seguro (SHA).

SHA es una familia de algoritmos hash en la que cada uno funciona de forma diferente. No entraremos en detalles en este contenido, pero uno de los SHA más usados es el SHA-256, que genera un valor hash de 256 bits de longitud.



Descripción del hashing y su aplicación en la firma digital

¿Qué es una firma digital?

Una aplicación común del hashing es la firma digital. Al igual que una firma manuscrita, **una firma digital valida que el documento lleva la firma que procede realmente de la persona que lo firmó. Además, las firmas digitales se usan para validar que el documento no se haya alterado.**

¿Cómo funciona una firma digital?

Una firma digital siempre será única para cada persona que firme un documento, de forma muy parecida a una firma manuscrita. **Todas las firmas digitales usan un par de claves asimétricas: la privada y la pública.**

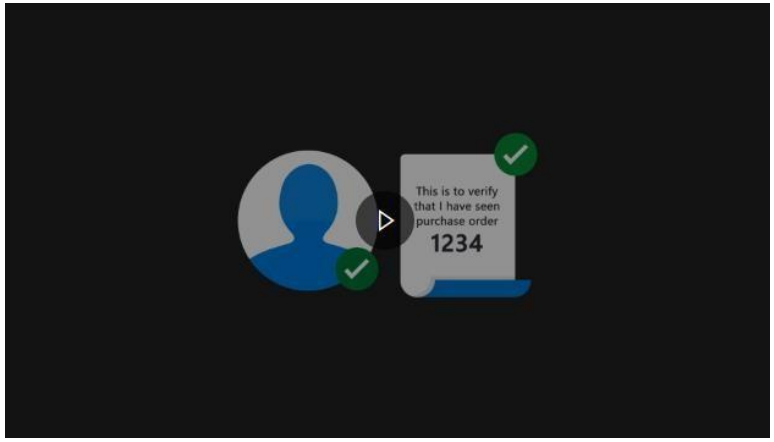
Con un servicio de firma digital, Mónica puede asignar una firma digital al documento para demostrar que este no ha cambiado. Al firmar el documento, se crea un hash con marca de tiempo. A continuación, este hash se cifra mediante la clave privada de Mónica. A continuación, el servicio de firma anexa el hash al documento original, que no está cifrado. Por último, tanto el documento firmado digitalmente como la clave pública de Mónica se envían a Victoria.

Descripción del hashing y su aplicación en la firma digital

¿Cómo funciona una firma digital?

Cuando esta última recibe el documento firmado digitalmente, usa el mismo servicio de firma digital para extraer el hash de Mónica del documento y generar un hash nuevo para el documento de texto no cifrado original. A continuación, con la clave pública de Mónica, se descifra el hash cifrado. Si el hash descifrado de Mónica coincide con el que creó Victoria para el documento, la firma digital será válida. Y así Victoria sabrá que el documento no se ha alterado.

En el siguiente vídeo de dos minutos verá cómo funcionan las firmas digitales y cómo se muestran estas si se ha alterado un documento.



La firma digital requiere el uso de un servicio de firma digital. Muchas empresas ofrecen esta funcionalidad. Dos de los más populares son DocuSign y Adobe Sign.

Descripción de los certificados digitales

La criptografía tiene muchas aplicaciones en el mundo moderno actual. Ha visto cómo **el cifrado puede garantizar la confidencialidad de los mensajes.** También ha aprendido cómo se usa el hash en firmas digitales para comprobar que un mensaje no se ha alterado.

En esta unidad, obtendrá información sobre **los certificados digitales** y cómo proporcionan una capa adicional de seguridad.

Los certificados abordan la posibilidad de que una persona poco ética intercepte, modifique o falsifique mensajes, algo que puede ocurrir en la comunicación digital.

Básicamente, **un certificado digital es una credencial emitida por una entidad de certificación (CA) que se usa para comprobar la identidad de la persona o entidad a la que se emite el certificado, que se denomina firmante**. En este sentido, un certificado digital es como un pasaporte u otra credencial de identidad emitida por una autoridad de confianza o una agencia gubernamental para comprobar una identidad. Los datos de un certificado incluyen información sobre el firmante y su clave pública de su par de claves pública y privada, y han sido comprobados por la CA.

Descripción de los certificados digitales

Para obtener un certificado digital, la persona o entidad envía una solicitud de certificación a una CA de confianza.

Los detalles de la identidad del solicitante y su clave pública, del par de claves pública y privada generadas a partir de una herramienta disponible, se incluyen en la solicitud de certificado.

En algunos casos, el solicitante puede pedir que la CA emita un par de claves en su nombre como parte de la solicitud. En cualquier caso, la entidad o persona siempre mantiene en secreto la clave privada.

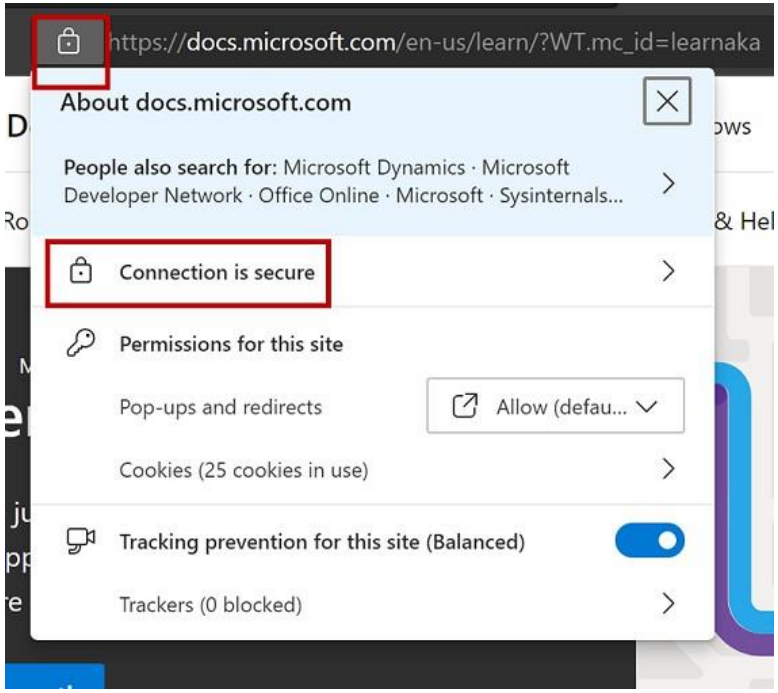
La CA revisa toda la información de identidad enviada en la solicitud para determinar si cumple los criterios para emitir un certificado.

Si la CA aprueba la solicitud, firma y emite un certificado que contiene información sobre el firmante y su clave pública.

Descripción de los certificados digitales

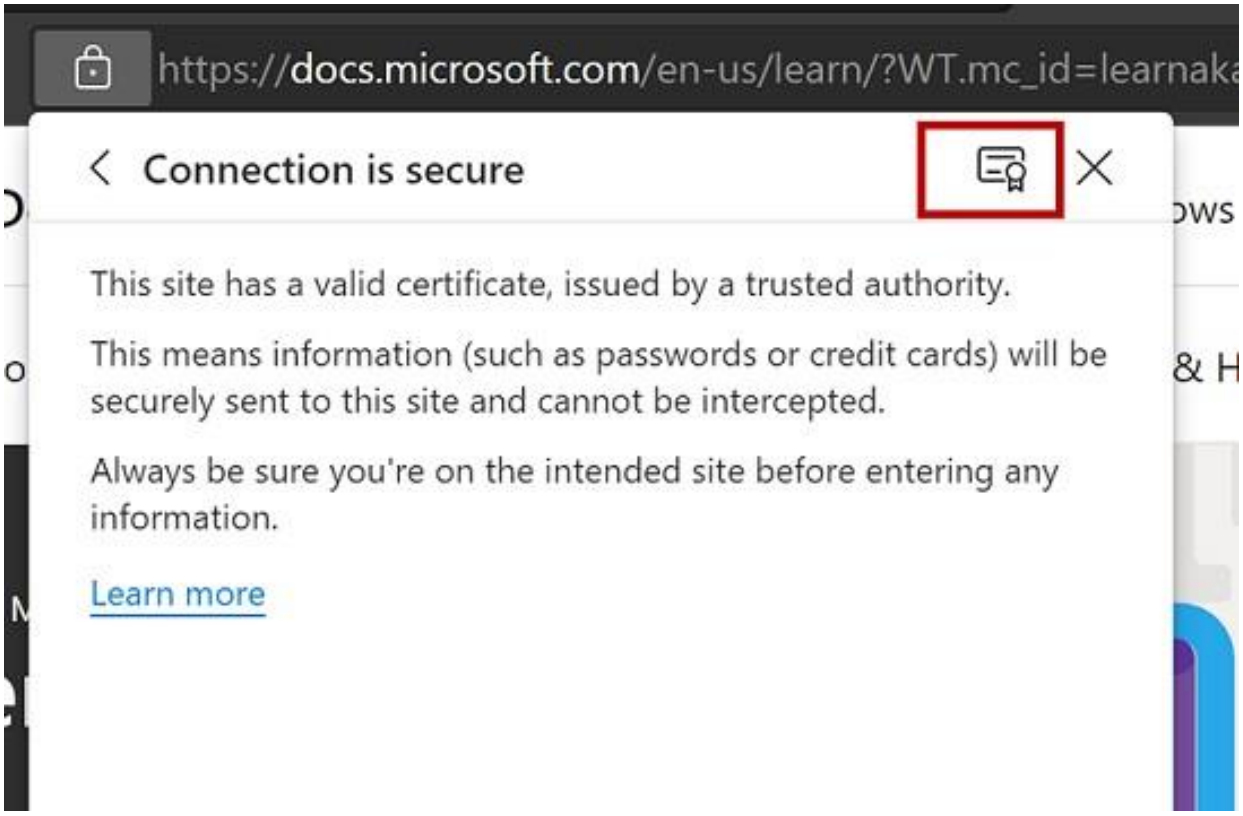
La duración de un certificado digital tiende a ser de un año, después del cual expira. Cuando esto sucede, se muestra un mensaje de advertencia sobre los certificados expirados. La advertencia indica que no se puede confirmar la identidad del firmante.

Una aplicación común de los certificados digitales, que es visible para el usuario, está en la comunicación basada en web. **Los certificados digitales se emplean en sitios web que usan la comunicación *HTTPS* segura**, que se denota mediante un icono de un candado en la barra de direcciones del explorador. Al seleccionar el candado en la barra de direcciones, se pueden elegir varias opciones y obtener información adicional.



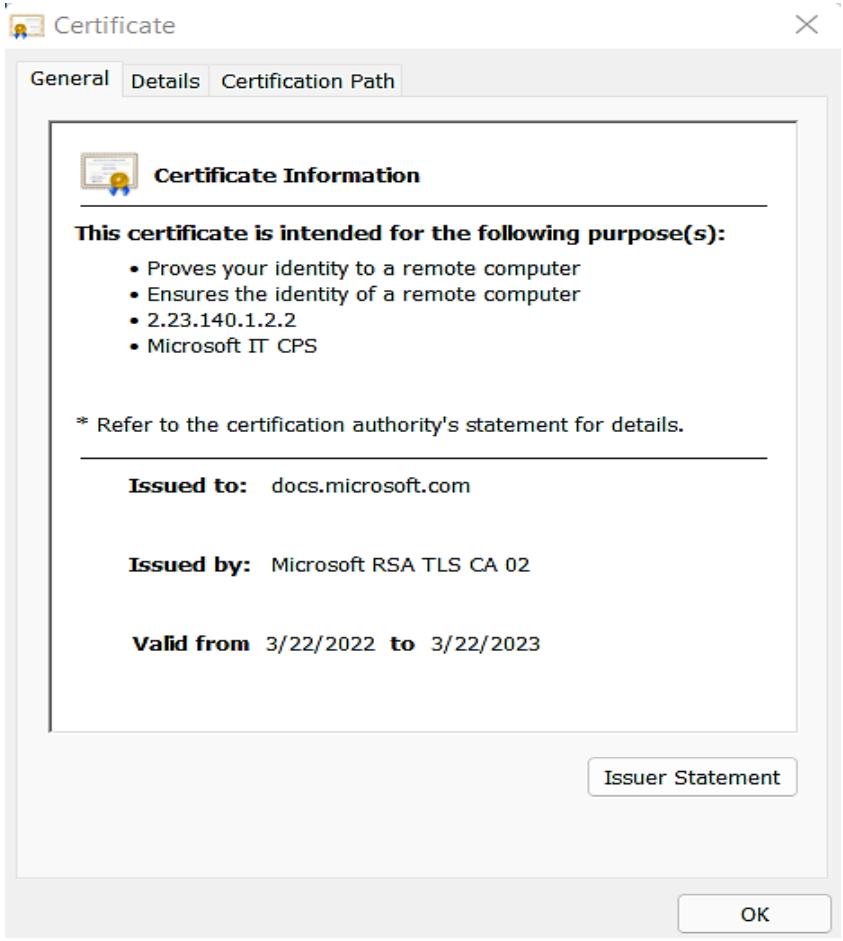
Descripción de los certificados digitales

Al seleccionar "La conexión es segura", se proporciona información sobre la conexión, como se muestra en la imagen siguiente.



Descripción de los certificados digitales

Al seleccionar el icono de certificado, se proporcionan detalles sobre el certificado digital.



Descripción de los certificados digitales

¿Por qué necesitamos certificados digitales?

En una unidad anterior, describimos el proceso de cifrado asimétrico y cómo se usan los pares de claves pública y privada. En el ejemplo, Quincy y Monica quieren comunicarse de forma segura, así que cada uno genera su par de claves con software al que se puede acceder fácilmente. Monica y Quincy comparten su clave pública entre sí, pero mantienen en secreto su clave privada. Cuando Quincy quiere enviale un mensaje seguro a Monica, utiliza la clave pública de Monica para cifrar y enviar el mensaje. A su vez, Monica utiliza su clave privada para descifrar el mensaje.

El uso del cifrado asimétrico, descrito en el ejemplo, **garantiza la confidencialidad del mensaje**. Dado que las claves públicas son públicas, no hay nada que confirme que la clave pública que usó Quincy proviene realmente de Monica. Del mismo modo, no hay nada que confirme que fue Quincy quien, efectivamente, envió el mensaje. Existe la posibilidad de que una persona poco ética intercepte, altere o falsifique los mensajes. Los certificados digitales desempeñan un papel importante a la hora de abordar este riesgo.

Descripción de los certificados digitales

¿Por qué necesitamos certificados digitales?

Supongamos que una CA de confianza le ha emitido a Monica un certificado digital y que lo comparte con Quincy. **El certificado vincula la identidad** de Monica **con la clave pública**. Dado que Quincy usa la clave pública del certificado de Monica, Quincy está seguro de que la clave pública procede de Monica y solo la clave privada de Monica descifrará el mensaje.

Supongamos que Quincy también ha obtenido un certificado digital a través de una CA de confianza. Quincy usa su clave privada para firmar digitalmente el mensaje. Quincy envía el mensaje firmado a Monica junto con el certificado digital que contiene su clave pública. El certificado digital vincula la identidad de Quincy a la clave pública, por lo que el uso de la clave pública del certificado sirve para comprobar que el mensaje no se ha alterado y verifica que el mensaje procede de Quincy. Sin el certificado digital, una firma digital solo sirve para comprobar que el mensaje no se ha alterado.

Resumen y recursos

La criptografía es fundamental para proteger la confidencialidad, la integridad y la disponibilidad de la información. También sirve para defenderse de los ciberataques.

En nuestro recorrido por **la criptografía y el cifrado**, ha visto cómo los mensajes **secretos han evolucionado desde el cifrado simétrico hasta la aplicación moderna del cifrado de claves asimétricas** en el correo electrónico y la ciberseguridad en línea.

A continuación, ha visto cómo **el hashing y las firmas digitales usan el cifrado para validar la identidad y la autenticidad del mensaje y el contenido que se envía**. Por último, ahora entiende por qué los certificados son esenciales para mantener una buena ciberseguridad.

Después de completar este módulo, podrá:

- *Describir algunos de los conceptos básicos de la criptografía.*
- *Describir el cifrado y sus usos en la ciberseguridad.*
- *Describir el hashing y la firma digital.*
- *Describir los certificados digitales.*

CONTENIDOS

1. DESCRIPCIÓN DE AMENAZAS, ATAQUES Y MITIGACIONES BÁSICOS DE CIBERSEGURIDAD
2. DESCRIPCIÓN DE LOS CONCEPTOS DE CRIPTOGRAFÍA
3. **DESCRIPCIÓN DE LA AUTENTICACIÓN Y LA AUTORIZACIÓN EN CIBERSEGURIDAD**
4. DESCRIBIR LAS AMENAZAS DE RED Y LAS MITIGACIONES
5. DESCRIPCIÓN DE LAS AMENAZAS BASADAS EN DISPOSITIVOS Y LOS CONTROLES DE SEGURIDAD
6. DESCRIPCIÓN DE AMENAZAS BASADAS EN APLICACIONES Y CÓMO PROTEGERSE FRENTE A ELLAS

DESCRIPCIÓN DE LA AUTENTICACIÓN Y LA AUTORIZACIÓN EN CIBERSEGURIDAD

Introducción

Una buena ciberseguridad depende de numerosos factores para proporcionar la confianza y la garantía de que los datos están protegidos y se usan según lo previsto. **La autenticación es uno de estos factores**. **Proporciona un mecanismo que le permite confiar en que una persona es realmente quien dice ser**. Para ser eficaz, la autenticación debe ser sólida y sencilla de usar.

Cuando haya autenticado un usuario, deberá decidir qué puede hacer**. La autorización concede a cada usuario un nivel específico de acceso a los datos y los recursos.** Por lo general, a los usuarios se les deben conceder permisos suficientes para acceder a los recursos que necesitan.

Supongamos que está en el aeropuerto para coger un vuelo. Para poder obtener la tarjeta de embarque, debe demostrar quién es. Se presenta con su pasaporte y, si las identidades coinciden, ha superado el proceso de autenticación y recibe la tarjeta de embarque. Ahora que tiene una tarjeta de embarque, puede usarla para subir al avión. La tarjeta de embarque es la autorización, ya que solo le permitirá subir al avión que realiza el vuelo que ha reservado.

DESCRIPCIÓN DE LA AUTENTICACIÓN Y LA AUTORIZACIÓN EN CIBERSEGURIDAD

Introducción

La autenticación es la llave que abre la puerta y la autorización decide adónde puede ir y qué puede ver.

Después de completar este módulo, podrá:

- *Describir la autenticación*
- *Describir algunos de los ataques comunes basados en la autenticación*
- *Describir las técnicas de seguridad de autorización*

Definir la autenticación

La autenticación es el proceso de demostrar que una persona es quien dice ser. Cuando alguien compra un artículo con una tarjeta de crédito, es posible que tenga que mostrar una forma adicional de identificación. De esta manera, demuestra que es la persona cuyo nombre aparece en la tarjeta. En este ejemplo, el usuario puede mostrar el DNI, que sirve como forma de autenticación y verifica su identidad.

Si quiere acceder a un equipo o un dispositivo, se encontrará con el mismo tipo de autenticación. Es posible que se le pida que escriba un nombre de usuario y una contraseña. El nombre de usuario indica quién es, pero no es suficiente por sí solo para concederle acceso. Cuando lo combina con la contraseña, que solo usted debe conocer, obtiene acceso a los sistemas. El nombre de usuario y la contraseña son una forma de autenticación.

Los métodos de autenticación sólida son esenciales para mantener una buena ciberseguridad y garantizar que solo los usuarios autorizados puedan obtener acceso a datos y recursos confidenciales.

Si bien la autenticación verificará al usuario, no rige lo que un usuario puede hacer una vez que ha sido autenticado. **El control de lo que un usuario puede hacer se denomina autorización**. Más adelante en este módulo veremos en qué consiste.

Definir la autenticación

Métodos de autenticación

La autenticación se puede dividir en tres tipos: ***algo que sabe, algo que tiene y algo que forma parte de usted.***

- **Algo que sabe**, por ejemplo:
  - Contraseñas
  - Números PIN
  - Preguntas de seguridad
- **Algo que tiene**, por ejemplo:
  - Documentos de identidad
  - Llaves USB
  - Computers
  - Teléfonos móviles
- **Algo que forma parte de usted**, por ejemplo:
  - Una huella digital
  - Reconocimiento facial
  - Un examen de retina
  - Otras formas de identificación biométrica

Tipos de autenticación

La identificación biométrica se compone de características físicas que identifican de forma única a una persona.

Definir la autenticación

Autenticación de factor único

La autenticación de un solo factor es un sistema en el que solo se usa un tipo de autenticación, lo que lo convierte en el método menos seguro, pero el más sencillo.

Un ejemplo de este sistema es cuando el usuario proporciona **algo que sabe**, como una contraseña, para autenticarse. Las contraseñas simples son fáciles de recordar, pero los delincuentes pueden piratearlas fácilmente. Las contraseñas complejas pueden parecer más seguras, pero son imposibles de recordar. Es muy probable que la persona escriba en algún sitio este tipo de contraseña, lo que hace que sea mucho menos segura.

Otro método de autenticación de un solo factor consiste en usar **algo que tiene**. Por ejemplo, puede usar el teléfono móvil para pagar por un artículo. Un servicio de tocar para pagar autentica al usuario a través de algo que tiene, pero no requiere otro método de comprobación.

Definir la autenticación

Autenticación de factor único

Una característica biométrica (es decir, **algo que forma parte de usted**) se puede usar como método de autenticación de un solo factor, pero en algunos escenarios comunes no es necesariamente más segura. Piense, por ejemplo, en cuando usa la huella digital para desbloquear el teléfono móvil. Probablemente en alguna ocasión la huella digital no se reconocía fácilmente y se le ofrecía la opción de escribir un PIN. Esto puede hacer que resulte más fácil de adivinar. En la mayoría de los casos, las características biométricas se usan junto con otra forma de autenticación.

La autenticación de un solo factor es cómoda, **pero no se considera adecuada para un sistema altamente seguro.**

Definir la autenticación

Autenticación multifactor

La autenticación multifactor es un sistema en el que se usan dos o incluso tres tipos de autenticación.

Al proporcionar *algo que sabe, algo que tiene* y *algo que forma parte de usted*, **la seguridad del sistema aumenta enormemente.**

Por ejemplo, en un sistema de autenticación multifactor que usa dos tipos de autenticaciones, es posible que se le pida una contraseña y, luego, se le envíe un número al teléfono móvil.

Debe introducir este número, lo que demuestra que sabe la contraseña y tiene el teléfono móvil.

Este es un procedimiento habitual cuando se usa la autenticación multifactor para acceder a una cuenta bancaria en línea. La autenticación multifactor reduce la probabilidad de que una persona con malas intenciones pueda obtener acceso a información confidencial.

Definir la autenticación

Autenticación multifactor

Como ya se ha mencionado, la autenticación biométrica suele usarse junto con otro método de autenticación.

Piense, por ejemplo, en un banco que tiene una zona protegida donde mantiene las cajas de seguridad de los clientes. Para que alguien pueda obtener acceso, normalmente primero se le pide que escriba correctamente una contraseña y que supere un examen de la huella digital.

La autenticación multifactor es un método primordial para que los usuarios y las organizaciones mejoren la seguridad.

Debería ser el procedimiento predeterminado para la autenticación.

Descripción de los ataques basados en la autenticación

Los ataques de autenticación se producen cuando alguien intenta robar las credenciales de una persona. Después, puede simular que es esa persona. Dado que un objetivo de este tipo de ataques es suplantar a un usuario legítimo, a menudo también se les puede denominar **ataques de identidad. Entre los ataques comunes se incluyen los siguientes:**

- *Atacante por fuerza bruta*
- *Ataque de diccionario*
- *Relleno de credenciales*
- *Registro de claves*
- *Ingeniería social*

Descripción de los ataques basados en la autenticación

Atacante por fuerza bruta

En un ataque por fuerza bruta, un delincuente intenta obtener acceso simplemente probando diferentes combinaciones de nombre de usuario y contraseña. Normalmente, los atacantes tienen herramientas que automatizan este proceso mediante el uso de millones de combinaciones de nombre de usuario y contraseña.

Las contraseñas simples, con autenticación de un solo factor, son vulnerables a los ataques por fuerza bruta.

Ataque de diccionario

Un ataque por diccionario es una forma de ataque por fuerza bruta, en el que se aplica un diccionario de palabras de uso frecuente.

Para evitar los ataques por diccionario, es importante usar símbolos, números y combinaciones de varias palabras en una contraseña.

Descripción de los ataques basados en la autenticación

Relleno de credenciales

El relleno de credenciales es un método de ataque que aprovecha el hecho de que numerosas personas usan el mismo nombre de usuario y contraseña en muchos sitios.

Los atacantes usarán las credenciales robadas, normalmente obtenidas después de una vulneración de datos en un sitio, para intentar acceder a otras áreas. Los atacantes suelen usar herramientas de software para automatizar este proceso.

Para evitar el relleno de credenciales, es importante no reutilizar las contraseñas y cambiarlas periódicamente, sobre todo después de una vulneración de seguridad.

Registro de claves

El registro de claves implica el uso de software malintencionado que registra pulsaciones de teclas.

Con un registrador de claves, un atacante puede registrar (robar) combinaciones de nombre de usuario y contraseña, que luego se pueden usar para ataques de relleno de credenciales. Se trata de un ataque común en cibercafés o en cualquier lugar en el que se usen equipos compartidos.

Para evitar el registro de claves, no instale software que no sea de confianza y use software de confianza para la detección de virus.

Descripción de los ataques basados en la autenticación

Registro de claves

El registro de claves no se limita a los equipos informáticos. Supongamos que una persona malintencionada instala un dispositivo sobre el lector de tarjetas y el teclado de un cajero automático.

Cuando usted inserta la tarjeta, pasa primero a través del lector de tarjetas de la persona malintencionada, que captura los detalles de la tarjeta antes de que se introduzca en el lector de tarjetas del cajero automático.

Ahora, cuando introduzca su PIN con el teclado de la persona malintencionada, también obtendrá esta información.

Descripción de los ataques basados en la autenticación

Ingeniería social

La ingeniería social conlleva intentar que una persona revele información o realice una acción para hacer posible un ataque.

La mayoría de los ataques de autenticación implican la vulneración de equipos o el proceso de probar muchas combinaciones de credenciales. Los ataques de ingeniería social son diferentes, ya que aprovechan las vulnerabilidades de las personas. El atacante intenta ganarse la confianza del usuario legítimo y persuadirle para que divulgue información o realice una acción que posibilite causar daños o robar información.

Se pueden usar varias técnicas de ingeniería social para el robo de autenticación, entre las que se incluyen las siguientes:

- **suplantación de identidad (phishing)**
- **Pretexto**
- **Baiting**

Descripción de los ataques basados en la autenticación

Ingeniería social

- La **suplantación de identidad (phishing)** se produce cuando **un atacante envía un correo electrónico aparentemente legítimo con el objetivo de lograr que un usuario revele sus credenciales de autenticación.**

  Por ejemplo, puede parecer que un correo electrónico lo ha enviado el banco del usuario. Incluye un vínculo a lo que parece ser la página de inicio de sesión del banco, pero en realidad es un sitio falso.

  Cuando el usuario inicia sesión en el sitio falso, sus credenciales quedan a disposición del atacante.

  Existen diversas variantes de suplantación de identidad, incluido el phishing de objetivo definido, que suele estar dirigido a organizaciones, empresas o personas concretas.

Descripción de los ataques basados en la autenticación

Ingeniería social

- El **pretexto es un método por el cual un atacante se gana la confianza de la víctima y le convence para que divulgue información segura.** Después, puede usar estos datos para robar su identidad.

  Por ejemplo, un hacker podría llamarle por teléfono fingiendo ser del banco y pedirle su contraseña para comprobar su identidad. Otro método conlleva el uso de las redes sociales.

  Podrían pedirle que responda a una encuesta o un cuestionario con preguntas aparentemente aleatorias e inocentes que le harán revelar datos personales, o bien podrían enviarle un mensaje con un juego divertido, como crear el nombre de su grupo de pop imaginario con su lugar de nacimiento y el nombre de su primera mascota.

- El **baiting** es una forma de ataque en el que **el delincuente ofrece una recompensa o un premio falsos para animar a la víctima a divulgar información segura.**

Descripción de los ataques basados en la autenticación

Otros métodos de ataque basados en la autenticación

Estos son solo algunos ejemplos de ataques basados en la autenticación.

Siempre existe la posibilidad de que aparezcan nuevos tipos de ataque, pero todos los que se enumeran aquí se pueden evitar si se instruye a las personas y se usa la autenticación multifactor.

Describir las técnicas de seguridad de autorización

Cuando autentique a un usuario, tendrá que decidir adónde puede ir y qué se le permite ver y tocar. Este proceso se denomina **autorización.**

Supongamos que quiere pasar la noche en un hotel. Lo primero que hará es ir a la recepción para iniciar el "proceso de autenticación".

Una vez que el recepcionista haya comprobado quién es, le dará una tarjeta-llave y ya podrá dirigirse a su habitación.

Piense en la tarjeta-llave como el proceso de autorización. La tarjeta-llave solo le permitirá abrir las puertas y los ascensores a los que puede acceder, como la puerta de su habitación.

En términos de ciberseguridad, **la autorización determina el nivel de acceso de una persona autenticada a los datos y los recursos.**

Existen **diferentes técnicas de seguridad que las organizaciones usan para administrar la autorización:**

- **Acceso condicional**
- **Acceso con privilegios mínimos**
- **Desplazamiento lateral**
- **Confianza cero**

Describir las técnicas de seguridad de autorización

Acceso condicional

Como su nombre indica, el acceso condicional **implica el acceso con condiciones**. Una manera de pensar en el acceso condicional es con instrucciones if-then. Si algo es cierto, se le concede acceso, pero si es falso, se le deniega.

Veamos cómo funcionaría esto en un escenario de IT. Cada vez más personas trabajan desde casa. Probablemente usan su equipo personal para acceder a contenido relacionado con el trabajo. Con el acceso condicional, una organización podría conceder acceso a un usuario autenticado a un sistema confidencial, como el de las nóminas, solo si se usan equipos corporativos seguros ubicados en su sede central. Si el usuario autenticado intenta acceder al sistema de nóminas desde un equipo personal en casa, se bloquearía el acceso.

Describir las técnicas de seguridad de autorización

Acceso con privilegios mínimos

El concepto de privilegio mínimo consiste en conceder a un usuario los derechos mínimos que necesita. Esto se aplica a todas las configuraciones relacionadas con la seguridad.

Por ejemplo, cuando sube a un avión, tiene acceso a la zona principal de la cabina para llegar a su puesto, pero no se permite que ningún pasajero entre en la cabina del piloto. Además, si viaja con un billete de clase turista, solo podrá sentarse en esa zona. Para mejorar la seguridad, cada persona solo puede acceder a las áreas que necesita.

El mismo concepto se aplica en el contexto de la ciberseguridad. Piense en el caso de los usuarios que tienen acceso a una carpeta pública de una red. Si solo necesitan leer un archivo, se les debe conceder ese permiso específico.

Un usuario casi siempre se pondrá en contacto con el administrador si no tiene los derechos suficientes para desempeñar su rol. En cambio, rara vez le comunicará que tiene demasiados derechos. Así pues, el riesgo de ser demasiado cautelosos al asignar derechos de usuario es escaso.

Describir las técnicas de seguridad de autorización

Acceso con privilegios mínimos

El concepto de privilegio mínimo consiste en conceder a un usuario los derechos mínimos que necesita. Esto se aplica a todas las configuraciones relacionadas con la seguridad.

Por ejemplo, cuando sube a un avión, tiene acceso a la zona principal de la cabina para llegar a su puesto, pero no se permite que ningún pasajero entre en la cabina del piloto. Además, si viaja con un billete de clase turista, solo podrá sentarse en esa zona. Para mejorar la seguridad, cada persona solo puede acceder a las áreas que necesita.

El mismo concepto se aplica en el contexto de la ciberseguridad. Piense en el caso de los usuarios que tienen acceso a una carpeta pública de una red. Si solo necesitan leer un archivo, se les debe conceder ese permiso específico.

Un usuario casi siempre se pondrá en contacto con el administrador si no tiene los derechos suficientes para desempeñar su rol. En cambio, rara vez le comunicará que tiene demasiados derechos. Así pues, el riesgo de ser demasiado cautelosos al asignar derechos de usuario es escaso.

Al implementar el acceso con privilegios mínimos, reducirá las acciones de un atacante si se produce una vulneración.

Describir las técnicas de seguridad de autorización

Desplazamiento lateral

Si un atacante obtiene acceso a un sistema, podría usar la cuenta en peligro para recopilar más información, que a su vez podría permitirle infiltrarse en otros sistemas u obtener acceso elevado. El atacante puede moverse por el sistema y buscar más recursos hasta alcanzar su objetivo. Dado que el atacante intentará moverse entre distintas secciones, es poco probable que el ataque final proceda de la cuenta en peligro inicial.

Piense en un edificio de oficinas en el que un delincuente supera el control de seguridad de la zona de recepción principal. Por lo general, podrá moverse por el resto del edificio y acceder a diferentes plantas y oficinas. Es importante proporcionar capas de seguridad adicionales para protegerse frente a intrusiones en áreas confidenciales.

Por ejemplo, muchos edificios de oficinas requieren un código de seguridad para acceder a las plantas en las que se encuentra el equipo ejecutivo. Todas las oficinas de esas plantas están cerradas y solo se permite el acceso a los empleados que disponen de una tarjeta especial. Es evidente que no quiere que un delincuente acceda a su edificio, pero si asume que podría producirse una vulneración y agrega capas de seguridad adicionales para protegerse contra este tipo de desplazamiento lateral, puede limitar los daños.

El mismo concepto se aplica en un escenario de IT. Debe partir de una autenticación segura para reducir la probabilidad de que un atacante acceda a los sistemas. Ningún sistema es infalible, pero puede proporcionar capas de seguridad adicionales. Estas medidas ayudarán a mitigar la probabilidad de que un atacante que entra en el sistema pueda acceder a otros recursos más confidenciales mediante el desplazamiento lateral

Describir las técnicas de seguridad de autorización

Confianza cero

El término "Confianza cero" es habitual en ciberseguridad. Se trata de un método que mitiga los ataques cada vez más comunes que se producen hoy en día.

La Confianza cero es un modelo que permite a las organizaciones proporcionar acceso seguro a sus recursos, ya que nos enseña a "nunca confiar, siempre comprobar". Se basa en tres principios que emplean conceptos con los que ya está familiarizado.

- **Comprobar explícitamente**: con la Confianza cero, todas las solicitudes se autentican y autorizan por completo antes de conceder acceso. Las organizaciones pueden implementar la autenticación multifactor y el acceso condicional para asegurarse de que todas las solicitudes se comprueban explícitamente.
- **Usar el acceso con privilegios mínimos**: como ya se mencionó en esta unidad, el concepto de privilegios mínimos consiste en autorizar a un usuario solamente con los derechos mínimos que necesita. Esto limita los daños que puede hacer un usuario y reduce los desplazamientos laterales.
- **Asumir la vulneración:** al asumir que se ha producido o que se producirá una vulneración, una organización puede planear mejor los niveles de seguridad adicionales. Esto minimiza el radio de vulneración de un atacante y evita el desplazamiento lateral.

Al emplear un modelo de seguridad de Confianza cero, las organizaciones pueden adaptarse mejor a un área de trabajo distribuida moderna que proporciona acceso seguro a los recursos.

Resumen y recursos

La autenticación y la autorización seguras son una de las piedras angulares de la protección frente a las amenazas de ciberseguridad en el trabajo y en el hogar. Cuando se implementan correctamente, la autenticación y la autorización pueden ayudar a protegerse contra las personas malintencionadas, al mismo tiempo que se mantiene la confidencialidad de los datos y los recursos.

Como ya ha visto en este módulo, **la autenticación se centra en identificar correctamente a un usuario**. Ha aprendido que **la autenticación multifactor se basa en tres conceptos (algo que tiene, algo que forma parte de usted y algo que sabe)** para proporcionar un medio sólido para demostrar que es quien dice ser. Ha descubierto que los ciberdelincuentes aprovecharán cualquier oportunidad para obtener información que les permita suplantarle, desde el registro de claves hasta la ingeniería social. Por último, ha visto que **la autorización controla y limita a dónde pueden ir los usuarios y qué datos y recursos pueden** ver. Juntas, la autenticación y la autorización mejoran en gran medida la confidencialidad de los datos y reducen la probabilidad de que los datos acaben en las manos equivocadas.

Resumen y recursos

Ahora que ha completado este módulo, podrá realizar lo siguiente:

- Describir la autenticación
- Describir algunos de los ataques comunes basados en la autenticación
- Describir las técnicas de seguridad de autorización

Más información

- Microsof t Security, Compliance, and Identity Fundamentals
- Orden ejecutiva sobre la mejora de la ciberseguridad de la nación estadounidense

CONTENIDOS

1. DESCRIPCIÓN DE AMENAZAS, ATAQUES Y MITIGACIONES BÁSICOS DE CIBERSEGURIDAD
2. DESCRIPCIÓN DE LOS CONCEPTOS DE CRIPTOGRAFÍA
3. DESCRIPCIÓN DE LA AUTENTICACIÓN Y LA AUTORIZACIÓN EN CIBERSEGURIDAD
4. **DESCRIBIR LAS AMENAZAS DE RED Y LAS MITIGACIONES**
5. DESCRIPCIÓN DE LAS AMENAZAS BASADAS EN DISPOSITIVOS Y LOS CONTROLES DE SEGURIDAD
6. DESCRIPCIÓN DE AMENAZAS BASADAS EN APLICACIONES Y CÓMO PROTEGERSE FRENTE A ELLAS

DESCRIBIR LAS AMENAZAS DE RED Y LAS MITIGACIONES

Introducción

La necesidad de comunicar y compartir conocimientos ha estado con nosotros desde la primera vez que aprendimos a hacer marcas en una superficie. A medida que hemos crecido y hemos pasado de asentamientos a pueblos y ciudades, también lo ha hecho el tamaño de la red de comunicación necesaria para ayudar a compartir noticias e ideas. Desde un jinete que entregaba una carta a una ciudad vecina, hasta la invención del telegrama y, finalmente, Internet y el correo electrónico, **hemos construido redes más grandes y complejas. En la actualidad, el mundo es un lugar mucho más pequeño gracias a la red más grande del mundo, Internet.**

Proteger la red es esencial en el moderno mundo en línea de hoy en día, donde **la información es la nueva moneda de cambio.** Cada día, miles de ciberataques amenazan a las redes. En su mayor parte, estos ataques se frustran, pero de vez en cuando, los titulares de las noticias informan sobre un robo de datos.

DESCRIBIR LAS AMENAZAS DE RED Y LAS MITIGACIONES

Introducción

Aquí descubrirá los diferentes tipos de redes que existen, los medios por los que se conecta a ellas y cómo se mueven los datos en una red. Tendrá una idea de los tipos de ataques que los ciberdelincuentes utilizarán para entrar en una red, y de las herramientas disponibles para ayudarle a detenerlos.

Al final de este módulo, habrá obtenido información sobre cómo:

- Describir los conceptos básicos de las redes.
- Describir las amenazas a la seguridad de la red.
- Describir formas de proteger la red.
- Describir formas de conectarse y comunicarse de forma segura a través de una red.

Describir los distintos tipos de redes

En el mundo moderno actual, **las redes existen en todas partes. Las redes de inicio conectan su portátil, equipo, televisión, consola de juegos, smartphones, tabletas y dispositivos de Internet de las cosas (IoT). Esto les permite comunicarse entre sí y con Internet.**

En un negocio, ya sea una humilde organización que funciona en un garaje o empresas de mayor envergadura, las redes son la columna vertebral que les permite funcionar y compartir datos, ideas y recursos.

Las redes se utilizan para acceder a información de todo tipo, desde las fotos que comparte con sus amigos, hasta información confidencial como las transacciones bancarias y de tarjetas de crédito. La aplicación bancaria del dispositivo móvil usa varias redes para llegar al banco. A continuación, navegará por la red del banco para llegar a sus detalles.

Describir los distintos tipos de redes

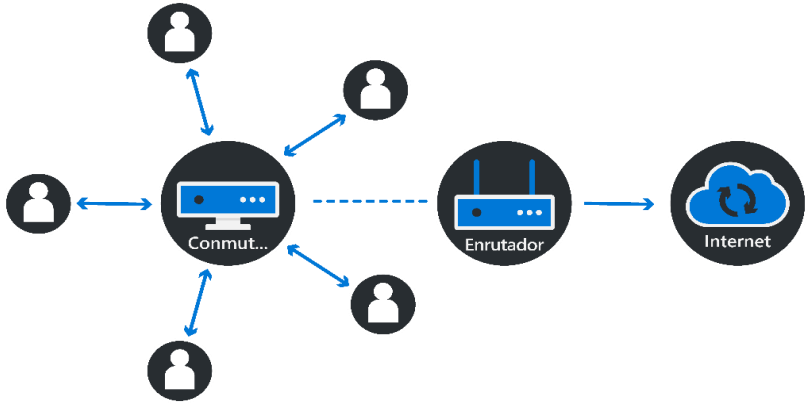
¿Qué es una red?

Una red es una agrupación de componentes físicos interconectados que funcionan juntos para proporcionar una columna vertebral sin fisuras para que todos sus dispositivos se comuniquen.

La nube e Internet pueden parecer intangibles, pero incluso tienen raíces físicas. Aunque hay docenas de **elementos que ayudan a definir una red**, los que es más probable que encuentre son: **enrutadores, conmutadores, firewalls, puntos de acceso y centros de conectividad.**

Aunque la mayoría de ellos quedan fuera del ámbito de esta unidad, hay dos que merecen ser destacados:

- El **conmutador** es el bloque de creación fundamental de una red moderna. Permite que varios dispositivos se comuniquen entre sí.
- El **enrutador** permite que distintas redes se comuniquen entre sí.



Describir los distintos tipos de redes

¿Qué es una red?

Es posible que haya oído hablar de diferentes tipos de redes, como redes inalámbricas y redes de área local.

Sin embargo, fundamentalmente, todas ellas entran en una de las dos categorías siguientes:

- Una **red privada** es aquella en la que se requiere un nivel de autenticación y autorización para acceder a dispositivos y recursos, como la puede encontrar en su lugar de trabajo.
- Una **red pública**, como Internet, está abierta a cualquier usuario.

Describir los distintos tipos de redes

Conexión a la red

Con independencia del tipo de red que use, existen varias maneras diferentes de conectarse a ella.

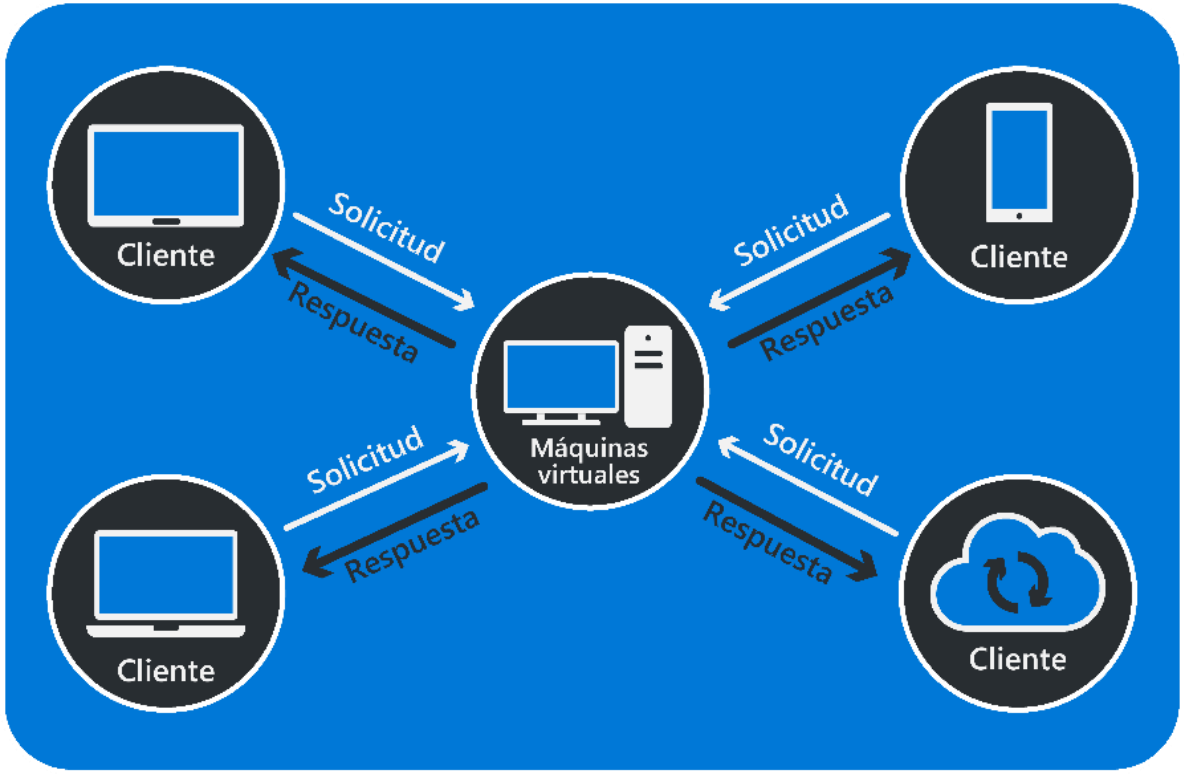
- La conexión **cableada** o **Ethernet** sigue siendo la manera más común de conectarse a la red de una oficina. Para ello, hace falta un cable de red físico para conectar el equipo de escritorio o portátil a un conmutador de la red.
- Una conexión **inalámbrica** permite que el dispositivo se conecte a la red mediante Wi-Fi. Se usa normalmente en casa o en grandes lugares públicos.
- Una conexión **Bluetooth** conecta un dispositivo de corto alcance al método de comunicación del dispositivo. Los dispositivos pequeños, como los podómetros, los auriculares y los relojes inteligentes, tienden a usar Bluetooth.

Describir los distintos tipos de redes

La topología cliente-servidor

Aunque las redes permiten que los dispositivos o las aplicaciones se comuniquen entre sí, una de las implementaciones de red más comunes se conoce como **topología cliente-servidor**.

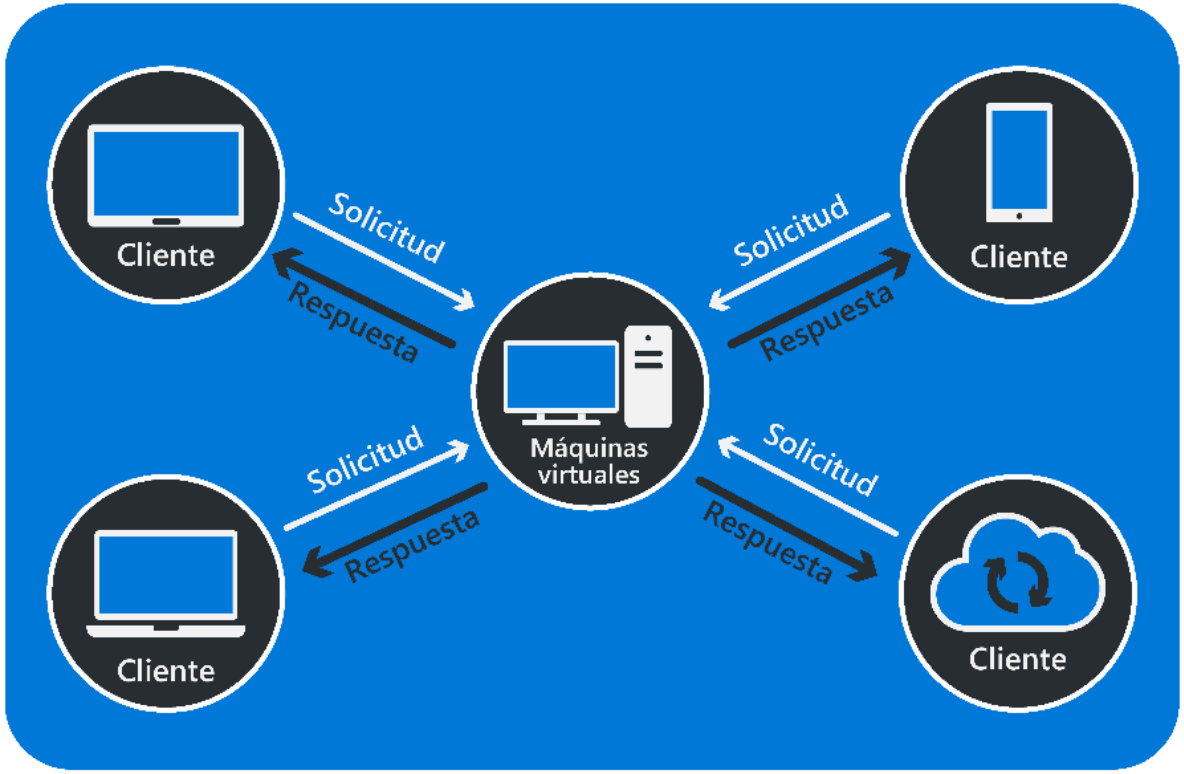
En este modelo, **el cliente puede ser uno o varios dispositivos o aplicaciones en un dispositivo que quiera hacer algo. El servidor es responsable de procesar cada solicitud de cliente y de devolver una respuesta.**



Describir los distintos tipos de redes

La topología cliente-servidor

Un ejemplo del modelo cliente-servidor es cuando se usa un smartphone o una tableta para acceder a un servicio de streaming digital. El dispositivo es el cliente, que realiza una solicitud al servidor de streaming para acceder al programa de televisión o a la película que quiere ver. El servidor responde transmitiendo el contenido al dispositivo. Otro ejemplo es cuando se usa el explorador para acceder al contenido desde Internet.



Descripción de cómo se mueven los datos por una red

Una red existirá cuando tenga dos o más dispositivos que compartan datos. Como se ha visto en la unidad anterior, una red se compone de muchas partes físicas diferentes que trabajan juntas para garantizar que los datos lleguen a donde se necesitan.

Esta transmisión de datos a través de una red está habilitada por un conjunto de protocolos de comunicación, a menudo denominado TCP/IP.

Se denomina por los dos protocolos principales: **el protocolo de control de transmisión (TCP), que controla la conexión entre dos dispositivos, y el protocolo de Internet (IP), que es responsable de enrutar la información a través de la red.**

Todas las redes del planeta comparten y mueven datos cada segundo del día. Estos datos pueden tener todo tipo de forma y tamaño, desde un simple mensaje hasta imágenes e incluso las películas que se transmiten a su hogar.

Descripción de cómo se mueven los datos por una red

El datagrama o paquete

Existen redes para facilitar la comunicación entre dispositivos o sistemas. **Sea cual sea el tamaño de los datos, todo debe dividirse en fragmentos pequeños y uniformes**. Estos fragmentos **se denominan datagramas**, pero también **se conocen más comúnmente como paquetes**.

Imagine que quiere transmitir una película al dispositivo. Dado el tamaño enorme de los datos implicados, el servidor de streaming no puede ofrecer toda la película de una sola vez.

En su lugar, la película se divide en miles de millones de paquetes. Cada paquete contiene una pequeña parte de la película, que se envía al dispositivo.

El dispositivo tiene que esperar hasta que se reciban suficientes paquetes para poder empezar a ver la película.

En segundo plano, el servidor sigue enviando un flujo constante de paquetes a su dispositivo

Descripción de cómo se mueven los datos por una red

El datagrama o paquete

Existen redes para facilitar la comunicación entre dispositivos o sistemas. **Sea cual sea el tamaño de los datos, todo debe dividirse en fragmentos pequeños y uniformes**. Estos fragmentos **se denominan datagramas**, pero también **se conocen más comúnmente como paquetes**.

Imagine que quiere transmitir una película al dispositivo. Dado el tamaño enorme de los datos implicados, el servidor de streaming no puede ofrecer toda la película de una sola vez.

En su lugar, la película se divide en miles de millones de paquetes. Cada paquete contiene una pequeña parte de la película, que se envía al dispositivo.

El dispositivo tiene que esperar hasta que se reciban suficientes paquetes para poder empezar a ver la película.

En segundo plano, el servidor sigue enviando un flujo constante de paquetes a su dispositivo justo antes de lo que se muestra. Si la velocidad de red se ralentiza, es posible que los paquetes no lleguen a tiempo. Es posible que la imagen que vea se desvirtúe o bloquee y que haya lagunas en el sonido.

Descripción de cómo se mueven los datos por una red

Direcciones IP

Cuando quiera enviar una carta a un amigo, primero escribirá la carta antes de meterla en un sobre. A continuación, escribirá la dirección de su amigo en el sobre antes de enviarla. El servicio postal lo recoge y, después de pasar por varias oficinas de clasificación, finalmente se entrega.

Las redes funcionan de forma similar. El mensaje está contenido en el paquete, como un sobre. A continuación, se agregan al paquete las direcciones del remitente y del destinatario.

La función principal del protocolo de Internet (IP) es asegurarse de que todos los dispositivos de una red se puedan identificar de forma única. Para que un paquete se pueda enviar a través de la red, se le debe decir la dirección IP a dónde va y la dirección IP de dónde procede.

Actualmente **hay dos estándares de dirección IP denominados IPv4 e IPv6.** Los detalles están fuera del ámbito de este módulo, pero el tipo más común de dirección IP y con el que puede estar familiarizado es IPv4. Se trata de cuatro grupos de dígitos separados por un punto, por ejemplo: 127.100.0.1.

Descripción de cómo se mueven los datos por una red

DNS

Al igual que todos los dispositivos de una red necesitan una dirección IP única, cada sitio web de acceso público necesita su propia dirección IP. Podría usar la dirección IP para visitar su tienda, banco o servicio de vídeo de streaming en línea favoritos. Pero con tantos sitios web disponibles, esto sería difícil de recordar. En su lugar, puede escribir el nombre del servicio que busca en el explorador y este le llevará al sitio web que quiera. Todo esto es gracias al **servicio de nombres de dominio o DNS.**

El DNS contiene una tabla con el nombre del sitio web; por ejemplo, microsoft.com, **que se asigna a su dirección IP correspondiente.** El explorador lo usa para encontrar el sitio web real de la misma manera que podría usar una libreta de teléfono para buscar un número de teléfono.

Cada vez que el dispositivo se conecta a Internet, usa un servidor DNS local para encontrar el nombre del sitio web que está buscando. Si el DNS no encuentra el sitio, comprueba otros servidores DNS. Si no se encuentra el sitio o se agota el tiempo de espera de la solicitud, recibirá un mensaje de error como "El servidor DNS no responde".

Descripción de cómo se mueven los datos por una red

Enrutamiento

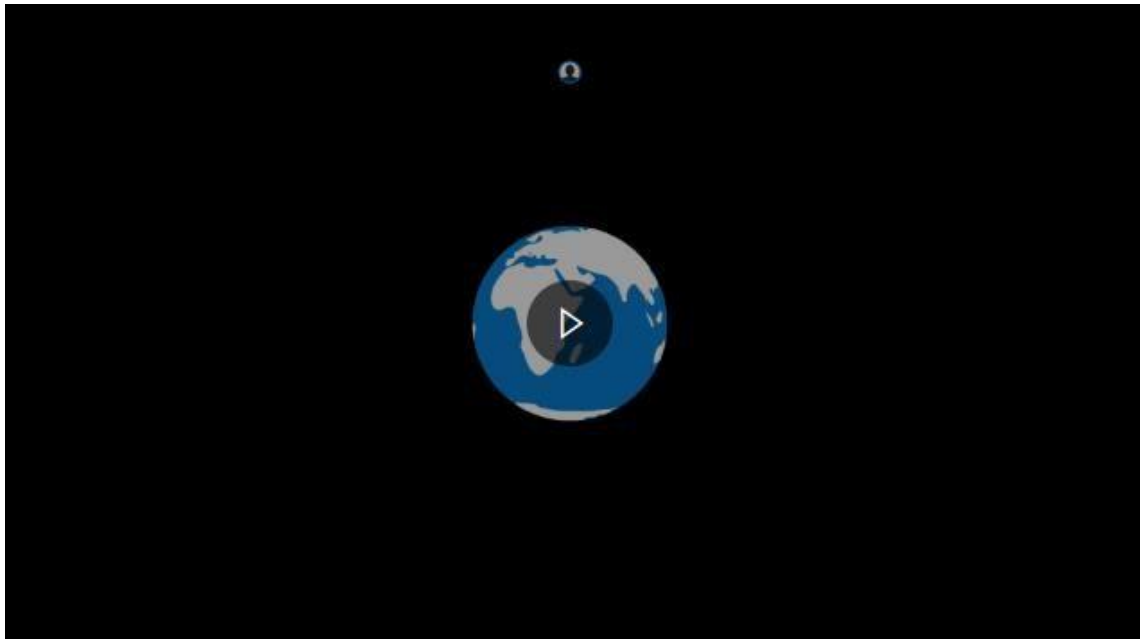
Cuando se han agregado las direcciones IP al paquete, ya se puede transmitir a través de la red. Si la dirección IP existe en la red, el paquete se envía directamente al dispositivo. Sin embargo, si la dirección IP está fuera de la red, tendrá que pasar por un enrutador. **Un enrutador es un dispositivo físico que conecta una red a otra.**

Siguiendo con nuestro ejemplo de la carta, si su amigo solo estuviera a unas cuantas calles de distancia, podría decidir entregar el mensaje en mano. Su amigo está dentro de la red local.

Sin embargo, si su amigo está en otra ciudad, país o región, deberá enviarlo y dejar que el servicio postal lo entregue. En este caso, el servicio postal es **el enrutador. Toma el mensaje de la red y**, a continuación**, busca la mejor ruta para llegar a la red de su amigo para su entrega.**

Descripción de cómo se mueven los datos por una red

En este breve vídeo de dos minutos, verá cómo las actividades diarias crean redes, desde hablar con sus amigos por teléfono hasta compartir correos electrónicos. A continuación, veremos cómo se desglosan los mensajes en paquetes que se pueden enviar a través de la red. Por último, verá cómo cada paquete de un mensaje se enruta a través de Internet para llegar a su destinatario.



Descripción de las amenazas a la seguridad de la red

Las redes son la columna vertebral de nuestro mundo moderno, ya que nos permiten comunicarnos, comprar, jugar y trabajar desde cualquier lugar. Permiten acceder a una gran cantidad de información no solo sobre nosotros mismos, sino también de las empresas.

Esto las convierte en un objetivo principal para los ciberdelincuentes que ven la información como la nueva moneda de cambio. Una seguridad de red débil corre el riesgo de exponer los datos críticos sensibles y de dañar la confidencialidad, la disponibilidad y la integridad de los datos almacenados.

Comprender las amenazas es una parte fundamental de la creación de una red de seguridad fuerte.

Descripción de las amenazas a la seguridad de la red

Ataques de red comunes

Las formas en que se pueden atacar las redes son demasiado numerosas como para detallarlas aquí. Veamos las más comunes:

- **Ataques de tipo "Man in the middle" o "eavesdropping"**: este tipo de ataque puede producirse cuando los ciberdelincuentes comprometen o emulan rutas en la red, lo que les permite interceptar los paquetes de información. Se podría considerar como una forma de intervención telefónica. Los atacantes no solo roban datos, sino que ponen en peligro la integridad de estos.
- **Ataques de denegación de servicio distribuido (DDoS)**: el objetivo de un ataque DDoS es poner en peligro la disponibilidad de la red o del servicio de destino. Lo que hacen los atacantes es bombardear la red o el servicio objetivo con millones de peticiones simultáneas, procedentes de orígenes distribuidos por toda la red, lo que hace que se desborde y provoque su caída.

Descripción de las amenazas a la seguridad de la red

Ataques de red comunes

En este breve vídeo, verá una simulación de cómo funciona cada uno de estos ataques. En el caso del ataque de tipo "Man in incluso decenas de millones de equipos. Una vez más, por motivos de simplicidad, solo se muestran unos pocos.the middle", hemos elegido usar solo una ruta para simplificarlo. Con el ataque DDoS, se usan cientos de miles o incluso decenas de millones de equipos. Una vez más, por motivos de simplicidad, solo se muestran unos pocos.

Descripción de las amenazas a la seguridad de la red

Ataque DNS común

Un ataque DNS busca aprovechar los puntos débiles del servidor DNS, ya que estos servidores están diseñados para mejorar la eficacia y la facilidad de uso, y no con la seguridad en mente.

Un ataque DNS común es el **envenenamiento de DNS**. En este tipo de ataque **el atacante cambia las direcciones IP de las tablas de búsqueda DNS para desviar el tráfico de un sitio legítimo y dirigirlo a un sitio ilegítimo** que puede contener vínculos malintencionados u otro malware.

Descripción de las amenazas a la seguridad de la red

Ataques inalámbricos comunes

Las redes inalámbricas permiten que nuestros dispositivos se conecten fácilmente a redes de todas partes.

En su casa, la red inalámbrica permite que su smartphone y sus dispositivos IoT siempre activos se conecten a Internet.

La amplia disponibilidad de estas redes las convierte en el objetivo perfecto para los ciberdelincuentes. Hay muchas maneras diferentes de atacar una red inalámbrica:

- **Wardriving**
- **Suplantación de zonas Wi-Fi**
- **Ataque Bluetooth**

Descripción de las amenazas a la seguridad de la red

Ataques inalámbricos comunes

- **Wardriving**: este término se popularizó en un par de películas de los 80. **El atacante**, que normalmente trabaja desde un vehículo, **busca redes inalámbricas no seguras que tengan vulnerabilidades**. La mayoría de los ataques de "wardriving" buscan usar la red para actividades delictivas, como la piratería de otros equipos y el robo de información personal.
- **Suplantación de zonas Wi-Fi**: es parecido a un ataque de tipo "Man in the middle". **El atacante usa su portátil o un dispositivo conectado a él para ofrecer un punto de acceso de red que imita un punto de acceso original**. Por ejemplo, si está en una cafetería y quiere acceder a Internet mediante su Wi-Fi de invitado, es posible que vea un par de puntos de acceso que tienen el nombre de la cafetería. Pero puede ocurrir que uno de ellos proceda de un actor malintencionado. Una vez que se haya conectado al punto de acceso falso, todo lo que haga a través de la red se puede interceptar. También permite que el ciberdelincuente le dirija a sitios web poco seguros o capture sus datos privados.

Descripción de las amenazas a la seguridad de la red

Ataques inalámbricos comunes

- **Ataque Bluetooth**

  Se ha producido un crecimiento de los dispositivos Bluetooth, desde los relojes inteligentes y los dispositivos de audio hasta la comunicación entre dispositivos. Los ataques a las redes Bluetooth son menos comunes que los que sufren las redes inalámbricas, principalmente porque el atacante debe estar dentro del alcance del dispositivo, pero sigue siendo un vector de ataque válido. Un ataque **bluejacking** es donde **un atacante envía mensajes no solicitados a cualquier dispositivo que tenga habilitado el Bluetooth y que esté dentro de su alcance.** El ataque de tipo Bluejacking es similar a cuando alguien llama a la puerta y, a continuación, se marcha antes de que pueda responder. Es principalmente molesto.

Protección de su red

La protección de redes es una parte esencial de una directiva de seguridad sólida. Como vimos en la unidad anterior, hay muchas maneras de atacar una red. No existe una solución única que proteja su red; sin embargo, la mayoría de estos ataques pueden mitigarse mediante una combinación de soluciones de hardware y software.

Cómo un firewall protege la red

Un firewall suele ser la primera línea de defensa de la red. Se trata de un dispositivo que se encuentra entre Internet y la red, y filtra todo el tráfico que sale y entra. Un firewall puede estar basado en software o hardware, pero para obtener la mejor protección, es recomendable tener ambos tipos. Un firewall supervisa el tráfico entrante y saliente. **Mediante el uso de reglas de seguridad, mantendrá fuera el tráfico no deseado, al tiempo que permitirá que el tráfico autorizado pase libremente**.

Protección de su red

Mantenimiento de una red en buen estado mediante un antivirus

Los virus vienen en todas las formas y tamaños y ninguno de ellos es bueno para los dispositivos y servidores que utilizan su red. Los ciberdelincuentes pueden utilizarlos con muchos fines, desde obtener las credenciales de los usuarios para poder acceder a su red, hasta tipos más dañinos que cifran todos los datos de un dispositivo o servidor a menos que se paguen grandes sumas de dinero. Igual que el cuerpo lucha contra un virus cuando se infecta**, los equipos también pueden protegerse utilizando un software antivirus.** Una vez instalado el software antivirus, se ejecuta en segundo plano y analiza todos los datos que llegan al dispositivo. Un virus detectado se eliminará automáticamente para evitar que el usuario lo ejecute accidentalmente.

Ahora puede tener un antivirus en la mayoría de sus dispositivos, incluidos servidores, equipos, tabletas, smartphones y cualquier otro dispositivo conectado a Internet.

Protección de su red

Mejora de la autenticación mediante el control de acceso de red

Aunque un firewall impide que los dispositivos no deseados accedan a la red, todavía necesita controlar los que quiere usar. **El control de acceso a la red (NAC) es una solución de seguridad que controla el acceso de dispositivos y usuarios mediante la aplicación de directivas estrictas**.

Las directivas de dispositivo controlan lo que se puede hacer en la red y limitan lo que hace el usuario en un dispositivo.

A través de NAC, puede mejorar la seguridad al solicitar que todos los usuarios usen la autenticación multifactor para iniciar sesión en la red. NAC le permite definir los dispositivos y usuarios que pueden acceder a los recursos de red, lo que reduce las amenazas y detiene el acceso no autorizado.

Protección de su red

División de la red en partes

Cada habitación de su casa tiene un propósito diferente, como la cocina, el salón, la sala de estar, el estudio, las habitaciones y los baños. Puede controlar el acceso a cada una de estas estancias colocando cierres digitales en todas las puertas. Cuando llegue un invitado, puede darle una llave que le permita acceder a estancias específicas de su casa. Puede hacer el mismo tipo de cosas con la red mediante el concepto de segmentación de red.

La segmentación de la red crea límites en torno a las operaciones o recursos críticos, de la misma manera que pondría a su equipo de finanzas en su propia oficina. Esto mejora la integridad de los recursos de red al garantizar que, incluso si se accede a la red de forma maliciosa, el atacante no pueda llegar a las áreas segmentadas.

Protección de su red

Protección de las conexiones mediante una red privada virtual

Una red privada virtual o VPN sirve de conexión dedicada y segura a través de Internet, entre un dispositivo y un servidor. Una conexión VPN cifra todo el tráfico de Internet y, luego, lo oculta para que sea imposible conocer la identidad del dispositivo original.

Este tipo de conexión segura dificulta que los ciberdelincuentes realicen un seguimiento de sus actividades y obtengan datos. Si alguna vez se ha conectado a la red de trabajo desde una zona Wi-Fi pública, como el aeropuerto, lo más probable es que haya usado una VPN.

La VPN establece una conexión segura a través de una red pública no segura. Los proveedores de VPN se han vuelto muy comunes no solo para escenarios de trabajo remotos, sino también para uso personal.

Protección de su red

Cifrado de la red inalámbrica

Tanto si configura un punto de acceso inalámbrico en su hogar como en su lugar de trabajo, la habilitación del cifrado es fundamental para protegerse de los ataques. **El acceso protegido Wi-Fi 2 o WPA2 es el método de cifrado Wi-Fi que se usa de forma más habitual.** Emplea el Estándar de cifrado avanzado (AES) para proteger la conexión.

Resumen y recursos

Las redes constituyen la columna vertebral de nuestro mundo conectado digitalmente. También representan un punto de entrada para los ciberataques.

En este módulo, hemos mostrado los distintos tipos de red que existen y cómo se conectaría a ellas. Ha aprendido los conceptos básicos de la comunicación de red y cómo los datos se mueven por una red de cualquier tamaño. Asimismo, ya se ha hecho una idea de las muchas formas que un ciberdelincuente puede usar para intentar entrar en una red, y de las herramientas disponibles para detenerlo.

Cuando haya completado este módulo, sabrá cómo:

- *Describir los conceptos básicos de las redes.*
- *Describir las amenazas a la seguridad de la red.*
- *Describir formas de proteger la red.*
- *Describir formas de conectarse y comunicarse de forma segura a través de una red.*

CONTENIDOS

1. DESCRIPCIÓN DE AMENAZAS, ATAQUES Y MITIGACIONES BÁSICOS DE CIBERSEGURIDAD
2. DESCRIPCIÓN DE LOS CONCEPTOS DE CRIPTOGRAFÍA
3. DESCRIPCIÓN DE LA AUTENTICACIÓN Y LA AUTORIZACIÓN EN CIBERSEGURIDAD
4. DESCRIBIR LAS AMENAZAS DE RED Y LAS MITIGACIONES
5. **DESCRIPCIÓN DE LAS AMENAZAS BASADAS EN DISPOSITIVOS Y LOS CONTROLES DE SEGURIDAD**
6. DESCRIPCIÓN DE AMENAZAS BASADAS EN APLICACIONES Y CÓMO PROTEGERSE FRENTE A ELLAS

DESCRIPCIÓN DE LAS AMENAZAS BASADAS EN DISPOSITIVOS Y LOS CONTROLES DE SEGURIDAD

Introducción

En nuestro mundo moderno, las personas y las organizaciones confían en los dispositivos conectados para satisfacer sus necesidades diarias más vitales. **Los dispositivos acceden y almacenan datos empresariales y personales importantes a la vez que recopilan continuamente información sobre nosotros**.

Como resultado, **los ciberdelincuentes tienen como destino dispositivos con el fin de obtener acceso y control no autorizados** de datos valiosos, lo que crea estragos para usuarios y organizaciones. En este módulo, aprenderá a protegerse contra ciberataques basados en dispositivos para proteger los datos y mitigar el impacto en personas y organizaciones.

Al término de este módulo, sabrá hacer lo siguiente:

- *Descripción de lo que el dispositivo sabe de usted.*
- *Descripción de cómo los dispositivos se convierten en amenazas de ciberseguridad.*
- *Descripción de cómo mitigar las amenazas relacionadas con el dispositivo.*

Descripción de lo que el dispositivo sabe de usted

Los dispositivos son una parte importante del día a día y dependemos de ellos para muchas cosas. **Para llevar a cabo su trabajo de forma eficaz, los dispositivos deben capturar, almacenar y compartir todo tipo de información confidencial sobre nosotros.** Es posible que no nos demos cuenta de la medida en que usamos algunos dispositivos. Se han vuelto casi invisibles para nosotros. Con el fin de proteger la información confidencial a la que tienen acceso nuestros dispositivos, debemos tener en cuenta cómo los estamos usando, independientemente de si es de forma consciente o subconsciente.

¿Qué son los dispositivos?

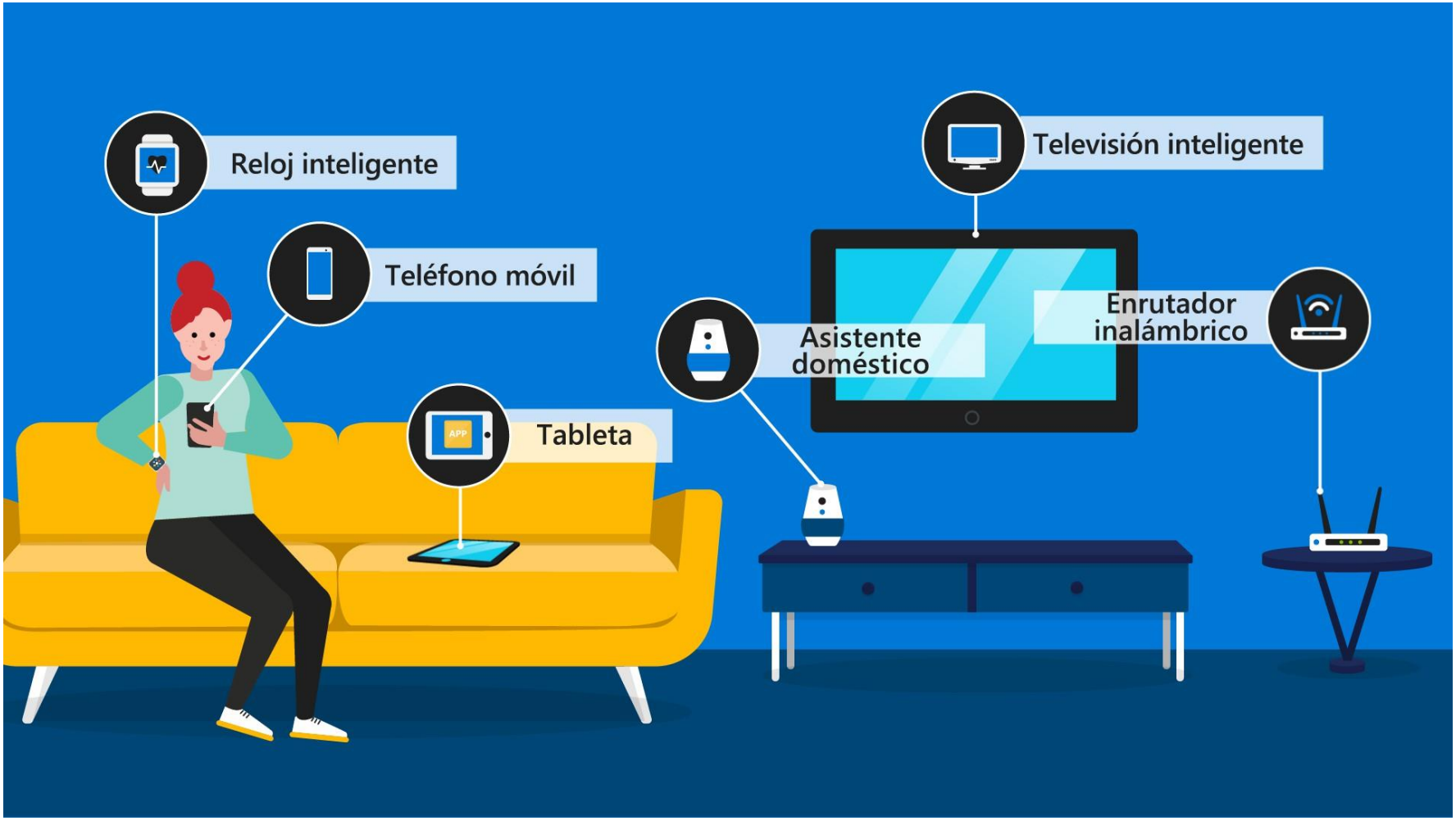
Cuando escucha hablar de "dispositivos", ¿qué es lo primero que se le viene a la mente? Probablemente piense en los que está familiarizado, como **el teléfono, un portátil o una tableta**. Los dispositivos abarcan mucho más que esto. Por ejemplo:

- **Unidades USB.**
- **Cualquier dispositivo conectado a la red doméstica, incluidos dispositivos de asistencia doméstica siempre conectados, impresoras, televisiones, dispositivos, cámaras de puerta, impresoras, etc.**
- **Paneles de automóviles, incluido el sistema de navegación y el control de voz.**
- **Zonas Wi-Fi.**

Desde nuestras casas hasta nuestras oficinas y en todas partes, entramos en contacto con los dispositivos.

Descripción de lo que el dispositivo sabe de usted

Echemos un vistazo a Kayla. En su casa está rodeada de dispositivos como su teléfono, un asistente para el hogar siempre activo, una tableta, un reloj inteligente, un enrutador inalámbrico, etc.



Descripción de lo que el dispositivo sabe de usted

Kayla usa su coche para empezar a trabajar. Su automóvil tiene dispositivos integrados que puede usar mientras conduce, como el sistema de navegación y el punto de acceso inalámbrico que permite que su automóvil sirva como zona con cobertura inalámbrica móvil.

Descripción de lo que el dispositivo sabe de usted

En el trabajo, el teléfono móvil y el equipo de Kayla se conectan de forma inalámbrica a la red de su organización para acceder a los recursos corporativos, incluida una impresora. También usa una unidad USB para almacenar determinados archivos y presentaciones.

Descripción de lo que el dispositivo sabe de usted

En el contexto de ciberseguridad, todo lo que pueda tocar o con lo que pueda interactuar y que también pueda conectarse a otra cosa se considera un dispositivo. Es posible que esté usando un dispositivo conscientemente, como cuando usa el teléfono o cuando inserta una unidad USB en el portátil. O es posible que no se dé cuenta de que está usando un dispositivo porque una conexión se produce automáticamente, como cuando el teléfono se conecta a una zona Wi-Fi o porque lo configura una vez y luego se olvida de él, como el enrutador de la red doméstica.

Lo importante aquí es que debemos expandir lo que nos viene a la mente cuando pensemos en los dispositivos. Es importante hacerlo, ya que, en el contexto de ciberseguridad, todos ellos se pueden considerar vectores de amenazas, destinos para ciberdelincuentes que quieren causar daños.

Descripción de lo que el dispositivo sabe de usted

Dispositivos y datos

¿Por qué los dispositivos son una parte integral de nuestra vida? En gran medida, se debe a que recopilan y almacenan información, y nos mantienen conectados a otros dispositivos y servicios.

Piense en la comodidad de recibir información de tráfico en tiempo real en el teléfono móvil o en la molestia cuando llegan anuncios al dispositivo en función del historial de búsqueda en Internet. Este tipo de contenido de destino se envía porque nuestros dispositivos, a través de sus aplicaciones, recopilan enormes cantidades de información sobre nosotros. Esto incluye detalles de ubicación, sitios web visitados, cuánto tiempo permanecemos en un sitio y mucho más.

Los dispositivos conectados también nos permiten acceder fácilmente a la información y compartirla. Por ejemplo, probablemente haya usado el teléfono móvil para compartir fotos familiares con sus amigos, acceder a un documento de trabajo o pagar por algo en una tienda.

Tanto si usa el dispositivo por motivos personales como laborales, o ambos, la información accesible suele ser confidencial y privada. **Los ciberdelincuentes lo saben e intentan poner en peligro los dispositivos como medio para acceder a los datos.**

Descripción de lo que el dispositivo sabe de usted

Ha aprendido que estamos rodeados de dispositivos y que estos contienen todo tipo de información personal. También ha visto que los ciberdelincuentes se dirigirán a los dispositivos para obtener esta información. Pero ¿cómo lo hacen?

Dispositivos como vectores de amenazas

Aunque los dispositivos nos ayudan a realizar nuestro trabajo y nuestra vida diaria, también presentan oportunidades a los ciberdelincuentes que quieren causar daños. Esto se debe a que son vectores de amenazas: proporcionan diferentes formas en que los ciberdelincuentes pueden llevar a cabo ataques. Por ejemplo:

- **Teléfono, portátil o tableta: la descarga de una aplicación malintencionada puede dar lugar a que el dispositivo esté contaminado con malware que puede filtrar datos confidenciales almacenados localmente, sin el conocimiento del usuario**. Esto pone en peligro la confidencialidad y la integridad porque el ciberdelincuente ahora puede ver o modificar los datos.
- **Unidades USB**: los ciberdelincuentes **pueden colocar software o archivos malintencionados en una unidad USB e insertarlo en un dispositivo como un portátil**. Por ejemplo, la unidad podría ejecutar ransomware, lo que significa que la disponibilidad de los datos se ha puesto en peligro porque está bloqueada a cambio de un rescate.

Descripción de lo que el dispositivo sabe de usted

Dispositivos como vectores de amenazas

- **Dispositivos de asistencia para el hogar siempre en marcha**: estos dispositivos siempre escuchan u observan. Un ciberdelincuente **puede colocar software malintencionado en las tiendas de aplicaciones para estos dispositivos.** Si un usuario lo instala, el ciberdelincuente podría, por ejemplo, atacar el dispositivo con spyware para grabar información de forma secreta y poner en peligro la confidencialidad de los datos. También podrían moverse lateralmente a otros dispositivos del hogar y poner en peligro sus datos.

Echemos un vistazo al siguiente vídeo para ver cómo los dispositivos que nos rodean pueden convertirse en vectores de amenazas:

Descripción de lo que el dispositivo sabe de usted

Vulnerabilidades del dispositivo

Un dispositivo puede verse comprometido debido a un estado deficiente, ya sea porque no tiene las actualizaciones de seguridad más recientes o porque tiene una autenticación débil.

Si conecta este tipo de dispositivo a una zona Wi-Fi, por ejemplo, en un aeropuerto, es un objetivo fácil para los atacantes. Conocen las vulnerabilidades comunes de los dispositivos y las aplicaciones, así como la forma de obtener acceso no autorizado.

Una vez que un atacante consigue el acceso, puede ejecutar scripts para instalar malware.

En la mayoría de los casos, el malware como puertas traseras o redes de robots (botnets) puede persistir en el dispositivo incluso después de actualizarlo. Esto provoca un daño mayor cuando un usuario conecta el dispositivo infectado a una red doméstica o de trabajo.

Descripción de lo que el dispositivo sabe de usted

Vulnerabilidades del dispositivo

Algunos usuarios quieren obtener más control de sus dispositivos para la personalización u otros fines, y podrían recurrir al *jailbreaking*.

Aquí es donde un usuario encuentra formas no oficiales de obtener acceso total a los sistemas principales de un dispositivo. El dispositivo se vuelve vulnerable porque esta acción podría sortear las medidas de seguridad.

Esto ofrece a los ciberdelincuentes la oportunidad de proporcionar instrucciones falsas o software que ponga en peligro el dispositivo.

Cualquier dispositivo conectado puede ser un vector de amenaza si no está protegido correctamente.

Una vez aprendido esto, podemos pensar en las distintas formas de proteger nuestros dispositivos.

Descripción de cómo mitigar las amenazas relacionadas con el dispositivo

Hemos aprendido que los dispositivos pueden ser vectores de amenazas para los ciberdelincuentes que quieren obtener acceso o control de los datos para causar daños. Pero ¿qué podemos hacer para protegernos?

Medidas de mitigación

Hay diferentes maneras de proteger los dispositivos y los datos. Echemos un vistazo a algunas de las más comunes:

Protección de dispositivos

Cifrado

Limitación del acceso al dispositivo de la aplicación

Descripción de cómo mitigar las amenazas relacionadas con el dispositivo

Medidas de mitigación

Protección de dispositivos

La protección de dispositivos es la forma en que se minimiza la posibilidad de que se puedan aprovechar las vulnerabilidades del dispositivo. Puede usar los siguientes métodos:

- *Asegúrese de que los dispositivos tienen las actualizaciones de seguridad más recientes.*
- *Apague los dispositivos no usados.*
- *Habilite las características de seguridad admitidas a través del sistema operativo del dispositivo.*
- *Requiera PIN o biometría (como el reconocimiento facial) para acceder a los dispositivos.*

Muchos sistemas operativos modernos tienen funcionalidades que admiten la protección de dispositivos. Por ejemplo, los usuarios pueden habilitar las actualizaciones automáticas del sistema operativo para ayudar a protegerse frente a vulnerabilidades conocidas y garantizar la disponibilidad continua del dispositivo. Las actualizaciones también admiten características de seguridad como la protección contra virus y amenazas, y la funcionalidad de firewall.

Estas características se habilitan fácilmente y pueden ayudar a proteger el dispositivo conectado para mantener la confidencialidad y la integridad de los datos accesibles.

Descripción de cómo mitigar las amenazas relacionadas con el dispositivo

Medidas de mitigación

Cifrado

El cifrado es un proceso que convierte la información del dispositivo en datos ininteligibles. La única manera de que esta información sea útil es invertir el cifrado. Esto requiere una contraseña o clave específica que solo está disponible para el usuario autorizado. Una vez cifrada la información, deja de ser útil sin la clave o contraseña correctas. De este modo, se mantiene la confidencialidad de los datos.

El contenido de un dispositivo se puede cifrar de diversas maneras. Por ejemplo, algunos sistemas operativos incluyen herramientas integradas que le permiten cifrar la unidad de disco duro del equipo o cualquier dispositivo de almacenamiento al que se conecte.

Descripción de cómo mitigar las amenazas relacionadas con el dispositivo

Medidas de mitigación

Limitación del acceso al dispositivo de la aplicación

Hasta ahora, hemos visto las distintas formas en que las aplicaciones y los dispositivos podrían verse comprometidos y los pasos que puede seguir para mitigar las amenazas.

Pero uno de los vectores de ataque más pasados por alto es cuando alguien usa directamente las aplicaciones en el dispositivo físico.

Supongamos que ha dejado el smartphone en el escritorio y se apresuró para ir a una reunión urgente. Una persona con malas intenciones podría usar el teléfono para acceder a cualquiera de las aplicaciones. Podría enviar mensajes, acceder a cuentas bancarias y realizar compras, todo ello mediante el uso de aplicaciones desde el dispositivo. Si es inteligente, dejará el dispositivo donde lo encontró, por lo que nunca lo sabrá.

Esta amenaza también se aplica al equipo de trabajo. Supongamos que está ocupado trabajando en datos importantes y confidenciales y se aleja del equipo para tomar un café. Un delincuente podría usar ahora el equipo no seguro para buscar datos confidenciales o secretos, o descargarlos en una unidad USB.

Descripción de cómo mitigar las amenazas relacionadas con el dispositivo

Medidas de mitigación

Limitación del acceso al dispositivo de la aplicación

En estos dos casos, todo lo que haga el actor malintencionado se registrará y se realizará un seguimiento en su nombre. Hay pocas probabilidades de que se haga un seguimiento de las acciones para llegar hasta el actor malintencionado, y usted tendrá que afrontar las consecuencias y la limpieza.

La mejor manera de limitar el acceso a las aplicaciones es asegurarse de que se cierran o protegen cuando no se usan. Para ello, bloquee el dispositivo cuando se aparte de él. Si el dispositivo es lo suficientemente pequeño, lléveselo.

Resumen y recursos

Ha aprendido que **los dispositivos pueden ser la clave para la información fundamental sobre individuos y organizaciones**, y que **los ciberdelincuentes tienen como destino los dispositivos para obtener acceso no autorizado a los datos.** Los ciberdelincuentes usan diversos medios para poner en peligro los dispositivos. Si se protegen los datos, se protegen las personas y las organizaciones. Ha aprendido a proteger los dispositivos a través de medidas de ciberseguridad que le ayudan a lograr y mantener la confidencialidad, la integridad y la disponibilidad de los datos.

Ahora que ha completado este módulo, podrá realizar lo siguiente:

- *Descripción de lo que el dispositivo sabe de usted.*
- *Descripción de cómo los dispositivos se pueden convertir en amenazas de ciberseguridad.*
- *Descripción de cómo mitigar las amenazas relacionadas con el dispositivo*

CONTENIDOS

1. DESCRIPCIÓN DE AMENAZAS, ATAQUES Y MITIGACIONES BÁSICOS DE CIBERSEGURIDAD
2. DESCRIPCIÓN DE LOS CONCEPTOS DE CRIPTOGRAFÍA
3. DESCRIPCIÓN DE LA AUTENTICACIÓN Y LA AUTORIZACIÓN EN CIBERSEGURIDAD
4. DESCRIBIR LAS AMENAZAS DE RED Y LAS MITIGACIONES
5. DESCRIPCIÓN DE LAS AMENAZAS BASADAS EN DISPOSITIVOS Y LOS CONTROLES DE SEGURIDAD
6. **DESCRIPCIÓN DE AMENAZAS BASADAS EN APLICACIONES Y CÓMO PROTEGERSE FRENTE A ELLAS**

DESCRIPCIÓN DE AMENAZAS BASADAS EN APLICACIONES Y CÓMO PROTEGERSE FRENTE A ELLAS

Introducción

En el mundo conectado digitalmente de **hoy en día, hay una aplicación para prácticamente cualquier cosa**. Las aplicaciones influyen en muchos aspectos de la vida cotidiana y les dan forma, lo que incluye la manera en que se interactúa con los amigos, cómo se trabaja, qué bienes y servicios se adquieren y de qué forma, cómo se aprende e, incluso, a qué se dedica el tiempo libre. Dado que las aplicaciones desempeñan un papel tan importante en la vida personal y profesional, son un atractivo objetivo para los ciberdelincuentes, que intentan aprovechar cualquier oportunidad.

Aquí aprenderá a describir **qué son las aplicaciones**, en relación con otros tipos de software, y **cómo pueden convertirse en vectores de ataque para los ciberdelincuentes**. También verá los pasos que puede seguir para reducir el riesgo y tener la certeza de que las aplicaciones que usa son seguras.

Después de completar este módulo, podrá:

- *Describir qué son las aplicaciones.*
- *Describir el panorama de amenazas de aplicaciones.*
- *Describir los controles de seguridad basados en aplicaciones comunes.*

Describir qué son las aplicaciones

Hoy en día, muchos hablamos de aplicaciones incluso en nuestras conversaciones más informales. ¿Pero sabemos realmente qué es una aplicación? Para entender mejor cómo pueden las aplicaciones convertirse en vectores de ataque para ciberdelincuentes, primero es necesario identificar lo que ellas saben sobre nosotros.

¿Qué es el software?

El *software* es una colección o un conjunto de comandos en forma de código que indica a un equipo o dispositivo que realice algún tipo de trabajo. El software se ejecuta en el *hardware* (componentes físicos) de un dispositivo. En términos generales, el software puede ser de **dos tipos:**

- *Software del sistema*
- *Software de aplicación*

Describir qué son las aplicaciones

¿Qué es el software?

Software del sistema

El *software del sistema* es lo primero que se ejecuta al encender el dispositivo y administra los distintos componentes que hacen que funcione. También crea un marco que permite a las aplicaciones ejecutarse correctamente y mitigar problemas cuando dejan de funcionar.

El software del sistema se caracteriza por lo siguiente:

- *Controla o facilita el hardware y los procesos de un sistema, como el teclado, el mouse, la red y el vídeo.*
- *Se puede ejecutar de forma independiente.*
- *Normalmente se ejecuta en segundo plano.*

Por ejemplo, el sistema operativo y utilidades como el antivirus y el firewall son todos software del sistema.

El software del sistema es un área grande y compleja, y queda fuera del ámbito de esta unidad. Pero merece la pena tener en cuenta que **el software del sistema también puede ser el objetivo de los ataques de los ciberdelincuentes.**

Describir qué son las aplicaciones

¿Qué es el software?

Software de aplicación

El *software de aplicación*, también conocido como aplicaciones, está diseñado con un propósito específico. Incluye el procesamiento de texto, hojas de cálculo, correo electrónico y mensajería instantánea, por nombrar algunos. Estas aplicaciones están diseñadas para funcionar en instancias concretas de software del sistema, y la mayoría están disponibles en los sistemas más populares.

El software de aplicación se caracteriza por lo siguiente:

- *Realiza un trabajo especializado, como el procesamiento de texto, la edición de vídeo y la mensajería.*
- *Estar diseñado para que el usuario interactúe directamente con él.*
- *Normalmente no se ejecuta de forma independiente y necesita al software del sistema.*
- *Debe ser instalado por un usuario.*

Describir qué son las aplicaciones

¿Qué es el software?

Software de aplicación

Los procesadores de texto, las aplicaciones de correo electrónico, los exploradores de Internet y los editores de imágenes son ejemplos de software de aplicación. Estamos usando software de aplicación más que nunca para hacer todo tipo de cosas, por lo que ahora viene en todas las formas y tamaños. Las aplicaciones se pueden ejecutar en todos los tipos de dispositivos, como escritorios, móviles y otros dispositivos. Por ejemplo, los juegos son aplicaciones que se pueden ejecutar en equipos de escritorio, dispositivos móviles e, incluso, televisores inteligentes.

Las aplicaciones también se están volviendo proactivas e inteligentes. Por ejemplo, la aplicación de mapas del teléfono móvil puede estar haciendo un seguimiento de la ubicación para proporcionar información de tráfico en tiempo real, aunque no se esté interactuando activamente con ella. Las aplicaciones de los dispositivos recopilan datos importantes sobre los usuarios, como la ubicación, cuánto tiempo permanecen en un lugar determinado, el historial de búsquedas del explorador, etc.

Describir qué son las aplicaciones

¿Qué es el software?

Software de aplicación

Normalmente, la información recopilada se comparte con otras aplicaciones. Por ejemplo, el historial de búsqueda del explorador a menudo se comparte con sitios de redes sociales, por lo que pueden proporcionar anuncios dirigidos basados en esa información.

Dado que **las aplicaciones** están tan entrelazadas en la vida diaria, y se ejecutan en todo tipo de dispositivos, **se han convertido en clave para obtener información sobre nosotros. Los ciberdelincuentes son conscientes de esto y van a intentar poner en peligro las aplicaciones para obtener nuestra información.**

Describir el panorama de amenazas de aplicaciones

Las aplicaciones están ampliamente disponibles y se usan para prácticamente cualquier cosa, desde el hogar y el uso personal, hasta el trabajo y la educación. Son una parte fundamental de nuestra vida cotidiana. Nos ponen fácil lo difícil.

Al mismo tiempo, las aplicaciones recopilan y conservan activamente grandes cantidades de datos sobre lo que hacemos, quiénes son nuestros amigos, dónde hemos estado, en qué gastamos nuestro dinero, cuáles son nuestras aficiones, etc. Los ciberdelincuentes son plenamente conscientes de la cantidad de datos que estas aplicaciones conservan y a la que acceden, y buscan cualquier punto débil para aprovecharlo.

Es esencial proteger los datos, tanto si es un individuo como una gran empresa. **El comprender cómo se pueden poner en peligro las aplicaciones y de dónde provienen estas amenazas mejora la seguridad de las aplicaciones y la confidencialidad de los datos almacenados o a los que se accede.**

Describir el panorama de amenazas de aplicaciones

Aplicaciones de orígenes no confiables

La posibilidad de descargar aplicaciones en el dispositivo ya sea un equipo, un smartphone o una tableta, se ha vuelto más sencilla. La mayoría de nosotros usamos grandes tiendas de aplicaciones consolidadas. Algunas de ellas comprueban la autenticidad de las aplicaciones antes de publicarlas y prohíben la venta de determinados tipos en su plataforma.

Pero hay otros lugares donde puede descargar aplicaciones. Las aplicaciones disponibles tienen poca o ninguna restricción y una mínima comprobación de su autenticidad. No todas las aplicaciones de estas tiendas son ilegítimas, pero un ciberdelincuente puede crear y empaquetar código fuente y darle el nombre de una aplicación legítima con la que los usuarios puedan estar familiarizados. Después, la cargan en un sitio de hospedaje junto con aplicaciones legítimas.

Si instala o ejecuta aplicaciones desde orígenes que no son de confianza, podría convertirse en víctima de un ciberataque.

Describir el panorama de amenazas de aplicaciones

Aplicaciones con vulnerabilidades inherentes

Aunque los desarrolladores de aplicaciones se esfuerzan por garantizar que sus aplicaciones sean seguras, es imposible garantizar una protección del cien por cien. Los ciberdelincuentes buscan cualquier vulnerabilidad que puedan aprovechar.

Hay muchos tipos diferentes de vulnerabilidades en las aplicaciones, dos de las más comunes son **las vulnerabilidades de código abierto y de día cero**.

Describir el panorama de amenazas de aplicaciones

Aplicaciones con vulnerabilidades inherentes

Vulnerabilidades de código abierto

Los desarrolladores de software suelen crear bibliotecas de funciones comunes para resolver un problema específico. Cualquiera puede acceder a las bibliotecas de código abierto y el código fuente suele estar disponible libremente. Cuando un desarrollador de aplicaciones quiere resolver un problema específico, primero comprueba si hay una solución de código abierto.

Una de las ventajas del código abierto es que los problemas y las vulnerabilidades se identifican públicamente y se solucionan. Pero estas bibliotecas también están disponibles para los ciberdelincuentes, que buscan formas de aprovecharlas. Los desarrolladores deben tener la versión más reciente de las bibliotecas de código abierto que han usado como componentes en sus aplicaciones para evitar los ciberataques.

Describir el panorama de amenazas de aplicaciones

Aplicaciones con vulnerabilidades inherentes

Vulnerabilidades de día cero

Los ciberdelincuentes realizan un reconocimiento detallado de las aplicaciones y buscan en el código errores que podrían aprovechar. Cualquier error desconocido por el propietario de la aplicación y no corregido se considera una vulnerabilidad de día cero. Cuando un ciberdelincuente encuentra una vulnerabilidad de día cero, no la hace pública, sino que la aprovechará al máximo.

Por ejemplo, un ciberdelincuente podría haber observado que una aplicación bancaria tiene una vulnerabilidad de día cero y la usa para robar información y dinero de forma silenciosa a los usuarios de la aplicación. El nombre, día cero, deriva del número de días que tiene un desarrollador desde que se identifica una vulnerabilidad hasta que hay una corrección disponible, que es de cero días.

Describir el panorama de amenazas de aplicaciones

Amenazas basadas en explorador

Los exploradores pueden ser la puerta de enlace a Internet, pero también son aplicaciones. Por eso, la mayoría de las amenazas que se va a encontrar se manifiestan mediante la actividad del explorador. Estas son dos de las amenazas basadas en explorador más comunes:

Ataques basados en cookies

Es posible que haya oído hablar de las cookies, ¿pero sabe realmente qué son? Una cookie es un archivo de texto no cifrado simple que contiene pequeños fragmentos de datos: las credenciales de usuario, la última búsqueda que realizó, el último artículo comprado, etc. El propósito de las cookies es mejorar la experiencia del explorador y facilitar la navegación, al simplificar la necesidad de iniciar sesión continuamente en el sitio.

Un tipo habitual de ataque con cookies es la *reproducción de sesión*. Si el ciberdelincuente puede interceptar o realizar escuchas de las comunicaciones, puede robar los datos de cookies y los de inicio de sesión y, después, usarlos para acceder al sitio web haciéndose pasar por usted.

Describir el panorama de amenazas de aplicaciones

Amenazas basadas en explorador

Error tipográfico deliberado

El *typosquatting*, o error tipográfico deliberado, es un tipo de ataque basado en explorador que consiste en que un ciberdelincuente obtiene deliberadamente nombres de dominio mal escritos. Estos se basan en sitios web populares, donde pueden colocar su propio código malintencionado, enmascarado como un sitio web legítimo del dominio. Los usuarios podrían confundir el sitio web malintencionado con el legítimo que quieren visitar. Si un usuario escribe cualquier información personal o sigue las instrucciones del sitio web, se habrá convertido en víctima de un ciberataque.

Describir cómo proteger las aplicaciones

En el mundo actual estamos conectados constantemente, y las aplicaciones se han convertido en fundamental para interactuar con los demás. Da igual si está hablando con amigos o compañeros, haciendo compras u operaciones bancarias: las aplicaciones hacen que todo esto sea posible.

Todos los desarrolladores de software y aplicaciones de buena reputación aspiran a compilar productos sólidos y seguros que proporcionen la funcionalidad necesaria y la seguridad para mantener a raya a los ciberdelincuentes.

Una aplicación protegida es aquella en la que el desarrollador ha probado todos los ciberataques más recientes antes de ponerla disponible para su descarga. Los desarrolladores de software ofrecen revisiones y actualizaciones para asegurarse de que la experiencia del usuario sea lo mejor y más segura posible.

Pero los ciberdelincuentes son incansables en su deseo de obtener los datos e intentan aprovechar cualquier debilidad o vulnerabilidad.

Hay algunas cosas que se pueden hacer, ya sea como individuo o como organización empresarial, para proteger las aplicaciones que se usan.

Describir cómo proteger las aplicaciones

Rápida aplicación de revisiones

Los sistemas operativos y la mayoría de las aplicaciones estándar (por ejemplo, los procesadores de texto y las aplicaciones de música), publican actualizaciones o revisiones. Algunas de estas ofrecen mejoras de funcionalidad, pero la mayoría sirve para corregir una vulnerabilidad o debilidad de seguridad conocida en el software, o para mejorar la seguridad de la aplicación. Los ciberdelincuentes y los hackers se centran en estas aplicaciones en busca de vulnerabilidades que se puedan aprovechar. Cuando identifican una, actúan rápidamente para escribir código malintencionado. Si lo hacen correctamente, este malware puede tomar el control de la aplicación o interceptar los datos a los que se accede hasta que se publica la siguiente revisión, momento en que el ciclo se vuelve a iniciar.

Como parte de un proceso o una directiva de seguridad sólidos, debe asegurarse de que todas las aplicaciones que se usan en el dispositivo tienen las revisiones o actualizaciones más recientes.

Describir cómo proteger las aplicaciones

Configuración de aplicaciones

La mayoría de las aplicaciones se desarrollan pensando en un equilibrio entre seguridad y facilidad de uso. Todas las aplicaciones incluyen una configuración predeterminada diseñada para un uso óptimo y para permitir el mayor acceso posible. Algunas pueden tener una cuenta de usuario predeterminada (administrador, por ejemplo) con una contraseña predeterminada estándar.

Los ciberdelincuentes identifican estas vulnerabilidades rápidamente y las aprovechan usando la configuración predeterminada para acceder a las aplicaciones. Es fundamental comprobar los valores de configuración de las aplicaciones y, siempre que sea posible, cambiar las contraseñas de las cuentas predeterminadas y la configuración. Este pequeño paso puede frustrar a un atacante y mejorar la confidencialidad de los datos y la integridad de la aplicación.

Describir cómo proteger las aplicaciones

Configuración de privacidad

Se realiza el seguimiento y el registro de todas las actividades que realice, desde una aplicación de mensajes instantáneos o simplemente con el explorador. Una pequeña parte de esto es para que los desarrolladores puedan mejorar la aplicación, pero la mayoría de los datos recopilados los usan los anunciantes para ofrecer contenido dirigido en función de las cosas que esté viendo o haciendo.

Todas las aplicaciones proporcionan un grado de control sobre los datos que se recopilan, ofreciendo una configuración de privacidad, que varía con cada aplicación. Por ejemplo, una aplicación de mapas puede tener una configuración de privacidad que evite el registro de las rutas que se han usado. Se puede indicar a una aplicación de compras que no recuerde los artículos que se han visto.

Un procedimiento recomendado es buscar la configuración de privacidad y adaptarla a lo que se quiere.

Describir cómo proteger las aplicaciones

Cookies

Los exploradores usan cookies para conservar detalles sobre lo que se ha estado haciendo en un sitio web determinado, desde lo último que se ha buscado hasta contraseñas u otros datos personales. Se han incorporado algunas medidas para intentar limitar la cantidad de datos que se conserva en las cookies y en el sitio web. Un ciberdelincuente podría aprovechar el explorador y acceder a estas cookies para obtener información y datos.

Todos los exploradores ofrecen la posibilidad de limpiar las cookies no usadas o de quitarlas todas. Se recomienda realizar una limpieza periódica de las cookies. Pero hay otra manera de administrar las cookies mediante la ventana de exploración privada del explorador. Es posible que las haya visto como ventanas de incógnito o de privacidad, y ofrecen un mayor nivel de seguridad para navegar con más confianza. Al cerrar la ventana del explorador, todas las cookies y el historial se eliminan automáticamente.

Describir cómo proteger las aplicaciones

Uso de aplicaciones comprobadas

Hace solo unos años, la única manera de obtener una aplicación era comprarla en una tienda, llevarse la caja a casa y usar el CD-ROM para instalarla en el equipo. A pesar de todos sus aspectos anticuados, esta era, con diferencia, la manera más segura de obtener y usar software. Internet ha hecho que el mundo sea un lugar más pequeño y ahora puede obtener aplicaciones desde la comodidad del dispositivo elegido sin salir de casa.

Hay una gran variedad de tiendas en línea que ofrecen la mejor oportunidad para encontrar la aplicación que está buscando. Pero, por cada tienda verdadera que vende una aplicación, es probable que haya otra que ofrezca una versión más barata, que podría contener algunas adiciones no deseadas.

Describir cómo proteger las aplicaciones

Uso de aplicaciones comprobadas

Un ciberdelincuente podría copiar la aplicación más reciente o más vendida y piratearla para incluir malware. Luego puede ofrecerla en una tienda a un precio más económico que cualquier otro lugar. A todos nos gusta una ganga, especialmente si significa obtener la aplicación más reciente a una fracción de su precio.

Es posible que la aplicación pirateada se comporte exactamente como la verdadera, pero por debajo, el ciberdelincuente puede buscar en el dispositivo datos personales o confidenciales, Después, esto se puede extraer y usar para con fines propios.

Como procedimiento recomendado, siempre debe descargar las aplicaciones desde tiendas comprobadas y de confianza.

Resumen y recursos

La proliferación de aplicaciones en el panorama digital presenta mayore oportunidades para los ciberdelincuentes.

Las aplicaciones influyen en cómo interactuamos con nuestros amigos y llevamos a cabo nuestro negocio. Ha visto que un diseño de software sólido puede mejorar la confidencialidad de los datos a los que se accede por medio de una aplicación. Además, ha visto que **las aplicaciones son objeto de ataques, al crear vectores que los ciberdelincuentes pueden usar para obtener datos sobre usted o su empresa**. Por último, ha aprendido algunos pasos que puede seguir para proteger las aplicaciones frente a ataques.

Ahora que ha completado este módulo, podrá realizar lo siguiente:

- *Describir qué son las aplicaciones.*
- *Describir el panorama de amenazas de aplicaciones.*
- *Describir los controles de seguridad basados en aplicaciones comunes*.

ESTO ES TODO

Extraído de ruta de aprendizaje de Microsoft Learn