CIBERSEGURIDAD
Y SU IMPORTANCIA PARA PROCESOS CRÍTICOS

PROCETRADI

Las compañías con operaciones críticas del sector industrial se enfrentan hoy en día a un riesgo digital creciente: el **ciberataque**, el cual consiste en utilizar las debilidades y vulnerabilidades de los sistemas corporativos para colectar la información, explotar deliberadamente sistemas informáticos, redes independientes, entre otros.

El fin de estos ataques con código malicioso es el de alterar la información y provocar delitos cibernéticos, como el de amenazar y perjudicar las operaciones en curso, robo de información, robo de identidades y pedir una recompensa a cambio.

Para prevenir estos ciberataques existen actualmente prácticas de seguridad que protegen los activos y las redes de las empresas: la **ciberseguridad**.

¿Qué es la ***CIBERSEGURIDAD?***

La **ciberseguridad** es la práctica para la protección de **redes**, **activos** e **infraestructura digital** contra ciberataques maliciosos ocasionados por hackers. Se espera que en lo que va del año 2021 la cifra en daños ocasionados por estos ataques supere los 6 billones de dólares y que los sectores con operaciones críticas y demandantes estén invirtiendo en infraestructura de ciberseguridad para proteger tanto la **red IT** (Tecnologías de la información) y la **red OT** (Tecnologías de la operación).

BENEFICIOS

- Previene el acceso de usuarios no autorizados.
- Protección perimetral a las empresas de operaciones criticas contra ciberataques enfocados en objetivos que comprometen la continuidad de las operaciones.
- Protección de los datos y redes.
- Disminuir el tiempo de recuperación ante intentos de ciberataques.
- Brinda confianza en la continuidad de las operaciones.

¿Qué es un ***CIBERATAQUE?***

Es un intento deliberado por parte de hackers que atacan e intentan explotar y comprometer la integridad, disponibilidad y confidencialidad de los **sistemas informáticos** de una organización.

Se utilizan distintos métodos, procedimientos ilegales con el objetivo de causar daño e interrumpir la operación para acceder a los recursos internos como las computadoras, dispositivos, aplicativos, redes, bases de datos, **SCADA**, **RTUs**, **IED's**, etc.

Tipos de CIBERATAQUE

Los ciberataques se presentan en diferentes formas, se pueden presentar como ataques abiertos de **ransomware**, que consiste en el secuestro de información, productos o credenciales a cambio de dinero.

También hay de la forma en que los hackers se pueden infiltrar dentro del sistema de una empresa para recabar información valiosa y esto se llega a descubrir después de meses.

Algunos de los **ciberataques** más comunes son los siguientes:

- **Ingeniería social**

  Es un conjunto de técnicas que consiste en **manipular psicológicamente** a las personas para que brinden su información privada. Consiste en engañar a usuarios para el envío de datos confidenciales, mediante mensajes, correos, mensajes de voz, entre otros.

- **Pishing**

  Consiste en un método de envío de **comunicaciones maliciosas** utilizadas para engañar y conseguir información personal, contraseñas, datos privados, cuentas de banco, entre otros.

  Generalmente son en forma de correos o mensaje de texto utilizando nombres, logos, redacción y correos similares a entidads reconocidas. Una vez que se hace clic en el link del mensaje falso, los ciberdelincuentes pueden tener acceso a los datos confidenciales que la persona haya brindado.

- **Malware**

  Consiste en un **programa malicioso** o **código maligno** que realiza acciones dañinas a un sistema de forma malintencionada, infringiendo las redes a través de una vulnerabilidad.

  Por ejemplo, cuando se hace clic en enlaces de correo electrónicos sospechosos o se instala una aplicación peligrosa. Una vez dentro de la red, el malware puede obtener información confidencial e incluso provocar un daño en toda la red.

Ransomware

Es un **tipo de malware** que no permite acceder a las redes, archivos, fotos personales comprometiendo toda la información y solicitando una recompensa por los **datos secuestrados**.

Cuando el atacante logra ingresar a una red mediante el software malicioso, lo que realiza es **bloquear** la pantalla o **cifrar** la información personal para solicitar un rescate en forma de dinero para que la victima pueda recuperar su información.

Ataque Man in the Middle

Es un tipo de ataque que ocurre cuando los ciberdelincuentes se infiltran en medio de un tráfico entre una **comunicación** entre dos partes. El objetivo del ataque Man in the Middle es obtener información **confidencial** de los usuarios, páginas **webs** o **base de datos** de importantes empresas.

Ataque de día cero

Es un tipo de ataque que es desconocido para usuarios y fabricantes de productos de seguridad. Su objetivo es ejecutar códigos maliciosos donde se encuentran vulnerabilidades en la red.

La mayoría de las empresas no están preparadas para estos ataques recientes, por lo cual, luego de reportar estos ataques por parte de fabricantes de productos, recién salen actualizaciones de parches de seguridad que los mitigan.

Seguridad EN LA RED

Actualmente vivimos en una época de cambios tecnológicos variables y las **amenazas cibernéticas** son cada vez más difíciles de detectar. Las empresas de operaciones criticas recurren a una variedad de soluciones para obtener una protección integra de sus datos y redes.

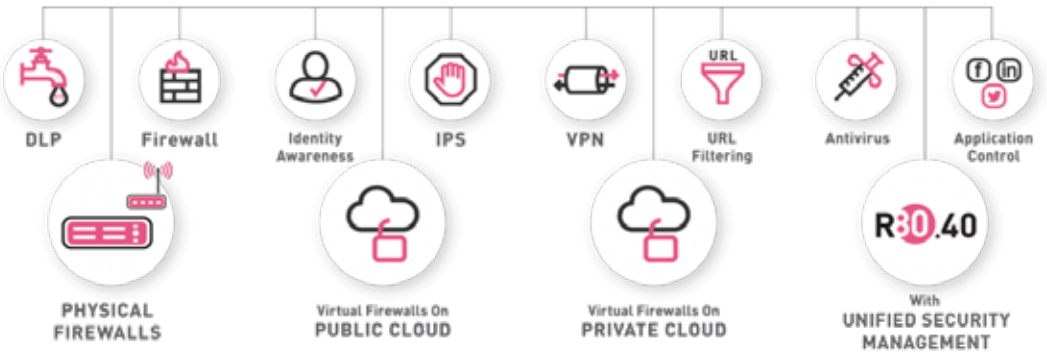
Para ello, en **PROCETRADI**, en alianza con CHECK POINT SOFTWARE TECHNOLOGIES, ofrecemos soluciones de seguridad de red que simplifican la seguridad sin afectar el rendimiento de la red, ni comprometer las operaciones, brindando un enfoque único para operaciones optimizadas que permite escalamiento para un crecimiento empresarial continuo.

¿Por qué es necesario proteger MI EMPRESA DE LOS CIBERATAQUES?

Toda **red** necesita de una defensa contra los distintos tipos de ciberataques, y la defensa avanzada contra ellos implica muchas capas de protección, incluyendo análisis continuos de la red. Los equipos **firewall** de red pueden brindar protección contra: **virus**, **troyanos**, **spyware**, **adware**, **ransomware**, entre otros.

Los **firewalls** de próxima generación (**NGFW**) de **Check Point** son capaces de identificar y bloquear completamente un malware antes de que ingrese a una red de operaciones críticas. Detecta y combate ataques rápidamente en toda la red, siendo un componente esencial

de solución de **ciberseguridad** para empresas del sector industrial, eléctrico, minero, entre otros, ya sea que se encuentre en un **data center**, en **red** o en la **nube**.



Ciberseguridad para sistemas ***DE CONTROL INDUSTRIAL***

Los sistemas de control industrial (ICS) utilizados en la **infraestructura crítica** y las industrias de fabricación, son objetivos comunes de los ciberataques actuales. Para ello, nuestro partner Check Point ofrece un Gateway de Seguridad "**Check Point** Quantum Rugged ™ 1570R" que brinda seguridad integrada para la implementación en entornos industriales como parte de una solución completa de **seguridad ICS** de extremo a extremo.

Además, ofrece prevención de amenazas para la protección de sistemas de control industrial en los sectores fábrica, energía, servicios públicos y transporte.

Transporte **Petróleo** **Fabricación** **Energía** **Utilidades**

En **Procetradi** brindamos soluciones de **ciberseguridad** para entornos industriales y de operaciones críticas, que garantizan la integridad de su entorno OT, protegiendo su red de para una mejor segmentación y concentrando mayor atención en los riesgos de OT, vulnerabilidades y adaptación de políticas basadas en inteligencia de amenazas.

Si deseas más información, escríbenos a **marketing@procetradi.com** para que uno de nuestros especialistas pueda contactarse con usted.

PROCETRADI

www.procetradi.com