Ciberseguridad

Sitio: Agencia de Habilidades para el Futuro
Curso: Práctica Profesional 1: Aproximación al mundo laboral 1º D
Libro: Ciberseguridad

Imprimido por: Eduardo Moreno
Día: lunes, 16 de junio de 2025, 16:12

Tabla de contenidos

Ciberseguridad: Protección de los sistemas importantes y la información confidencial de los ataques digitales

Para iniciar este temática, es importante primero partir de una serie de conceptos:

- La seguridad se refiere a la protección de la información personal frente a amenazas. La seguridad pone el foco en el acceso no autorizado a nuestros datos.
- La privacidad, por otro lado, se refiere a los derechos o el control que se tiene sobre la información y la forma en que se utiliza. Se centra en que nuestra información personal se procese y recopile basándonos en el consentimiento del propietario.
- Cifrado: es el proceso utilizado para convertir datos legibles en datos ilegibles, llamados texto cifrado.
- Codificación: hace referencia al proceso en el que los datos se cambian de un formato a otro mediante un algoritmo, para que sea legible para los sistemas.
- Hashing: es la conversión de cualquier texto en un conjunto de letras y números mediante un algoritmo.

Mientras que la encriptación está destinada a garantizar la confidencialidad, la codificación se centra en la usabilidad de los datos. El hashing, por su lado, asegura la autenticidad al verificar que un dato no ha sido alterado.

- Spam: correo electrónico no deseado o mensajes enviados a una lista de destinatarios.
- Phishing: es un correo electrónico diseñado para perjudicar a los usuarios obteniendo información personal como nombres de usuario, contraseñas e incluso datos bancarios.
- Spoofing (Suplantación de identidad): es un conjunto de ataques de phishing en el que el atacante se hace pasar por una persona u organización con la intención de obtener información.

Mundo online y protección de los sistemas informáticos

El acrecentamiento de trabajo remoto por la pandemia provocó un aumento proporcional de ciberdelitos.

El conjunto de habilidades requeridas por los profesionales de la ciberseguridad va más allá de la simple piratería y se ramifica en áreas como el desarrollo web, la generación de informes, la respuesta a incidentes y el análisis de datos. No siempre los delitos son cometidos por especialistas en programación y redes, conocidos como piratas informáticos o "hackers". En ocasiones los usuarios de los programas son los que provocan las vulnerabilidades.

Protección de los sistemas informáticos

Aunque la piratería es una parte crucial del trabajo para muchos profesionales de la ciberseguridad, la amplitud de los roles en esta área va mucho más allá de eso.

El análisis, la generación de informes, la creación de aplicaciones y sistemas que protegen la información y los datos internos también son parte integrante del trabajo diario de muchos profesionales de la ciberseguridad.

Roles de ciberseguridad que no tienen que ver con la piratería

Conozcamos los perfiles que trabajan en este área

- Desarrolladores de software: Desarrollan el software y las aplicaciones que protegen los sistemas informáticos contra malware o ataques de phishing, por lo que el enfoque está en el desarrollo en lugar de la piratería o las pruebas de penetración.
- Gestión: supervisión de las tareas diarias y la actividad de un equipo o de varios equipos.
- Expertos en IA: desarrollo y capacitación de herramientas de IA para predecir violaciones de seguridad o ataques de phishing.
- Gestores de incidentes: en lugar de testear y probar a piratear el sistema informático de una empresa, los gestores de incidentes trabajan para minimizar el daño causado por un ataque cuando ocurre.

Responder a un ataque

Los gestores de incidentes son especialmente importantes para las empresas que manejan datos de consumidores o información financiera, como los detalles de la tarjeta de crédito.

Es posible que deban informar sobre un incidente, notificar al equipo en general y a todos los empleados de la empresa, o notificar a los líderes de la empresa.

Los gestores de incidentes deben asegurarse de estar al día de las últimas amenazas online que aparecen constantemente. Aunque es posible que necesiten entender la piratería y la arquitectura del sistema en general, el trabajo diario requiere mucha investigación y capacitación constante.

Saber descifrar datos digitales de diversas fuentes, así como rastrear huellas digitales informáticas es de gran importancia.

Hacker

¿Qué es un hacker y qué hace?

Hacker o pirata informático: es alguien que se dedica a intervenir o realizar alteraciones técnicas, con buenas o malas intenciones, sobre determinado producto o dispositivo.

La palabra la acuñaron en 1960 un grupo de pioneros del MIT. Viene del término anglosajón Hack, que hace referencia al sonido que hacían los técnicos de las empresas telefónicas cuando golpeaban los aparatos para que funcionasen.

¿Qué tipos de hackers existen?

Según sus intenciones se pueden diferenciar dos tipos:

Black Hat: son los ciberdelincuentes. Realizan actividades ilícitas para vulnerar y extraer información confidencial, casi siempre con un fin económico. También son los creadores de todo tipo malware. Tipos:

Crackers: pueden incrustar virus o robar contraseñas, modificar software y extender sus funcionalidades.

Phreakers: se dedican a realizar acciones en el mundo de las telecomunicaciones.

White Hat: son hackers éticos que buscan detectar fallos y vulnerabilidades en los sistemas para corregirlos. Es decir, su meta es la de mejorar los sistemas en materia de seguridad.

Grey Hat - intermedios:

- Se dedican a traspasar los niveles de seguridad de una empresa para, acto seguido, ofrecer sus servicios para solventar la situación.
- Realizan acciones que pueden ser moralmente reprobables, pero tras las que existen buenas intenciones. El ejemplo más conocido sería el caso de Anonymous.

Otros tipos:

- Lamer o script-kiddie son las personas con falta de habilidades técnicas cuyo objetivo es obtener beneficios del hacking. Son una especie de hackers aficionados.
- Newbie o neófitos, son los novatos del hacking. No poseen casi ningún conocimiento o experiencia en el mundo de la tecnología.
- Hacktivistas, utilizan sus habilidades para penetrar sistemas seguros con metas políticas.
- Los hackers-estafadores que se dedican a robar cuentas de email o de redes sociales.

Hackers estafadores

Según Google, los hackers usan sobre todo tres técnicas para acceder a servicios de cuentas online, de empresas y particulares:

1. Phishing (pescar). Buscan datos sensibles, por ejemplo, los bancarios. Se trata del robo de identidad por parte de los estafadores para obtener datos personales de los usuarios. Pueden ser desde nombres de usuario y contraseñas, hasta datos bancarios y cuentas de acceso a otros servicios en línea. En el phishing se usan mensajes falsos como cebo. Por ejemplo, haciéndose pasar por otras personas o entidades a través mails, mensajes o llamadas de teléfono. Es la mayor amenaza para los usuarios.
2. Keyloggers. Son programas espía que registran todo lo que se teclea o se ve en la pantalla de los usuarios, y esos datos se envían a un servidor externo. Este tipo de estafa digital se da con asiduidad en lugares de conexión pública. Suelen formar parte de infecciones de mayor magnitud a través de malware, los programas maliciosos. Por medio de esta técnica, los ciberdelincuentes pueden llegar a robar un gran volumen de información confidencial sin que las personas afectadas se percaten de ello.
3. Brechas de seguridad. Los ciberdelincuentes roban las bases de datos de las empresas. Después se suele comercializar con esos datos, por ejemplo, para acceder a cuentas de correo electrónico y demás servicios.

Ransomware

¿Qué y cuales son sus efectos?

- Técnica de ciberataque a las empresas cada vez más frecuente.
- Se trata de un software que restringe el acceso a determinadas partes o archivos de un sistema operativo que ha infectado. El que lo introdujo, generalmente, exige un pago a cambio de quitar esta restricción.
- Los ataques zero clic, o de clic cero, no requieren de ninguna interacción por parte de los usuarios a los que se dirigen; como entrar en un enlace, habilitar macros o iniciar un ejecutable. Son sofisticados y se utilizan a menudo en campañas de ciberespionaje.
- Además, tienden a dejar muy poco rastro, lo que los hace más peligrosos. Una vez que un dispositivo se ve comprometido, un atacante puede optar por instalar un software de vigilancia (spyware), o por implementar una estrategia mucho más destructiva cifrando los archivos y reteniéndolos para pedir un rescate. Por lo general, una víctima no puede saber cuándo y cómo se infectó a través de un ataque sin clic, lo que significa que puede hacer poco para protegerse.