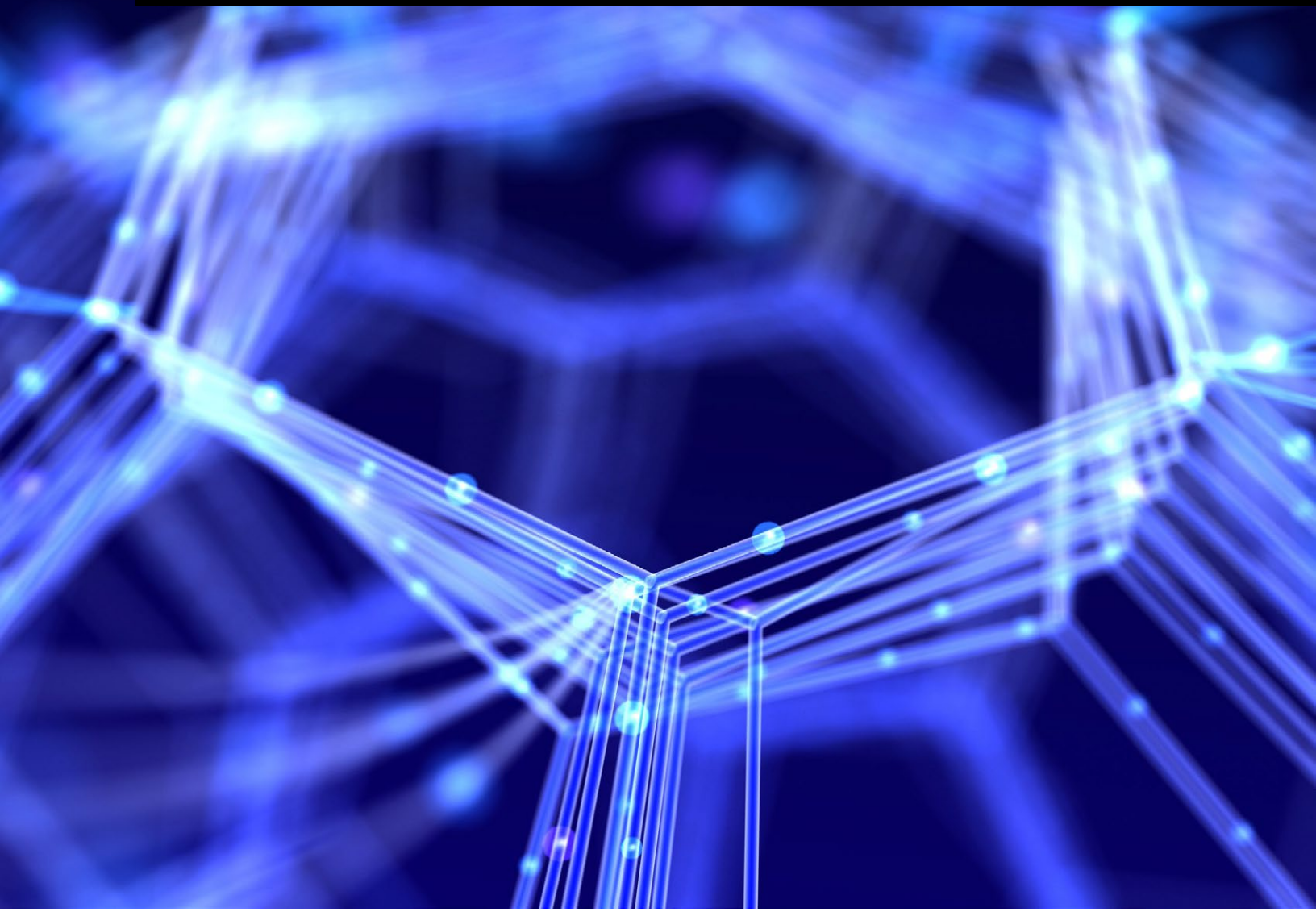
Glosario de términos de ciberseguridad

Noviembre 2022

LOCKTON®



Las exposiciones cibernéticas son una amenaza siempre presente para las empresas y otras organizaciones, una que está en constante evolución a medida que los atacantes crecen más sofisticados y emplean nuevas estrategias para interrumpir las operaciones y robar datos valiosos. Como los métodos de defensa contra tales ataques de manera similar evoluciona, también lo hace el lenguaje utilizado por las partes interesadas.

Este glosario está destinado a ayudar con los conceptos clave de ciberseguridad.

Esperamos que sirva como un documento de referencia útil como las organizaciones se preparan, mitigan y responden a las amenazas de ciberseguridad.

Contenido

A

Acceptable Use Policy (AUP)

Un plan escrito en el que se describen las restricciones y las prácticas que un usuario debe aceptar para acceder a la red de una organización o a internet. Las organizaciones suelen exigir a sus empleados y contratistas independientes que firmen una AUP antes de que se les conceda una identificación de red, y en el caso de instituciones educativas, también se puede exigir a los estudiantes que firmen el documento.

Active Directory (AD)

El servicio de directorio propietario de Microsoft. Un servicio de directorio mapea los nombres de los dispositivos de red a sus direcciones de red únicas. Se ejecuta en Windows Server y permite a los administradores gestionar los permisos y derechos de acceso. AD almacena los datos como objetos, cada uno de los cuales es un único elemento: un usuario, un grupo, una aplicación o un dispositivo, como una impresora. Los objetos pueden ser recursos, como impresoras o computadoras, o bien directores de seguridad, como usuarios o grupos.

Authentication

Prueba o garantía de que una persona que intenta iniciar sesión en un servicio o realizar una transacción en línea posee y controla activamente un token o autenticador que verifica su identidad.

Authenticator Assurance Level (AAL)

La confianza o el grado de seguridad de que un individuo posee un autenticador. Existen tres niveles de AAL:

- AAL1 requiere autenticación de un solo factor o autenticación multifactor utilizando una amplia gama de tecnologías de autenticación disponibles. El éxito de la autenticación requiere que el usuario demuestre posesión y control del autenticador a través de un protocolo de autenticación seguro.
- AAL2 proporciona una alta confianza en que el usuario controla uno o más autenticadores vinculados a la cuenta del usuario. Prueba de posesión y control de dos factores de autenticación diferentes se requiere a través de protocolos de autenticación seguros.
- AAL3 proporciona una muy alta confianza en que el usuario controla uno o más autenticadores vinculados a la cuenta del usuario. La autenticación en AAL3 se basa en la prueba de la posesión de una clave mediante un protocolo criptográfico. La autenticación en AAL3 requiere un autenticador basado en hardware y un autenticador que proporcione resistencia a la suplantación del verificador; el mismo dispositivo puede cumplir ambos requisitos.

B

Breach & Attack Simulation (BAS)

Un método avanzado de pruebas de seguridad informática. Un BAS identifica las vulnerabilidades de los entornos de seguridad imitando los probables métodos de ataque utilizados por los ciberdelincuentes. Las soluciones BAS proporcionan detección automática de vulnerabilidades y priorizan las actividades de mitigación para minimizar la exposición.

Business Continuity (BC)

Acciones, políticas, procedimientos, procesos y herramientas para garantizar que una organización pueda continuar con las operaciones críticas en caso de un incidente cibernético.

Business Impact Analysis (BIA)

Un proceso por el cual los activos de una organización son catalogados y documentados para reflejar la importancia de cada uno para la organización.

C

Capability Maturity Model (CMM)

Un modelo de madurez es una herramienta que utilizan las empresas para evaluar sus operaciones.

En un CMM se incluyen cinco niveles, cada uno de los cuales contiene varias prácticas clave.

- CMM nivel 1: Salvaguardar la información de los contratos federales.
- CMM nivel 2: Servir como paso de transición en el avance de la madurez de la ciberseguridad hacia la protección de la información no clasificada controlada.
- CMM nivel 3: Proteger la información no clasificada controlada (CUI por sus siglas en inglés).
- CMM niveles 4-5: Proteger la CUI y reducir el riesgo de amenazas persistentes avanzadas.

Common Vulenarabilities & Exposures (CVE)

Una lista de fallas de seguridad informática divulgados y catalogados públicamente, donde a cada uno se le asigna un número de identificación CVE.

Los identificadores CVE son asignados por una autoridad de numeración CVE (CNA). Hay aproximadamente 100 CNAs, que representan a los principales proveedores de TI - como Red Hat, IBM, Cisco, Oracle y Microsoft, así como empresas de seguridad y organizaciones de investigación. MITRE, una organización sin ánimo de lucro que gestiona centros de investigación y desarrollo financiados por el gobierno federal de Estados Unidos, también puede emitir CVEs directamente.

Los avisos de seguridad emitidos por proveedores e investigadores casi siempre mencionan al menos un identificador CVE. Los CVEs ayudan a los profesionales de TI a coordinar sus esfuerzos para priorizar y abordar las vulnerabilidades con el objetivo de que los sistemas informáticos sean más seguros.

Common Vulnerability Scoring System (CVSS) Score

Una representación numérica (0-10) de la gravedad de una vulnerabilidad de la seguridad de la información. Las puntuaciones CVSS son comúnmente utilizadas por los profesionales de la seguridad de la información en programas de gestión de vulnerabilidades para proporcionar un punto de comparación entre vulnerabilidades y priorizar la remediación de estas.

Cross-site scripting (XSS o CSS)

Un ataque a una aplicación web utilizado para obtener acceso a información privada mediante la entrega de un código malicioso a los usuarios finales a través de sitios web de confianza. Normalmente, este tipo de ataque es exitoso debido a la falta de validación de la entrada del usuario en una aplicación - por ejemplo, permitiendo a los usuarios suministrar un código de la aplicación en formularios HTML en lugar de cadenas de texto normales.

D

Data Loss Prevention (DLP)

Herramientas, procesos y procedimientos que garanticen que los datos sensibles no se pierdan, no se utilicen indebidamente o no se acceda a ellos por parte de usuarios no autorizados. El software de

DLP clasifica los datos regulados, confidenciales y críticos para el negocio e identifica las violaciones de políticas definidas por las organizaciones o dentro de un paquete predefinido, normalmente alineadas a el cumplimiento regulatorio.

Demilitarized Zone (DMZ)

Una red perimetral que protege y añade una capa de seguridad adicional a la red de local interna de una organización contra el tráfico no confiable.

El objetivo de una DMZ es encontrar el equilibrio entre permitir el acceso a redes que no son de confianza, como Internet, mientras se garantiza que la red privada o LAN permanezca segura.

Disaster Recovery (DR)

Procesos, tareas y actividades necesarias para que una organización opere como normalmente lo hace y restablecer las operaciones después de un incidente perturbador.

Domain Name System (DNS)

Esencialmente, la guía telefónica de Internet. Los humanos acceden a la información en línea a través de nombres de dominio – por ejemplo, lockton.com, nytimes.com o espn.com. Los navegadores web interactúan a través de las direcciones IP. El DNS traduce nombres de dominio a direcciones IP para que los navegadores puedan cargar recursos de Internet.

E

Endpoint

Un endpoint es cualquier dispositivo conectado a una red informática. Algunos ejemplos son los servidores, computadoras de escritorio, computadoras portátiles, teléfonos móviles, tabletas, sistemas de puntos de venta (POS) y dispositivos de Internet of Things (IoT).

Endpoint Detection & Response (EDR)

Una solución integrada de seguridad para endpoints que combina la supervisión continua en tiempo real y la recopilación de datos de los endpoints con capacidades de respuesta y análisis basados en reglas. También se conoce como Endpoint Threat Detection and Response (ETDR).

H

Hypertext Markup Language (HTML)

Lenguaje de programación utilizado para crear páginas que puede mostrar un navegador web. La mayoría de las páginas web en internet se almacenan como archivos HTML. Un sitio web representa una colección de páginas HTML relacionadas, almacenadas en un servidor compartido.

I

Identity & Access Management (IAM)

Un sistema para garantizar que determinadas personas y puestos de una organización (usuarios) puedan acceder a las herramientas que necesitan para sus tareas y puestos específicos.

Un sistema IAM permite a una organización gestionar aplicaciones sin tener que iniciar sesión en cada aplicación como como administrador y gestionar una serie de identidades, incluyendo personas, software y hardware, como la robótica y dispositivos de IoT.

Identity Provider (IdP)

Un servicio que almacena y gestiona las identidades digitales. Estos servicios permiten a los empleados o usuarios de una organización conectarse con los recursos que necesitan, proporcionando una forma de gestionar el acceso - añadiendo o eliminando privilegios, al mismo tiempo que se mantiene la seguridad adecuada.

Si alguna vez has utilizado tu nombre de usuario de Google o Facebook para acceder a una aplicación, has utilizado un IdP. Tu nombre de usuario y contraseña abren las puertas a otro recurso, y no tienes que hacer nada adicional para hacer que suceda.

Incident Response Plan (IRP)

Un documento que describe los procedimientos, pasos y responsabilidades de una organización sobre su programa de respuesta a incidentes.

Internet of Things (IoT)

La red de objetos físicos - "cosas"- que llevan incorporados sensores, software y otras tecnologías con el fin de conectar e intercambiar datos con otros dispositivos y sistemas a través de internet. Ejemplos de productos de oficina con IoT son la iluminación inteligente, los termostatos inteligentes, cerraduras inteligentes, rastreadores GPS y aplicaciones de control de la calidad del aire.

Internet Protocol (IP)

El conjunto de normas que rigen el formato de los datos enviados a través de internet o la red local.

IP Address

Una dirección única que identifica a un dispositivo en internet o una red local.

IP Address Management (IPAM)

Un conjunto integrado de herramientas de hardware y/o software que permite planificar, desplegar, gestionar y supervisar la infraestructura de direcciones IP de principio a fin. IPAM descubre automáticamente los servidores de la infraestructura de direcciones IP y los servidores DNS de una red y permite a los administradores gestionarlos desde una interfaz central.

M

Managed Detection & Response (MDR)

Una combinación de tecnología y experiencia humana para llevar a cabo la búsqueda de amenazas, supervisión y respuesta. El uso de MDR puede ayudar a identificar y limitar rápidamente el impacto de las amenazas sin necesidad de personal adicional.

Managed Service Provider (MSP)

Un proveedor que gestiona y asume la responsabilidad de un conjunto definido de servicios de gestión diaria a sus clientes. Estos pueden incluir la red, bases de datos y otros servicios generales de apoyo de TI. Es habitual que organizaciones de todos los tamaños utilizar los MSPs.

Managed Security Service Provider (MSSP)

Un proveedor de supervisión y gestión de dispositivos y sistemas de seguridad. Los servicios MSSP pueden incluir la gestión de firewall, detección de intrusiones, VPNs, escaneo de vulnerabilidades y servicios antivirales. Un MSSP puede proporcionar planificación y servicios de respuesta a incidentes.

Multifactor Authentication (MFA)

Un método de autenticación que requiere que un usuario proporcione dos o más factores de verificación para obtener acceso a un recurso, incluyendo aplicaciones, plataformas, cuentas y procesos. Estos factores de verificación suelen ser una combinación de algo que el usuario conoce

(por ejemplo, contraseña), algo que el usuario tiene (por ejemplo, token) y/o algo que el usuario es (por ejemplo, huella digital). El MFA es un componente esencial de una sólida política de IAM y puede ayudar a reducir la probabilidad de un ciberataque exitoso.

P

Protected Health Information (PHI)

Cualquier información creada, utilizada o divulgada durante la prestación de servicios de salud que pueda utilizarse para identificar a una persona. Algunos ejemplos pueden incluir fechas, como la de nacimiento, la de alta, la de ingreso y la de defunción; identificadores biométricos, como las huellas dactilares y las impresiones de voz; e imágenes fotográficas de todo el rostro y cualquier otra imagen comparable, junto con un vídeo de sus movimientos.

Personally Identifiable Information (PII)

Cualquier información que permita inferir directa o indirectamente la identidad de una persona, incluyendo cualquier información que esté vinculada o sea vinculable a esa persona.

R

Recovery Time Objective (RTO)

El tiempo objetivo establecido para recuperarse de cualquier interrupción.

Remote Desktop Protocol (RDP)

Un protocolo de comunicaciones de red seguro desarrollado por Microsoft. RDP permite a los administradores de red diagnosticar remotamente los problemas que los usuarios individuales enfrenten y otorga a los administradores acceso al ordenador del usuario.

RDP puede ser útil para una variedad de usuarios - por ejemplo administradores responsables del mantenimiento del sistema y empleados que necesitan acceder a sus ordenadores en la oficina mientras trabajan desde casa o están de viaje, pero debe ser gestionado adecuadamente.

S

Security Information & Event Management (SIEM)

Software que proporciona un análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones y el hardware de la red. El software SIEM empata los eventos con las reglas y los motores de análisis y los alinea para detectar y analizar las amenazas avanzadas utilizando la inteligencia global. Esto proporciona a los profesionales de la seguridad de la organización visibilidad y un registro de las actividades dentro de sus entornos de TI proporcionando análisis de datos, correlación de eventos, agregación, informes y gestión de registros.

Security Operations Center (SOC)

Un grupo centralizado de personas que utiliza herramientas de hardware y software que supervisa, previene, detecta, investiga y responde a las ciberamenazas las 24 horas del día.

Software-as-a-Service (SaaS)

Un método de entrega de una aplicación a través de internet como un servicio. También se conoce como software basado en la web (web-based software), software bajo demanda (on-demand software) o software alojado (hosted software).

En lugar de instalar y mantener el software, los usuarios acceden al SaaS a través de internet. El proveedor administra el acceso a la aplicación, incluyendo la seguridad, disponibilidad y el rendimiento, liberando al comprador de las responsabilidades de tener que mantener y gestionar el software.

Structured Query Language (SQL)

Un lenguaje de programación informático estándar utilizado para almacenar, manipular y recuperar información en una base de datos. Ciberdelincuentes utilizan la inyección SQL como forma de atacar un sistema informático.

SQL Injection

Una forma de violación de seguridad en el que un atacante suministra SQL en forma de solicitud de acción a través de un formulario web, directamente a una aplicación web para obtener acceso al backend de la base de datos (parte que procesa la entrada desde el frontend que es la parte que interactúa con el usuario) y/o datos de la aplicación. Esto puede causar un comportamiento involuntario y malicioso en la aplicación objetivo. Normalmente, este tipo de ataque es exitoso debido a la falta de verificación de la entrada del usuario en una aplicación web - por ejemplo, permitiendo a los usuarios suministrar código de aplicación SQL en formularios HTML en lugar de cadenas de texto normales.

System & Organization Controls (SOC II)

Una norma de cumplimiento voluntario para las organizaciones que especifica cómo las compañías deben gestionar los datos de los clientes. La norma se basa en varios criterios de servicios de confianza, como la seguridad, disponibilidad, integridad, confidencialidad y privacidad.

V

Virtual Private Network (VPN)

Una conexión de red protegida cuando se utilizan redes públicas. Las VPN cifran el tráfico de internet y ocultan la identidad del usuario en línea, lo que dificulta que terceros rastreen sus actividades en línea y roben datos. El cifrado se realiza en tiempo real.

W

Web Application Firewall (WAF)

Un sistema que protege las aplicaciones web de una variedad de ataques a la capa de aplicación, como XSS, inyección SQL y envenenamiento de cookies, entre otros.

Los ataques a las aplicaciones son una causa importante de brechas de seguridad - son la puerta de entrada a los datos valiosos de cualquier organización. Una organización puede bloquear el conjunto de ataques que tienen como objetivo exfiltrar datos comprometiendo sistemas a través de las aplicaciones web mediante el uso de WAF.

PARA MAYOR INFORMACIÓN

Ricardo Millán
Head ProFin México
Lockton México
ricardo.millan@lockton.com

LOCKTON®

UNCOMMONLY INDEPENDENT

 |