HERRAMIENTAS DE CIBERSEGURIDAD EN 2022

EBOOK

2022

ADM Cloud & Services

ÍNDICE

03 TIPOS DE AMENAZAS
04 ¿SABÍAS QUÉ...?
05 SOLUCIONES
06 CONCLUSIÓN

TIPOS DE AMENAZAS

En la actualidad, los ataques cibernéticos no solo aumentan, sino que también mejoran sus técnicas de ataque, por ello, herramientas que antes eran efectivas, ahora se quedan obsoletas, necesitando actualizar este tipo de protección a medida que evolucionan las amenazas o ataques informáticos.

PHISHING

A través de una suplantación de identidad, el phising envía correos electrónicos fraudulentos con el objetivo de robar datos sensibles como números de tarjetas de crédito. Es el tipo más común de ciberataque.

RANSOMWARE

Software malicioso que tiene el objetivo de bloquear el acceso a archivos o sistemas. Los ciberdelincuentes acostumbran a pedir un dinero a cambio de la recuperación de la información, teniendo un coste de más de 30.000€ de media. Se propaga a través de correos electrónicos de Spam con enlaces infectados o archivos adjuntos.

MALWARE

Software creado para obtener accesos no autorizados o causar daños a equipos informáticos. Un malware puede infectar un ordenador a través de diversas formas, por ejemplo, descargas de software de una fuente dudosa, adjuntos en correos electrónicos, navegación web o descarga de archivos en sitios webs pirateados.

INGENERÍA SOCIAL

Técnica utilizada por los ciberdelincuentes que tiene como objetivo conseguir datos confidenciales del propio usuario. Los ataques de ingenia social no solo se realizan a través de internet, también pueden ser fuera de las redes como por ejemplo un dispositivo USB.

¿SABÍAS QUÉ...?

Según un nuevo informe de *Cybercrime Magazine* estima que los costos globales del delito cibernético crecerán un 15% durante los próximos años, alcanzando los $10,5 billones de dólares anuales para 2025, esta estimación se basa en cifras históricas de ciberdelincuencia.

SECTORES MÁS AFECTADOS POR CIBERDELINCUENTES

Según Hornetsecurity Lab, estos son los sectores que más ataques reciben por parte de los ciberdelincuentes, se puede observar el ranking de mayor a menor.

1.SECTORES DE LA FABRICACIÓN
2.INVESTIGACIÓN
3.MEDIOS DE TRANSPORTE
4.EDUCACIÓN
5.MEDIOS
6.AUTOMOCIÓN
7.SECTOR DEL ENTRETENIMIENTO
8.SECTOR HOTELERO
9.SECTOR DE LA AGRICULTURA
10.SECTOR SANITARIO

EMPRESAS CON MÁS SUPLANTACIONES DE IDENTIDAD

Los expertos de Hornetsecurity Lab, han creado un ranking de las empresas y organizaciones que más han sido suplantadas.

1.AMAZÓN
2.OTROS
3.DEUTSCHE POST/DHL
4.DOCUSIGN
5.PAYPAL
6.LINKEDIN
7.MICROSOFT
8.1&1
9.O2
10.FACEBOOK

SOLUCIONES

GESTIÓN DE REVISIONES

Cada vez más distribuidores de informática ofrecen valor añadido a sus clientes. Ese valor añadido ofrece actualizaciones de software, como, por ejemplo, actualizaciones en Windows, o revisiones del funcionamiento en las herramientas de ciberseguridad implementadas a los clientes.
Todo ello, es muy complicado, por tanto, con una herramienta de monitorización de sistemas informáticos, los distribuidores pueden ofrecer un valor añadido a sus clientes gracias a las funciones de automatización y programación que ofrecen este tipo de herramientas.

PROTECCIÓN WEB

Cada vez es más necesario disponer de un sistema que pueda bloquear el intento de acceso a URLs maliciosas, ya que los ataques de phishing u otros tipos de ataques son muy frecuentes cuando un usuario accede de forma inconsciente a un sitio web malicioso.

ANTIVIRUS AUTOGESTIONADO

Para prevenir los ataques de malware se utilizan antivirus actualizados, aunque cada vez se están quedando más obsoletos en la lucha contra amenazas, por ello, se opta por utilizar un software EDR. Los EDRs ofrecen a los proveedores de servicios gestionados un único panel para simplificar las implementaciones y gestiones masivas del día a día en dispositivos o servidores como también programar análisis automatizados.

FILTRADO DE CORREO ELECTRÓNICO

Uno de los clásicos en ciberseguridad. Permite hacer un análisis a los mensajes entrantes y salientes para detectar dominios, textos, URLs o adjuntos maliciosos.
El software de filtrado de correo electrónico protege a los clientes frente a ataques de phishing, spam, malware o rasomware. Los distribuidores de valor añadido tienen un total control sobre las listas blancas, listas negras y políticas de cuarentena, ofreciendo a su correo electrónico una mayor protección frente amenazas.

COPIAS DE SEGURIDAD O BACKUP

Sin duda, es recomendable hacer copias de seguridad, ya que en caso de un ciberataque a su empresa puede perder toda la información disponible en sus dispositivos, como, por ejemplo, un ordenador.

Este tipo de software, se encarga de crear una copia de seguridad en la nube, permitiendo restaurar la información de una forma rápida y sencilla.

CONCLUSIÓN

Las últimas amenazas cibernéticas observadas en 2021 superan tecnologías débiles y obsoletas o redes mal aseguradas.

Para superar estas nuevas amenazas cibernéticas, las empresas u organizaciones necesitan soluciones de protección modernas y actualizadas, por ejemplo, las herramientas nombradas en este documento.

Para más información contacta con nosotros ahora.