Cómo prevenir un ciberataque en su negocio y no ser hackeado en el intento

Rafael Marín

¿Deseas aprender cómo prevenir un ciberataque y tomar las medidas oportunas? En este post te damos las claves.

Pocas cosas son más peligrosas para un negocio o empresa que sufrir un **ciberataque** bien ejecutado.

Debido a ello, es primordial tomar **medidas significativas** para mejorar la seguridad de la red y prevenir un ciberataque que ponga en jaque la información de la empresa.

Si te interesa descubrir ciertas **claves para prevenir un ciberataque** en cualquier empresa sigue leyendo este artículo.

Cómo evitar un ciberataque empresarial

Las empresas y las organizaciones deben proteger sus datos de las numerosas **vulnerabilidades** cibernéticas que existen, y eso comienza con una **estrategia bien planificada**.

Contrariamente a la creencia popular, los ciberdelincuentes pueden apuntar a empresas de cualquier tamaño, por lo que se debe tener un plan para proteger y prevenir un ciberataque en su empresa, incluso si es un pequeño negocio.

De hecho, **las pymes y entidades similares tienen la misma probabilidad de enfrentarse a un ciberataque**.

La falta de recursos adecuados para monitorear y mantener las medidas de ciberseguridad suele ser lo que hace que las pymes sean tan vulnerables a los ataques.

Para intentar evitar estos ciberataques, a continuación, se darán una serie de claves a seguir para prevenir un ciberataque:

Utilizar autenticación multifactor

Una de las formas más efectivas de prevenir un ciberataque es asegurarse de que la **autenticación multifactor** esté habilitada para todas las aplicaciones que acceden a Internet en su empresa.

Tener solo una contraseña de inicio de sesión para los empleados no es suficiente. Si las contraseñas de los empleados se ven comprometidas a través de un pirateo o una estafa de phishing, los ciberdelincuentes pueden acceder fácilmente a los sistemas.

En cambio, habilitar un proceso de autenticación de múltiples factores para los inicios de sesión requerirá que los empleados proporcionen varios datos en lugar de solo uno.

Como resultado, la seguridad aumentará. Será mucho más difícil para cualquier persona no autorizada acceder a los sistemas.

Crear controles internos sólidos

Para prevenir ciberataques en una empresa, también es fundamental contar con **controles internos sólidos**.

Los controles de acceso ayudarán a garantizar que el acceso al sistema se actualice inmediatamente una vez que los empleados, contratistas y proveedores abandonen la organización.

Controlar el acceso al sistema es esencial. Cuando alguien abandona la empresa, debe revocar el acceso por razones de seguridad. Si no revoca el acceso de ex empleados, contratistas y otras partes relevantes, es posible que puedan acceder al sistema más adelante.

Al **monitorear** quién tiene acceso a los sistemas, se garantiza una mayor seguridad y se evitarán problemas potenciales.

Responsabilidades de seguridad de terceros

Si desea prevenir ataques cibernéticos y amenazas de seguridad, también es fundamental que tome medidas para gestionar el **riesgo cibernético de terceros**.

Es importante comprender las responsabilidades que tiene cuando se trata de seguridad de terceros.

Si hay proveedores o terceros que necesitan acceder al sistema, es fundamental estar al tanto de los riesgos y garantizar una mayor seguridad.

La creación de estrictos controles de seguridad, la identificación de amenazas potenciales y el monitoreo de red son aspectos cruciales para garantizar que el sistema sea seguro.

Hay que asegurarse de comprender plenamente las **responsabilidades**. Se debe evitar las vulnerabilidades de terceros si se desea que el negocio sea lo más seguro posible.

Educar a los empleados en materia de seguridad

La **educación de los empleados** también es una de las claves más importantes para mejorar la seguridad empresarial.

Es necesario realizar una capacitación exhaustiva de concienciación sobre ciberseguridad al incorporar nuevos empleados. También se debe proporcionar entrenamiento adicional en intervalos regulares.

La celebración de **sesiones de formación anuales** puede ayudar a garantizar que todo el personal sepa cómo prevenir un ciberataque.

También es importante educar sobre phishing. Hay que hacer entender a los empleados qué no se consideran solicitudes normales por correo electrónico y otros métodos de correspondencia.

Al tener un equipo bien informado, podrá crear un negocio mucho más seguro en general.

Crear copias de seguridad de datos

También es importante realizar copias de seguridad periódicas de los datos empresariales importantes. Hacer una copia de seguridad de los datos es una parte esencial para que un negocio funcione bien.

Es una medida importante que se debe tomar para evitar el peor de los casos en el que se pierden datos empresariales cruciales.

Si bien las otras acciones que tome para prevenir las amenazas de ciberseguridad deberían ser suficientes para proteger el negocio, a veces, independientemente de las medidas que se tomen, los ciberataques siguen ocurriendo.

Como resultado, es posible encontrar que los datos se borraron o corrompieron debido a un ataque cibernético. Al crear copias de seguridad de datos periódicas, se asegurará de que, pase lo que pase, su negocio no sufrirá pérdidas totales.

Evitará que sus operaciones comerciales se detengan. Podrá volver a encarrilarse más fácilmente después de que se produzca un ciberataque o una brecha de seguridad.

Mantener los sistemas actualizados

Mantener los sistemas y software empresarial actualizados también es una parte fundamental para proteger una empresa.

Los sistemas siempre deben ejecutar el software más reciente si se desea que los datos estén seguros.

Si bien algunos propietarios de negocios se sienten frustrados por la necesidad de actualizaciones constantes, son necesarias. De vez en cuando, surgirán nuevos problemas y vulnerabilidades en el software empresarial.

Existen actualizaciones para parchear las vulnerabilidades del software y para protegerse contra posibles amenazas a la seguridad.

A veces hay gastos importantes asociados con las actualizaciones de software y hardware. Sin embargo, el resultado suele merecer la pena.

No actualizar el sistema y el software con regularidad hará que todo el sistema sea vulnerable a amenazas. Como resultado, la empresa puede experimentar reveses importantes.

Instalar un antivirus y un firewall en cada equipo

El último paso a tomar para evitar violaciones de seguridad y prevenir un ciberataque es instalar un antivirus y un firewall.

Es necesario instalar antivirus y firewalls en todos los equipos que tenga la empresa y **actualizarlo** con regularidad.

Tener un antivirus y un firewall por sí solo no es suficiente para proteger completamente la empresa de las amenazas de seguridad.

Sin embargo, si se usa con las otras estrategias enumeradas anteriormente, se podrá crear un enfoque integrado para la seguridad del sistema.

Aprender a prevenir un ciberataque

Si está tratando de descubrir cómo **prevenir un ciberataque** para su empresa, debe asegurarse de tener en cuenta los consejos anteriores.

El uso de estas estrategias puede ser increíblemente útil para proteger la red empresarial y prevenir amenazas a la seguridad.

Extractado de: