GLOSARIO DE TÉRMINOS

ESTÁNDAR DE COMPETENCIAS PROFESIONALES: Auditar redes de comunicación y sistemas informáticos

Código: ECP0487_3 NIVEL: 3

Antivirus: Tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de un ordenador.

Auditoría: Revisión práctica que se realiza sobre los recursos informáticos con que cuenta una entidad con el fin de emitir un informe o dictamen sobre la situación en que se desarrollan y se utilizan esos recursos.

Cifrado: También, encriptado. Conversión de información de un formato legible a un formato codificado. La información cifrada solo se puede comprender y procesar tras el descifrado (desencriptado).

CMS: (Content Management System. En español, herramienta de gestión de contenidos). "Software" diseñado para ayudar a los usuarios a crear y editar un sitio "web".

Confidencialidad: También, principio de privacidad. Uno de los principios de la seguridad informática. Hace referencia a que la información solo debe ser conocida por las personas autorizadas para ello. Es decir, ciertos datos o programas solo pueden ser accesibles para las personas autorizadas.

Cookie: (Anglicismo). Información que un sitio web pone en el dispositivo de un usuario. Las cookies almacenan información limitada sobre una sesión del navegador en un sitio web concreto que puede ser recuperada más adelante.

Cortafuegos: (Firewall). Sistema que protege redes y terminales privadas de accesos no autorizados, especialmente durante la navegación por internet.

DDoS: (Ataque de denegación de servicio distribuido). Intento malintencionado de interrumpir el tráfico normal de un servidor, servicio o red determinada, sobrecargando el objetivo o su infraestructura asociada con una avalancha de tráfico de Internet.

Disponibilidad: Capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios o procesos autorizados cuando estos lo requieran. Es uno de los principios fundamentales de la ciberseguridad junto a la confidencialidad y la integridad.

DMZ: (Demilitarized Zone. En español, zona desmilitarizada). Red aislada que se encuentra dentro de la red interna de la organización. En ella se encuentran ubicados exclusivamente todos los recursos de la empresa que deben ser accesibles desde Internet, como el servidor web o de correo.

DoS: (Denial of Service, también DDoS por Distributed Denial of Service. En español, ataque de denegación de servicio o ataque distribuido de denegación de servicio). Tipo de ciberataque que intenta hacer que un sitio web o recurso de red no esté disponible colapsándolo con tráfico malintencionado para que no pueda funcionar correctamente.

EDR: (Endpoint Detection and Response). Herramienta que proporciona monitorización y análisis continuo del dispositivo terminal (endpoint) y la red. La finalidad es identificar, detectar y prevenir amenazas avanzadas (APT) con mayor facilidad. La tecnología EDR detecta ataques que nuestro antivirus ha pasado por alto. Monitoriza y evalúa todas las actividades de la red (eventos de

los usuarios, archivos, procesos, registros, memoria y red). Detecta ataques informáticos en tiempo real, y permite tomar medidas inmediatas si es necesario.

EPP: (Endpoint Protection Platform). Solución de seguridad integral desplegada en equipos terminales para protegerse de amenazas. Las soluciones EPP son gestionadas típicamente en la nube y usan datos en ella para asistir en soluciones avanzadas de monitorización y solución remotas. Contienen una suite de tecnologías de seguridad tales como antivirus, encriptación de datos y prevención de pérdida de datos.

Herramienta de gestión de contenidos: También llamada CMS ("Content Management System") y Sistema de Gestión de Contenidos. Tipo de "software" diseñado para ayudar a los usuarios a crear y editar un sitio "web".

IDS: (Intrusion Detection System. En español, Sistema de Detección de Intrusos). Sistema de supervisión que detecta actividades sospechosas y genera alertas al detectarlas.

Integridad: Garantía de que la información digital no está dañada y solo pueden acceder o modificar aquellos autorizados para hacerlo.

Inyección de SQL: (SQL inject). Tipo de ciberataque encubierto en el cual un hacker inserta código propio de acceso a base de datos en un sitio web con el fin de quebrantar las medidas de seguridad y leer o modificar datos protegidos. Una vez dentro, puede controlar la base de datos del sitio web y secuestrar la información de los usuarios.

IP: (Internet Protocol. En español, Protocolo de Internet). Conjunto de reglas que rigen el envío y recepción de datos enviados a través de Internet o de una red local basada en ese protocolo. Por extensión, se asimila a dirección IP, esto es, dirección lógica única que identifica a un dispositivo en Internet o en una red local basada en la arquitectura TCP/IP en un momento dado según las reglas del protocolo IP.

IPS: (Intrusion Prevention System. En español, Sistema de Prevención de Intrusiones). Dispositivo o aplicación software que monitoriza una red para detectar y responder a cualquier actividad maliciosa o violaciones de la política de seguridad. Cualquier actividad o violación maliciosa es reportada o recogida de manera centralizada usando un sistema de seguridad de la información y de gestión de eventos. A diferencia de los IDS, los IPS son capaces de responder a intrusiones detectadas en el momento de su descubrimiento.

Mesas limpias: Concepto asociado a la confidencialidad de todos aquellos documentos que puedan contener datos sensibles, considerando que dichos papeles no pueden estar a la vista de cualquier persona.

Mínimo privilegio: También "mínimo conocimiento" y "necesidad de saber"- Principio consistente en minimizar el impacto de cualquier fallo, accidente o vulnerabilidad del sistema, reduciendo los privilegios de las cuentas de usuario al mínimo necesario para el desempeño de sus tareas autorizadas. Dado que este principio está directamente relacionado con los distintos perfiles creados

dentro del sistema operativo, los expertos recomiendan disponer de al menos dos cuentas básicas.

Monitorización: Acción realizada por elementos físicos y "software" que registran la situación en que están cada uno de los aspectos que se desean controlar.

No repudio: También, irrenunciabilidad. Mecanismos hardware y software que proveen garantía al receptor de una comunicación en cuanto que el mensaje fue originado por el emisor y no por alguien que se hizo pasar por este. Además, previene que el remitente o emisor del mensaje afirme que él no envió el mensaje. Es uno de los principios fundamentales de seguridad de la información.

Nube: Red de servidores remotos conectados a internet para almacenar, administrar y procesar datos, servidores, bases de datos, redes y software.

Parche: Nueva versión de un software o de parte de él que incluye más y mejores funcionalidades y/o soluciona fallos de la versión precedente.

Protocolo: Conjunto de normas y procedimientos establecidos para el desarrollo de una actuación.

Punto de acceso: También AP o WAP, del inglés "Wireless Access Point". Equipos hardware configurados en redes Wifi y que hacen de intermediario entre el ordenador y la red externa (local o Internet). El "access point" o punto de acceso, hace de transmisor central y receptor de las señales de radio en una red inalámbrica.

Router: (Anglicismo. En español, encaminador). Dispositivo de interconexión entre redes de datos diferentes. Opera en el nivel tres de OSI. Un tipo es el router de banda ancha que interconecta una red local e Internet.

Servicio: Programa instalado en un equipo remoto llamado servidor y cuya funcionalidad se ofrece a otros equipos conectados a él por red llamados cliente. Son típicos los servicios/servidores de impresión, de archivos, de cualquier programa/software mediante llamadas a procedimientos remotos (RPC) o de páginas web. La mayor capacidad del servidor se pone al servicio de los clientes, lo que redunda en una mayor simplicidad y menor coste de los segundos.

Servidor: Máquina física integrada en una red informática en la que, además del sistema operativo, opera uno o varios servicios "software" que se ofrecen a otros equipos denominados clientes que pueden estar conectados a nivel local o a través de una red externa. El tipo de servicio depende del tipo de "software" del servidor. La base de la comunicación es el modelo cliente-servidor y, en lo que concierne al intercambio de datos, entran en acción los protocolos de transmisión específicos del servicio.

SIEM: (Security Information and Event Management. En español, gestión de información y eventos de seguridad). Solución de seguridad que ayuda a las organizaciones a reconocer posibles amenazas y vulnerabilidades de seguridad antes de que tengan la oportunidad de interrumpir operaciones empresariales.

Switch: (Anglicismo. En español, conmutador). Dispositivo de interconexión utilizado para conectar equipos en una red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen estándares tales como Ethernet (o técnicamente IEEE 802.3). Opera en el nivel 2 de OSI.

Trazabilidad: Conjunto de procedimientos que permiten seguir la evolución de los procesos o productos en cada una de sus etapas.

Virus: Programa informático elaborado de manera anónima que tiene la capacidad de reproducirse y transmitirse independientemente de la voluntad del operador y que causa alteraciones más o menos graves en el funcionamiento de la computadora.

VPN: (Virtual Private Network. En español, Red Privada Virtual). Servicio que cifra los datos de las comunicaciones entre dos puntos, incluyendo la navegación en Internet, construyendo una red privada y segura o túnel entre la conexión de una máquina cliente y un servidor destinatario.

Vulnerabilidad: Debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos "agujeros" pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.

WIFI: Solución informática de conectividad que comprende un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11, lo cual asegura la compatibilidad e interoperabilidad en los equipos certificados bajo esta denominación.

XSS: (Cross Site Scripting). Ataque que aprovecha fallas de seguridad en sitios web y que permite a los atacantes implantar scripts (códigos) maliciosos en un sitio web legítimo (también víctima del atacante) para ejecutar un script en el navegador de un usuario desprevenido que visita dicho sitio y afectarlo, ya sea robando credenciales, redirigiendo al usuario a otro sitio malicioso, o para realizar defacement en un sitio web.