GLOSARIO DE TÉRMINOS

ESTÁNDAR DE COMPETENCIAS PROFESIONALES: Configurar la seguridad en redes de comunicaciones y sistemas de correo electrónico

Código: ECP2797_2 NIVEL: 2

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

Clave pública: Una de las dos claves que genera un procedimiento de criptografía asimétrica. La clave privada y la pública están matemáticamente relacionadas. La clave pública se genera siempre a partir de la clave privada. La clave pública puede ser difundida por su propietario para ser usada por terceros. Estos terceros pueden usar la clave pública del propietario para cifrar mensajes que solo el propietario de la clave pública podrá leer usando su clave privada.

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.

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

DLP: (Data Loss Prevention. En español, prevención de fuga de datos). Herramienta que tiene como finalidad prevenir las fugas de información cuyo origen está dentro de la propia organización, de una manera activa y sin perder productividad. Estas herramientas suelen incorporar inteligencia artificial que les permite aprender sobre el tipo de documentos confidenciales que se utilizan y qué acciones llevan a cabo los usuarios sobre los mismos, para volverse cada vez más efectivas en la prevención de fugas de información.

DNS: (Domain Name System. En español, Sistema de Nombres de Dominio). Método de denominación empleado para nombrar mediante caracteres alfanuméricos legibles para humanos a los dispositivos que se conectan a una red a través del IP (Internet Protocol o Protocolo de Internet). El DNS se encarga de vincular informaciones asociadas al nombre de dominio que se le asigna a cada equipo y traducir a direcciones de red numéricas, por ejemplo, IP.

Dominio: Nombre único y exclusivo que se le da a un sitio web en Internet para que cualquiera pueda visitarlo.

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.

Evento: Notificación automática que ha habido algún tipo de acción y que suele disparar una acción o conjunto de acciones que, a su vez, pueden dar como resultado un evento en particular o una serie de eventos.

Framework: (Anglicismo). Marco o esquema de trabajo generalmente utilizado por programadores para realizar el desarrollo de "software". Utilizar un "framework" permite agilizar los procesos de desarrollo ya que evita tener que escribir código de forma repetitiva, asegura unas buenas prácticas y la consistencia del código.

Honeypots: (Anglicismo). Herramienta de seguridad informática dispuesto en una red o sistema informático para ser el objetivo de un posible ataque informático, y así poder detectarlo y obtener información del mismo y del atacante.

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.

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.

Nodo: Punto de conexión que puede recibir, crear, almacenar o enviar datos a lo largo de rutas de red distribuidas. Cada nodo de la red, ya sea un punto final para la transmisión de datos o un punto de redistribución, tiene una capacidad programada o diseñada para reconocer, procesar y reenviar transmisiones a otros nodos de la red.

Parsear: En inglés parsing. También parseo. Proceso de analizar una secuencia de símbolos a fin de determinar su estructura gramatical definida. También llamado análisis de sintaxis.

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.

Sistema operativo: Conjunto de programas que permite manejar la memoria, disco, medios de almacenamiento de información y los dispositivos asociados, periféricos o recursos del ordenador, como son el teclado, el ratón, la impresora, la tarjeta de red, entre otros.

Software de base: También "Software" base o "software" de sistema. Programa o conjunto de programas que se encargan de gestionar las funciones que dan soporte al resto de aplicaciones que soporta un dispositivo o sistema informático, que puede ser un servidor, ordenador de sobremesa, teléfono móvil o "tablet", entre otros. Usualmente son "software base" o "software de base" todo el "firmware", controladores y programas del sistema que constituyen el sistema operativo y ciertas utilidades asociadas.

Syslog: (Anglicismo. En español, registro de sucesos del sistema). Estándar de mensajes de log o sucesos que casi todos los dispositivos o aplicaciones pueden enviar o almacenar, conteniendo información sobre estado, eventos y diagnósticos, entre otros.

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.