Glosario - CIB

ÁLVARO ALLÉN PERLINES

Contenido

Amenazas y vulnerabilidades

Amenazas

Se refiere a cualquier tipo de peligro o riesgo que pueda surgir a través de la red o de dispositivos conectados a Internet. Estas amenazas pueden incluir virus informáticos, malware, phishing, ataques DoS, robo de datos, etc…

Bibliografía:

- Qué significa amenaza cibernética - Intelligent Protection

Cifrar

Según la RAE, cifrar es "transcribir en guarismos[1], letras o símbolos, de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger". En términos más informáticos es el proceso de transformar texto legible sin formato en texto cifrado ilegible para enmascarar información confidencial de usuarios no autorizados. Esta práctica es realizada por las empresas cuando quieren proteger información sensible como modelos, pruebas, resultados o cualquier otra cosa que pueda ser usada en su contra.

Bibliografía:

- ¿Qué es el cifrado? | IBM

Confidencialidad

Se trata de una propiedad de la información que pretende garantizar el acceso sólo a las personas autorizadas. Los responsables de dicha información deciden quien tiene derecho a acceder a la misma. La característica principal de la confidencialidad es la no divulgación de un contenido.

Bibliografía:

- Confidencialidad - Qué es, definición y concepto

[1] Guarismos: signos y cifras arábigas que representan cantidades numéricas del 0 al 9.

Cross-Site Scripting(XSS)

Es una vulnerabilidad de seguridad que permite a los atacantes inyectar scripts maliciosos en páginas web confiables. Estos scripts, normalmente en JS, se ejecutan en el navegador de los usuarios, comprometiendo su información personal, cookies de sesión o incluso redirigiéndose a sitios maliciosos.

Hay diferentes tipos de XSS:

- **Reflected XSS (no persistente):** el script se inyecta a través de entradas de usuario, como formularios o parámetros, y se disuelve directamente en la respuesta del servidor sin ser almacenado.
- **Stored XSS (persistente):** el script se almacena en el servidor, como en bases de datos o campos de comentarios. Cada vez que un usuario carga la página afectada, el script se ejecuta automáticamente, afectando a múltiples usuarios.
- **DOM-Based XSS:** el script malicioso se inyecta directamente en el DOM[2] del navegador, sin pasar por el servidor. Esto ocurre cuando el código JS manipula entradas no validadas, como "document.write(location.hash)"

Bibliografía:

- XSS (Cross-Site Scripting): ¿Qué es? ¿Cómo protegerse de esto?
- Cross Site Scripting (XSS) | OWASP Foundation (traducida con IA)

DDoS

Un ataque de Denegación de Servicio Distribuido (Distributed Denial of Service) es igual que un ataque DoS en su esencia, denegar el servicio de una web, pero usando varios dispositivos para dificultar la situación. La teoría es la siguiente: un servidor realiza ataques a dispositivos de IT (Internet of Things) que tienen un software muy pobre en temas de seguridad. Intenta conectarse mediante usuarios y contraseñas creadas de fábrica y usando la fuerza bruta. Una vez conectado el servidor guarda el usuario y la contraseña junto con la IP y le inyecta un malware en la memoria caché para que sea indetectable. Este malware es el que más tarde va a usarse para realizar el ataque. Cuando la red de dispositivos es de un tamaño considerable se realiza el ataque, en vez desde una IP, desde tantas como dispositivos haya infectados. En estos casos, es más complicado solucionar el ataque.

La solución principal de estos ataques reside en un firewall de red en el lado servidor. Este firewall también llamado **reverse proxy** es un tipo de servidor que actúa como intermediario entre los clientes y los servidores backend. Su principal función es recibir las solicitudes de los clientes y reenviarlas del servidor y mejorar la seguridad, el rendimiento y la fiabilidad.

[2] DOM (Modelo de Objetos del Documento): interfaz de programación que representa la estructura de un documento HTML o XML en la memoria.

Bibliografía:

- ¿Qué son los ataques DoS y DDoS? | Ciudadanía | INCIBE

Disponibilidad

La disponibilidad en ciberseguridad se refiere a la capacidad de acceder y utilizar información y sistemas informáticos cuando se necesitan. Es un principio fundamental de la seguridad informática que asegura la fiabilidad y el acceso oportuno a los datos por parte de individuos autorizados.

Bibliografía:

- Disponibilidad en seguridad informática, ¿qué quiere decir?

DoS

Un ataque de Denegación de Servicio (Denial of Service) es un ataque cibernético en el que se deniega el acceso a un servidor web mediante la petición masiva por parte de un dispositivo. Éste realiza una cantidad enorme de peticiones al servidor, el servidor intenta responder a todas sus peticiones usando todos sus recursos y se queda sin espacio para el resto de peticiones denegando el servicio a los clientes reales.

Para solucionar este problema, la empresa deberá denegar el acceso a la IP del ordenador atacante. Por tanto este tipo de ataque no suele hacer daño alguno.

Bibliografía:

- ¿Qué son los ataques DoS y DDoS? | Ciudadanía | INCIBE

Exploits

Es un software de ataque que aprovecha las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos o el hardware. Los exploits toman la forma de un programa de software o una secuencia de código previsto para hacerse con el control de los ordenadores o robar datos de red.

Bibliografía:

- ¿Qué es un exploit de ordenador? Definición de exploit

Ingeniería social

Es un conjunto de prácticas y técnicas utilizadas para manipular y engañar a las personas con el fin de obtener información confidencial o hacer que realicen acciones no deseadas. Estos ataques pueden llevar a que las víctimas compartan datos sensibles, descarguen software malicioso o realicen transacciones financieras a favor de los delincuentes. La esencia está en la explotación de la psicología humana en vez de la técnica de hacking.

Bibliografía:

- ingenieria social definicion - Búsqueda

Integridad

Es un valor de quien tiene entereza moral, rectitud y honradez en la conducta y en el comportamiento. Esta integridad se puede referir a un individuo educado, honesto, que tiene control emocional, que tiene respeto por sí mismo. También responsable, disciplinario, directo, puntual, leal, pulcro y que tiene firmeza en sus acciones.

Bibliografía:

- Confidencialidad, Integridad y Disponibilidad

Inyección SQL

Es la inyección de sentencias SQL usando vulnerabilidades de la página web como el apartado de inicio de sesión. Con la introducción de “id=1” || “”=”” puedes recibir toda la información de la tabla usuarios incluido nombre, correo, contraseña (debería estar cifrada), etc…

Bibliografía:

- Inyección de Código

Malware

Es un programa o código malicioso que es dañino para los sistemas. Este malware busca invadir, dañar o deshabilitar computadoras, sistemas informáticos, redes, tabletas y dispositivos móviles, a menudo controlando parcialmente las operaciones de un dispositivo.

Los usuarios que desarrollan estos códigos buscan ganar dinero, sabotear tu capacidad de trabajar, hacer una declaración política o, la peor de todas, por simple aburrimiento y chulería.

Bibliografía:

- ¿Qué es el Malware? Definición de Malware, Tipos y Protección

Man-in-the-Middle

Es un tipo de ciberataque en el que alguien intercepta la comunicación entre dos dispositivos conectados en la red. Alguien se pone en el medio sin permiso para interceptarla y hacer con ella lo que quiera. También pueden reenviarte a una página web que no has solicitado y robarte la información que introduzcas en ella. La forma de conseguir interceptar la comunicación es averiguando la IP y la MAC del dispositivo al que quieres suplantar e intercambiar ambas direcciones para que el emisor del mensaje lo mande al atacante.

Bibliografía: Ataque Man-in-the-Middle: qué es, cómo funciona y cómo protegerte de él

Ransomware

Es un tipo de malware que ataque de manera indiscriminada a dispositivos conectados en al red. El ataque consiste en cifrar todos los archivos de un dispositivo y pedir una transferencia de bitcoin a una cartera del Blockchain[3] para conservar el anonimato. El malware puede llegar desde una descarga de contenido pirata, el correo de un jefe o, incluso, en las macros de un Word el cual muestra un mensaje falso.

Bibliografía:

- ¿Qué es el ransomware? | IBM

[3] Blockchain: es un tipo de base de datos parecido a un libro de contabilidad digital, descentralizado y mantenido por una red distribuida de computadoras.

Vulnerabilidad

Es el riesgo que una persona, sistema u objeto puede sufrir frente a peligros inminentes. En términos de ciberseguridad, las amenazas que existen frente a un sistema informático, aprovechan estas vulnerabilidades para cometer actos ilegales, ataques o robos, entre otras.

Bibliografía:

- Vulnerabilidad: qué es, tipos y ejemplos - Enciclopedia Significados

Medidas de protección básicas

Autenticación “multifactor” (MFA)

Es un método de seguridad que requiere dos formas de identificación para acceder a recursos y datos. Normalmente, el primer factor es una contraseña y el segundo puede ser desde un mensaje SMS al teléfono indicado o pulsar en un dialogo emergente desde el dispositivo conectado. A día de hoy es muy común el uso de métodos biométricos como huellas dactilares y reconocimiento facial.

Bibliografía:

- ¿Qué es y cómo se usa el Doble Factor de Autenticación (2FA)? | Prometeo

Roles

En un sistema operativo, los roles son colecciones de permisos que se definen para un sistema específico y pueden ser asignados a usuarios en contextos particulares. En resumen, determinan las habilidades y niveles de acceso que un usuario tiene dentro del sistema, lo que es fundamental para la gestión de la seguridad y el control de acceso. Ejemplos de roles son administrador como jefe total de la aplicación, usuario identificado que se le atribuye los clientes y usuario no identificado que es aquel que se ha conectado al servidor pero no ha iniciado sesión. Éstos últimos suelen ser los que menos privilegios albergan. Dependiendo de que rol tengas podrás acceder a unos lugares u otros, incluso puede que la interfaz de la aplicación sea diferente.

Bibliografía:

- Roles En Informática: Definición, Importancia Y Ejemplos - ServerNet

Permisos

Los permisos informáticos son el conjunto de autorizaciones que se otorgan a un usuario o sistema para interactuar con un recurso específico. Estos permisos determinan que acciones pueden realizarse sobre el recurso, como leer, modificar, eliminar o ejecutar. La gestión de estos permisos y analizar a que usuarios deben darse es fundamental para proteger la información y los recursos. Los tipos de permisos más comunes son:

- **Lectura:** permite visualizar el contenido de un recurso sin modificarlo.
- **Escritura:** permite modificar el contenido de un recurso.
- **Ejecución:** permite ejecutar archivos o programas.
- **Eliminación:** permite borrar el recurso.
- **Permisos especiales:** como cambiar la configuración de seguridad o delegar permisos a otros usuarios.

Es importante recalcar que estos permisos están muy relacionados con los roles que un usuario tiene. Dependiendo del rol que ostenta tiene ciertos permisos.

Bibliografía:

- Definición de Permisos de acceso (informática)

Reglas

En informática, una regla se define como un conjunto de instrucciones o procedimientos que establecen los límites y condiciones bajo los cuales se debe desarrollar, implementar y mantener un sistema o aplicación. En programación, las reglas son directrices que se deben seguir al escribir código, definiendo la sintaxis y la estructura correcta que debe tener un programa para que sea válido y funcione correctamente.

Bibliografía:

- Definición de Regla en Informática según Autor, ejemplos, qué es, Concepto y Significado

Firewall

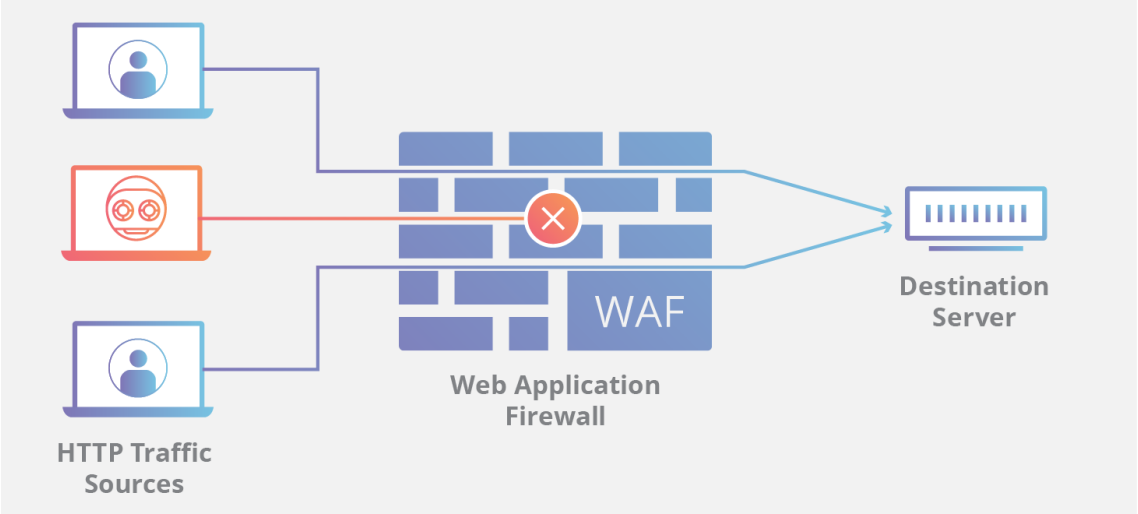
Es un sistema de seguridad de red que restringe el tráfico de Internet entrante y saliente o dentro de una red privada. Funciona bloqueando o permitiendo paquetes de datos de forma selectiva, protegiendo así a las computadoras o redes de accesos no autorizados. Además, supervisan y controlan el tráfico de la red según un conjunto de reglas de seguridad, situándose entre una red de confianza y una red no fiable, como Internet.

Bibliografía:

- ¿Qué es un firewall? Funcionamiento de los firewalls y tipos de firewalls

Filtrado

Cuando hablamos de filtrado en el desarrollo web nos referimos a la medida de seguridad que controla y restringe el acceso a sitios web específicos para proteger a los usuarios de amenazas en línea. Su objetivo es bloquear sitios web maliciosos, inapropiados o no relacionados con el trabajo, garantizando un entorno seguro y productivo.



Bibliografía:

- Implementación Control A.8.23 – Filtrado web - InfoProtección

Puertas

O mejor dicho, las **puertas traseras** se refieren a vulnerabilidades o agujeros en los sistemas que permiten el acceso no autorizado. Estas puertas pueden ser utilizadas tanto por administradores del sistema con fines legítimos como por hackers con intenciones maliciosas. Un ataque de puerta trasera ocurre cuando el atacante explota una vulnerabilidad para obtener acceso a un sistema sin ser detectado, lo que puede llevar a actividades maliciosas como el robo de datos o la manipulación de sistemas.

Bibliografía:

- Backdoor o Puerta Trasera: Qué es, Cómo Evitarlos y Eliminarlos

Protocolos

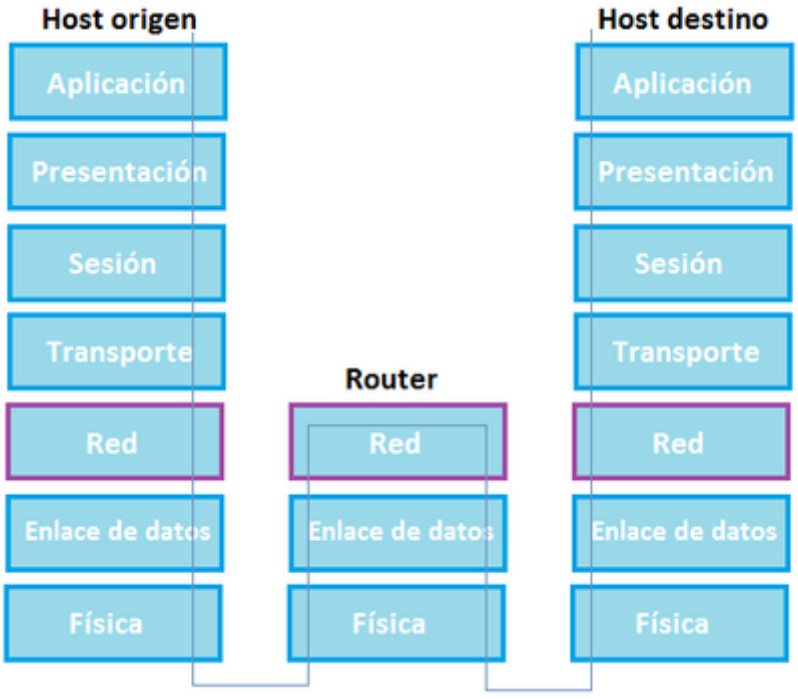
Los protocolos de ciberseguridad son conjuntos de reglas y normas que se establecen para proteger la información y los sistemas informáticos de posibles amenazas y ataques cibernéticos. Estos protocolos garantizan la confidencialidad, integridad, disponibilidad de los datos, así como la prevención del acceso no autorizado a la red y a los dispositivos. Incluyen medidas como el cifrado de datos, la autenticación de usuarios, la implementación de firewalls y la realización de copias de seguridad periódicas.

Bibliografía:

- Qué son los protocolos de ciberseguridad - Intelligent Protection

Routers

Es un dispositivo que permite interconectar redes con distinto prefijo en su dirección IP. Su función es la de establecer la mejor ruta que destinará a cada paquete de datos para llegar a la red y al dispositivo de destino. Es bastante utilizado para conectarse a Internet, ya que se conecta la red de nuestro hogar, oficina o cualquier red a la red de nuestro proveedor de este servicio. La mayoría de los rúteres que se utilizan para el hogar y oficinas tienen incorporadas otras funciones adicionales al enrutador, como el punto de acceso inalámbrico, el módem que convierte las señales analógicas en digitales y viceversa o el conmutador que conecta varis dispositivos a través de cable, creando una red local.



Bibliografía:

- Rúter - Wikipedia, la enciclopedia libre

Monitoreo

El monitoreo de ciberseguridad es un proceso sistemático y continuo que permite a las organizaciones observar y analizar los activos digitales para detectar y responder a posibles amenazas. Este proceso implica la recopilación de datos en tiempo real, lo que permite identificar brechas de seguridad, vulnerabilidades y actividades sospechosas antes de que causen daños significativos. Además, ayuda a garantizar la fiabilidad y estabilidad de los sistemas, asegurando que las operaciones empresariales y la integridad de la información estén protegidas.

Bibliografía:

- La importancia del monitoreo y análisis de ciberseguridad - Network Security Alliance

Auditoría

Una auditoría de ciberseguridad es un proceso esencial que evalúa la postura de seguridad de una organización. Este proceso incluye diversas actividades destinadas a identificar debilidades y riesgos en el ámbito cibernético, así como a establecer medidas para mitigar dichas amenazas. Se trata de una evaluación exhaustiva de los sistemas, políticas y prácticas de una organización para asegurar que se cumplen los estándares de seguridad.

Bibliografía:

- ¿Qué es una Auditoría de Ciberseguridad? - APPbera.com

Análisis de los incidentes de seguridad

Incidentes de seguridad

Se definen como cualquier evento que compromete la confidencialidad, integridad y disponibilidad de la información o los sistemas informáticos. Esto puede incluir ciberataques, accesos no autorizados, fugas de datos o malware.

Estos incidentes pueden ocurrir en cualquier momento. La clave está en reconocer los riesgos, actuar con rapidez y fortalecer constantemente las defensas tecnológicas.

Bibliografía:

- ¿Qué es un incidente de seguridad? - InfoProtección

Ciclo de vida de un incidente

Es un proceso continuo de planificación, implementación, monitoreo y mejora de las medidas de seguridad en un entorno digital. Este ciclo incluye varias etapas interconectadas que garantizan la efectividad y la adaptabilidad de las estrategias de seguridad

Fase 1: Detección

Implica la detección y clasificación de eventos que pueden comprometer la seguridad de la información. Para logarlo, es crucial implementar herramientas de monitoreo que ayudan a detectar actividades inusuales, comportamientos anómalos y posibles violaciones de políticas de seguridad.

Fase 2: Análisis

En esta fase se clasifica y se le da un nivel de prioridad según el grado de gravedad que tenga el incidente. Es por ello que hay que determinar la importancia de dicho incidente, su naturaleza, su alcance, las vulnerabilidades explotadas y los activos afectados.

Fase 3: Contención

Esta fase está diseñada para limitar el daño que un incidente puede causar, y se lleva a cabo a través de una serie de medidas tácticas. Aquí ya se empieza a implantar, por parte del equipo de seguridad, controles necesarios para prevenir que el incidente se propague. Entre las acciones posibles están: desconectar sistemas comprometidos, bloquear direcciones IP y restringir el acceso a áreas específicas de la infraestructura de TI.

Fase 4: Erradicación

Una vez contenido hay que erradicar el incidente. Para ello hay que buscar la causa raíz del incidente y evitar que vuelva a suceder en el futuro. Esto puede incluir la eliminación de malware, la aplicación de parches de seguridad y la renovación de credenciales comprometidas. Es importante encontrar y revisar todos los sistemas afectados, asegurando que no haya dejes que puedan causar futuros problemas.

Fase 5: Recuperación

Después de erradicar el incidente, habiendo revisado todos los sistemas afectados e implementados parches de seguridad, debemos recuperar los sistemas para que vuelvan a funcionar como antes. Hay que conectar los servicios como estaban antes del incidente y comprobar que todo funciona correctamente.

Fase 6: Aprendizaje

Una vez realizadas todas las fases, toca aprender. Cada vez que suceda un fallo de seguridad, un incidente o cualquier otra situación negativa y esté solucionada, debemos aprender de dicha experiencia para que, si en el futuro sucede otro, podremos actuar con mayor rapidez, usando soluciones de otros incidentes.

Bibliografía:

- Ciclo de Vida de un Incidente de Seguridad: Todo lo que Debes Saber

Indicadores de compromiso (IoC)

Son pruebas o señales que sugieren que un sistema ha sido infiltrado por un atacante o un software malicioso. Estos indicadores pueden incluir direcciones IP, nombres de dominio, hashes de archivos, patrones de tráfico de red y otros datos que ayudan a los equipos de ciberseguridad a identificar y responder a incidentes de seguridad.

Estos IoC ayudan a las organizaciones a identificar y confirmar la presencia de software malicioso en un dispositivo o red. Los ataques rastros de pruebas, tal como los metadatos. Los IoC se pueden obtener por varios métodos:

- **Observación:** de las actividades y comportamientos anormales en sistema o dispositivos.
- **Análisis:** para determinar las características de la actividad sospechosa y analizar su impacto.
- **Firmas:** de software malicioso para así identificarlos.

Bibliografía:

- ¿Qué son los indicadores de compromiso (IoC)? | Cloudflare

Estrategias proactivas

Análisis forense

También conocido como análisis forense digital es una técnica que se utiliza para investigar y analizar incidentes de seguridad informática, como por ejemplo, intrusiones de datos o ciberataques. Este proceso involucra la recopilación, preservación y análisis de datos digitales para determinar qué sucedió durante el incidente y quién es el responsable.

Bibliografía:

- Análisis forenses en ciberseguridad. ¿Qué son?

Herramientas y tecnologías de aplicación

Cortafuegos

O “Firewall” es un sistema de seguridad para bloquear accesos no autorizados a un ordenador mientras sigue permitiendo la comunicación de tu ordenador con otros servicios autorizados. También se utilizan en redes de ordenadores, sobre todo, en redes locales. Se trata de la primera medida de seguridad que empezó a implementarse en los ordenadores tras el nacimiento de Internet.

Hay dos tipos de cortafuegos: de software, de hardware o una combinación de ambos.

Software Firewall: son los más comunes a nivel usuario y vienen en forma de aplicación. A día de hoy, a parte de controlar la entrada de información, también vienen con protecciones adicionales contra troyanos y virus.

Hardware Firewall: pueden ser productos independientes o venir directamente integrados en el router. Los primeros se suelen situar entre el punto de acceso a Internet y el switch que se encarga de distribuir la conexión entre los ordenadores de una misma red. No son seguros en la mayoría de tipos de ataques por eso no es una medida tan usada.

Bibliografía:

- Firewall: qué es un cortafuegos, para qué sirve y cómo funciona

IDS/IPS

IDS (Intrusion Detection System): es un sistema que monitoriza el tráfico de red para identificar actividades no autorizadas o violaciones de políticas de seguridad.

IPS (Intrusion Prevention System): a parte de detectar una actividad no autorizada, también previene de ataques al bloquear el tráfico malicioso a tiempo real.

La diferencia entre ambos reside en que un IPS es un componente de la red activo que examina cada paquete que pasa y toma las medidas correctivas adecuadas en función de su configuración y política. Por el contrario, un IDS es un componente pasivo que generalmente no se implementa en línea y, en cambio, monitorea el flujo del tráfico con una tecnología de PAN o TAP para luego emitir notificaciones.

En resumen el IDS funciona como un observador y el IPS funciona como un cortafuegos.

Bibliografía:

- ¿Qué son y para qué sirven los SIEM, IDS e IPS? | Empresas | INCIBE

Antivirus

Son programas cuyo objetivo es detectar y eliminar virus informáticos. Con el paso del tiempo, los antivirus han evolucionado hacia programas más avanzados que además de buscar y detectar virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir una infección de estos. A día de hoy, son capaces de detectar muchos tipos de malware como spyware[4], gusanos[5], troyanos[6], rootkits[7] y pseudovirus[8]

Bibliografía:

- El antivirus | Ciudadanía | INCIBE

Cortafuegos basados en red

Es una solución de seguridad que supervisa y regula el tráfico de datos en función de normas de seguridad definidas. Actúa como una barrera entre redes internas y externas, permitiendo el tráfico seguro y bloqueando el acceso no autorizado. Como hemos visto en el apartado de cortafuegos de este tema, se puede implementar físicamente, lógicamente o una combinación de ambas.

Bibliografía:

- ¿Qué es un cortafuegos? | Definición de cortafuegos - Palo Alto Networks

Cortafuegos basados en host

Es un programa de software que se instala en un ordenador o servidor. Este tipo de cortafuegos está diseñado para proteger el ordenador individual de los ataques que provienen ordenadores de la red. Las cuatros reglas básicas de firewall son:

- **Denegar todo el tráfico.**
- **Permitir todo el tráfico.**
- **Permitir tráfico específico.**
- **Denegar tráfico específico.**

[4] Spyware: software malicioso que se instala sin permiso para espiar y robar información del usuario.
[5] Gusanos: malware que se reproduce y propaga automáticamente a través de redes, infectando múltiples dispositivos sin intervención del usuario.
[6] Troyano: malware que se oculta en programas legítimos para acceder y dañar el sistema sin que el usuario lo note.
[7] Rootkits: software malicioso que oculta la presencia de otros programas dañinos y permite el control remoto del sistema sin ser detectado.
[8] Pseudovirus: programa que simula ser un virus informáticos, pero no causa daño real al sistema.

IDS

(Intrusion Detection System): es un sistema que monitoriza el tráfico de red para identificar actividades no autorizadas o violaciones de políticas de seguridad.

Su funcionamiento en básico: analiza el tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc.. El IDS no solo analiza el tráficos sino que, también, revisa el contenido y su comportamiento.

Normalmente se integra con un firewall porque el detector de intrusos no es capaz de detener los ataques por sí solo, excepto los que trabaja conjuntamente con el dispositivo de puerta de enlace con funcionalidad de firewall, convirtiéndose en una herramienta muy poderosa ya que se une la inteligencia del IDS y el poder de bloqueo del firewall.

Bibliografía:

- ¿Qué es un sistema de detección de intrusiones (IDS)? | IBM

IPS

(Intrusion Prevention System): aparte de detectar una actividad no autorizada, también previene de ataques al bloquear el tráfico malicioso a tiempo real.

Al igual que pasa con los IDS, los métodos de prevención que usa los IPS son acerca de firmas o anomalías:

Detección basada en firmas: analizan paquetes de red en busca de firmas de ataques, es decir, características o comportamientos únicos asociados con una amenaza específica. Una secuencia de código que aparece en una variante particular de malware es un ejemplo de firma de ataque. Estas firmas están guardadas en una base de datos con el que compara. Estas bases de datos deben actualizarse regularmente por la constante mejora de la inteligencia de amenazas.

Detección basada en anomalías: utilizan inteligencia artificial y aprendizaje automático para crear y perfeccionar continuamente un modelo de referencia de la actividad normal de la red. El IPS compara la actividad de la red en curso con el modelo y responde cuando encuentra desviaciones, como un proceso que emplea más ancho de banda de lo normal.

Bibliografía:

- ¿Qué es un sistema de prevención de intrusiones (IPS)? | IBM

Antimalware

Se refiere a un tipo de software diseñado para prevenir, identificar y eliminar programas maliciosos de dispositivos y sistemas informáticos. Este software combate el código malicioso para proteger los activos digitales y la integridad de los datos.

Para realizar su cometido, emplea técnicas sofisticadas como la detección basada en firmas, la detección basada en el comportamiento y el sandboxing[9].

A día de hoy no se puede diferenciar de un antivirus ya que realizan las mismas funciones.

Bibliografía:

- Qué es un antimalware y cuál es la diferencia con un antivirus - Diario Panorama

OWASP

Es un organización internacional sin ánimo de lucro dedicada a mejorar la seguridad en el desarrollo de aplicaciones web. Su objetivo principal es proporcionar recursos gratuitos, como guías, herramientas y estándares, para ayudar a desarrolladores y empresas a proteger sus aplicaciones contra vulnerabilidades y ataques cibernéticos.

Uno de los proyectos más destacados de OWASP es **OWASP 10**, una lista que identifica las diez vulnerabilidades más críticas en aplicaciones web. Este informe no solo describe los riesgos, sino que también ofrece estrategias para mitigarlos. Entre las vulnerabilidades más comunes se encuentran la inyección de código, fallos de autenticación y problemas de configuración de seguridad.

Además, OWASP ofrece otros recursos como las Cheat Sheets, que son guías rápidas para implementar prácticas seguras, y herramientas como OWASP-ZAP, un proxy gratuito para detectar vulnerabilidades automáticamente. También fomenta una comunidad global activa con eventos y conferencias para el aprendizaje continuo.

Bibliografía:

- ¿Qué es el OWASP? ¿Qué es el OWASP Top 10? | Cloudflare

[9] **Sandboxing:** técnica de ciberseguridad que permite probar código o aplicaciones potencialmente maliciosas en un entorno controlado antes de ejecutarlas en un sistema.

Normativa y buenas prácticas de uso

Reglamento general de Protección de Datos (RGPD)

Norma promulgada por la Unión Europea que protege la privacidad de las personas en relación con el tratamiento de sus datos personales. Este reglamento entró en vigor el 25 de mayo de 2018 y afecta a todas las empresas que operan en la UE, independientemente de su tamaño, y establece directrices claras bore cómo se deben manejar los datos personales.

Bibliografía:

- Para más información, enlace directo al BOE del reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

ISO/IEC 27001

Es un estándar internacional que establece los requisitos para implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI). Su objetivo principal es ayudar a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de la información que manejan. Esta norma proporciona un marco estructurado para la gestión de la seguridad de la información, abarcando la evaluación y gestión de riesgos.

Bibliografía:

- Más información acerca de la Norma ISO/IEC 27001

Esquema Nacional de Seguridad (ENS)

Es un marco normativo en España que establece principios y requisitos para garantizar la seguridad del a información y los servicios electrónicos en el sector público y sus proveedores.

El ENS es de aplicación obligatoria para todas las entidades del sector público en España, así como para las empresas del sector privado que colaboran con estas entidades. Esto significa que cualquier organización que maneje información sensible o que preste servicios a la administración pública debe cumplir con los requisitos establecidos en el ENS.

El ENS está compuesto por una serie de elementos clave:

- **Políticas y requisitos mínimos:** medidas concretas que deben implementarse para garantizar la seguridad de los sistemas de información.
- **Auditoría y gestión de incidentes:** proceso de auditoría que las organizaciones deben superar para obtener la certificación del ENS, así como protocolos de respuesta ante incidentes de seguridad.

- **Dimensiones de seguridad:** el ENS considera cinco dimensiones de seguridad: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad cada cual asociada a un nivel de seguridad.

Bibliografía:

- Borrador del INCIBE que trata de forma detallada el ENS

Datos sensibles

Son aquellos que, si se divulgan o manejan de manera inapropiada, pueden afectar la esfera más íntima de una persona y conllevar un riesgo grave para su privacidad.

Según la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares**, se consideran datos sensibles aquellos que pueden revelar aspectos íntimos de una persona, cuya utilización indebida puede dar lugar a discriminación o conllevar un riesgo grave para el titular.

Bibliografía:

- Para más información y ejemplos concretos de información sensible

Políticas de acceso

Son conjuntos de directrices que determinan cómo se gestionan y controlan los derechos de acceso a la información dentro de una organización. Estas políticas son esenciales para garantizar que la información confidencial no caiga en manos equivocadas y que cada usuario tenga acceso solo a la información necesaria para desempeñar sus funciones.

Bibliografía:

- Página que trata acerca de las Políticas de Acceso Extendido

Ciclo de vida de la información

Abarca todas las etapas que atraviesa la información desde su creación hasta su eliminación, y es crucial para la gestión eficaz de datos en las organizaciones. Estas etapas son:

- **Creación de datos:** es la fase inicial donde la información se genera a través de diversas fuentes, como formularios, transacciones o interacciones en redes sociales. La calidad de los datos capturados en esta etapa es fundamental para su utilidad futura.
- **Almacenamiento y organización:** los datos deben ser almacenados de manera segura en servidores, bases de datos o en la nube. La organización adecuada de los datos facilita su acceso y uso posterior.
- **Procesamiento y análisis:** los datos se procesan para extraer la información valiosa. Se utilizan técnicas como minería de datos y análisis estadístico para identificar patrones y tendencias que pueden ser útiles para la toma de decisiones.
- **Distribución y acceso:** se distribuyen a los usuarios adecuados a través de informes o plataformas de visualización. Es esencial que la información esté disponible en el momento y formato correctos para su uso efectivo.
- **Retención y copia de seguridad:** no todos los datos se utilizan de inmediato, por lo que se establecen políticas de retención para determinar cuánto tiempo deben conservarse. Además, se realizan copias de seguridad para garantizar la recuperación de datos en caso de incidentes.
- **Eliminación:** los datos que ya no son necesarios deben ser eliminados de manera segura para evitar riesgos de seguridad. Esto es especialmente importante para la información sensible, que debe ser destruida de forma que no pueda ser recuperable.

Comprender y gestionar de manera correcta el ciclo de vida de la información permite a las organizaciones optimizar el uso de sus datos, mejorar la seguridad, cumplir con las regulaciones de privacidad y reducir costos innecesarios. La gestión eficaz de la información es esencial para la toma de decisiones informadas y el cumplimiento de los objetivos organizacionales.

Bibliografía:

- Página para introducirse en formas y métodos de gestión de información

Diagnóstico de fallos

Es un proceso crucial en el mantenimiento y la gestión de sistemas. Se refiere a la identificación y análisis de problemas que afectan el rendimiento de un sistema, permitiendo a las empresas tomar decisiones informadas para mejorar la eficiencia y prevenir futuras fallas. Este proceso puede incluir técnicas como el análisis de códigos de error, pruebas de rendimiento y revisiones mecánicas, y es esencial para el mantenimiento correctivo y la mejora de la fiabilidad del equipo.

Bibliografía:

- Para más información, aquí una página que trata de manera más detallada el diagnósticos de fallos

Propuesta de mejora

La propuesta de mejora o propuesta de valor en una empresa es la declaración que comunica de manera clara y concisa cómo los productos o servicios de la empresa abordan las necesidades específicas de seguridad informática de los clientes y les ofrecen un valor único y diferenciado. Ejemplos de propuestas de mejora en temas de ciberseguridad son:

- **Protección de Datos Confidenciales**
- **Prevención de Ataques de Ransomware**
- **Monitorización Continua de Amenazas**
- **Cumplimiento Normativo y Regulatorio**
- **Educación y Concienciación en Seguridad**

Bibliografía:

- Aquí una extensión de la información. En esta página se especifica cada uno de estos puntos con ejemplos reales de propuestas de valor.

Registro de incidencias

Es un documento que se utiliza para documentar y gestionar eventos o situaciones inusuales que ocurren en un entorno laboral, educativo o de servicios.

De manera más detallada, un registro de incidencias es un sistema que permite dejar constancia de cualquier evento que pueda afectar el normal funcionamiento de una organización. Estos eventos pueden variar en naturaleza y gravedad, desde situaciones leves hasta incidentes más serios que requieren atención inmediata. El propósito principal de este registro es documentar lo sucedido para prevenir la repetición de

incidentes similares en el futuro y mejorar la seguridad y eficiencia en el entorno donde se aplica.

Bibliografía:

- Guía nacional de notificación y gestión de ciberincidentes | INCIBE-CERT | INCIBE