MARAMBIO, RIVILLO, PÉREZ, PINEDA
CONSULTORES Y CONTADORES PÚBLICOS

Hablemos de **CIBERSEGURIDAD**

www.marambio-hlb.com

TOGETHER WE MAKE IT HAPPEN

Actualidad y Conocimientos | Agosto 2023

Introducción a la Ciberseguridad:

Hablamos de ciberseguridad al referirnos al conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que una organización emplea para proteger sus datos y archivos, así como para proteger a los usuarios en el ciberentorno.

De ahí que englobe todos los conceptos que rigen la seguridad en la red o Internet desde datos personales, información bancaria, claves de acceso a herramientas y plataformas, compras realizadas online, entre otros. Con toda la cantidad de información que circula por la red, los riesgos se hacen cada vez más visibles, tanto para el usuario de a pie como para las empresas, independientemente de si son grandes empresas, pymes o cualquier autónomo o emprendedor. Incluso las instituciones públicas tampoco están libres de sufrir un ciberataque (el evento no intencionado de incumplimiento y acceso no autorizado a un sistema informático, una red o recursos conectados se denomina ciberataque). Es por ello que, ante un ciberentorno cada día más y más grande, el aspecto fundamental para garantizar la seguridad total de todos nuestros movimientos en tan extensa red, es la ciberseguridad.

Pero, ¿qué diferencias hay entre la ciberseguridad y la seguridad de la información? Asociar el término de ciberseguridad al de seguridad de la información no es del todo correcto. La ciberseguridad busca proteger la información digital en los sistemas que se encuentran interconectados, y, a su vez, está comprendida dentro de la conocida seguridad de la información.

A modo de ejemplo diferenciador de ambos términos, cuando se busca proteger el hardware, redes, software, infraestructura tecnológica o servicios, nos encontramos en el ámbito de la seguridad informática o ciberseguridad. Y si hablamos de actividades de seguridad relacionadas con la información que manejan las personas, seguridad física, cumplimiento o concienciación, a lo que nos referimos es a la seguridad de la información (que tendrá siempre un alcance mayor que la ciberseguridad).

Los delincuentes cibernéticos suelen llamarse “crackers”, no “hackers”, ya que, aunque ambos son expertos en colarse en sistemas de seguridad, los “crackers” lo hacen con propósitos ilícitos. También son conocidos como “hackers de sombrero negro” (del inglés, black hat), mostrando sus habilidades en informática rompiendo sistemas de seguridad de ordenadores, colapsando servidores, entrando en zonas restringidas, infectando redes o apoderándose de ellas, entre otras.

¿Por qué es importante la ciberseguridad?

En los negocios de varios sectores, como la energía, el transporte, el comercio al detal y la fabricación, se usan sistemas digitales y conectividad de alta velocidad para proporcionar un servicio eficiente al cliente y ejecutar operaciones empresariales rentables. Igual que protegen los recursos físicos, deben proteger también los recursos digitales y los sistemas frente al acceso no intencionado. El éxito de un ciberataque produce la exposición, sustracción, eliminación o alteración de datos confidenciales. Las medidas de ciberseguridad defienden frente a ciberataques y proporcionan los siguientes beneficios:

Prevención o reducción del costo de las brechas de confianza**,** las organizaciones que implementan estrategias de ciberseguridad minimizan las consecuencias no deseadas de ciberataques que pueden afectar a la reputación empresarial, las capacidades financieras, las operaciones empresariales y la confianza del cliente. Por ejemplo, las compañías activan planes de recuperación de desastres para contener las posibles intrusiones y minimizar las interrupciones en las operaciones empresariales.

Mantenimiento de la conformidad normativa**,** las empresas de sectores y regiones específicos deben cumplir con los requisitos normativos para proteger los datos confidenciales frente a posibles riesgos cibernéticos. Por ejemplo, las empresas que operan en Europa deben cumplir el Reglamento General de Protección de Datos (GDPR), que espera que las

organizaciones adopten las medidas de ciberseguridad adecuadas para garantizar la privacidad de los datos.

Mitigación de las ciberamenazas en desarrollo, los ciberataques evolucionan a la par que las tecnologías cambiantes. Los delincuentes utilizan nuevas herramientas y elaboran nuevas estrategias para el acceso no autorizado al sistema. Las organizaciones emplean y actualizan las medidas de ciberseguridad para mantenerse al día de estas tecnologías y herramientas de ataque digital nuevas y en desarrollo.

¿Cuáles son los tipos de ataque contra los que intenta defender la ciberseguridad?

Los profesionales de ciberseguridad se esfuerzan por contener y mitigar las amenazas, tanto nuevas como existentes, que se infiltran en los sistemas informáticos de distintas maneras. A continuación, se ofrecen algunos ejemplos de ciberamenazas comunes:

Malware, significa software malintencionado. Incluye una variedad de programas de software creados para permitir que terceras partes accedan de manera no autorizada a información confidencial o interrumpan el funcionamiento normal de una infraestructura crítica. Entre los ejemplos más comunes de malware se incluyen los troyanos, spyware y virus.

Ransomware, hace referencia a un modelo empresarial y a un amplio rango de tecnologías asociadas, que los delincuentes pueden usar para cifrar los archivos de la víctima y exigir un rescate en dinero para recuperarlo y extorsionar a entidades y organizaciones.

Ataque de intermediario, implica que una parte externa intenta acceder de forma no autorizada por una red durante un intercambio de datos. Dichos ataques aumentan los riesgos de seguridad de la información confidencial, como los datos financieros.

Phishing, es una ciberamenaza que usa técnicas de ingeniería social para engañar a los usuarios a fin de que revelen información de identificación personal. Por ejemplo, los atacantes cibernéticos envían correos electrónicos que inducen a los usuarios a hacer clic e introducir los datos de la tarjeta de crédito en una página web de pagos ficticia. Los ataques de phishing también pueden incitar a la descarga de datos adjuntos malintencionados que instalen malware en los dispositivos de la empresa.

DDoS, es un ataque de denegación de servicio distribuido (DDoS) es un trabajo coordinado para sobrecargar un servidor enviando un gran volumen de solicitudes falsas. Estos eventos impiden que los usuarios normales se conecten o accedan al servidor de destino.

Amenaza interna, es un riesgo de seguridad introducido por personal con malas intenciones dentro de una organización. El personal posee acceso de alto nivel a los sistemas informáticos y puede desestabilizar la seguridad de la infraestructura desde dentro.

¿Cómo funciona la ciberseguridad?

Las organizaciones contratan especialistas de ciberseguridad para la implementación de las estrategias de ciberseguridad. Estos especialistas evalúan los riesgos de seguridad de los sistemas informáticos existentes, redes, almacenamiento de datos, aplicaciones y otros dispositivos conectados. A continuación, los especialistas de ciberseguridad crean un marco de ciberseguridad integral e implementan medidas protectoras en la organización.

Un programa de ciberseguridad de éxito implica la formación de los empleados sobre las prácticas recomendadas de seguridad y la utilización automatizada de tecnologías de defensa cibernética para la infraestructura de TI existente. Estos elementos trabajan juntos para crear varias capas de protección contra posibles amenazas en todos los puntos de acceso a datos. Identifican el riesgo, protegen las identidades, la infraestructura y los datos, detectan anomalías y eventos, responden y analizan la causa raíz y realizan la recuperación después de un evento.

¿Cuáles son los tipos de ciberseguridad?

Un enfoque sólido de ciberseguridad aborda los siguientes problemas de una organización: Ciberseguridad de la infraestructura crítica, seguridad de la red, seguridad en la nube, seguridad de IoT, seguridad de los datos, seguridad de las aplicaciones, seguridad de los puntos de conexión, planificación de la recuperación de desastres y continuidad del negocio, educación del usuario final.

¿Cuáles son los componentes de una estrategia de ciberseguridad?

Una estrategia sólida de ciberseguridad requiere un enfoque coordinado que implica a las personas, los procesos y la tecnología de una organización.

Personas: La mayoría de los empleados no conocen las amenazas y las prácticas recomendadas de seguridad más recientes para proteger sus dispositivos, red y servidor. La formación y educación de los empleados con respecto a los principios de ciberseguridad reduce los riesgos de descuidos que pueden dar lugar a incidencias no deseadas.

Procesamiento: El equipo de seguridad de TI desarrolla un marco de seguridad sólido para el monitoreo e informe continuado de las vulnerabilidades conocidas en la infraestructura informática de la organización. El marco es un plan táctico que garantiza que la organización va a responder y recuperar de inmediato las posibles incidencias de seguridad.

Tecnología: Las organizaciones utilizan tecnologías de ciberseguridad para proteger los dispositivos conectados, los servidores, las redes y los datos frente a posibles amenazas.

¿Qué son las tecnologías modernas de ciberseguridad?

Se trata de tecnologías que ayudan a las organizaciones a proteger sus datos, las mismas se detallan a continuación:

Confianza cero, es un principio de ciberseguridad que presupone de forma predeterminada que ninguna aplicación ni usuario es de confianza, incluso si están alojados dentro de la organización. En su lugar, el modelo de confianza cero presupone un control de acceso de privilegios mínimos, que requiere la autenticación estricta por parte de las autoridades respectivas y el continuo monitoreo de las aplicaciones.

Análisis del comportamiento, monitorea la transmisión de datos desde dispositivos y redes para detectar actividades sospechosas y patrones anómalos. Por ejemplo, se alerta al equipo de seguridad de TI de un pico repentino de transmisión o descarga de datos de archivos sospechosos a dispositivos específicos.

Sistema de detección de intrusiones, las organizaciones usan sistemas de detección de intrusiones para identificar y responder con rapidez a un ciberataque. Las soluciones de seguridad modernas usan machine learning y el análisis de datos para descubrir amenazas inactivas en la infraestructura informática de la organización.

Cifrado de la nube, cifra los datos antes de almacenarlos en las bases de datos de la nube. Impide que partes no autorizadas hagan un uso indebido de los datos en posibles brechas de seguridad.

Conclusión:

La transformación digital plantea entornos en las empresas cada vez más amplios, complejos, y con un mayor riesgo frente amenazas como consecuencia de un medio cada vez más expuesto al exterior. Por tanto, el crecimiento tecnológico en las compañías debe ir alineado al crecimiento en ciberseguridad, para garantizar el correcto funcionamiento de los nuevos servicios y activos digitalizados que se incorporen.

No es posible establecer un entorno 100% seguro en una organización, por lo que es necesario realizar con frecuencia auditorías que indiquen los niveles de seguridad para ser conscientes de los riesgos que está asumiendo una compañía y descubrir nuevos agujeros de seguridad.

MARAMBIO, RIVILLO,
PÉREZ, PINEDA
CONSULTORES Y CONTADORES PÚBLICOS

Contactos

Para nuestra Firma es muy importante estar en constante comunicación con usted, por ello, ponemos a su disposición nuestra ubicación a fin de atender sus requerimientos.

DIRECCIÓN:
Av. Francisco de Miranda,
Multicentro Empresarial del Este,
Torre Miranda Nivel SF. Chacao,
Caracas-Venezuela.

TELÉFONOS:
Máster: 58 (212) 264.01.60
267.79.89 / 267.79.42
Fax: 58 (212) 263.55.38

CORREO ELECTRÓNICO:
marambio@marambio-hlb.com

WEB:
marambio-hlb.com

@Marambio_hlb

@Marambio.hlb