Publicado en España el 18/06/2021

Ciberataques: la importancia de la ciberseguridad. Por LQN Soluciones

Durante la pandemia se ha producido un notable aumento de los ciberataques que violaron datos sensibles, vulneraron sitios y obligaron a bloquear máquinas

Las empresas españolas deben prepararse para el futuro, y para ello no hay más remedio que confiar en la ciberseguridad y que las empresas refuercen sus sistemas de seguridad mediante el adecuado mantenimiento informático de sus infraestructuras.

Desde el inicio de la digitalización, la ciberseguridad ha sido uno de los aspectos más importantes a tener en cuenta. Hoy en día, todas las empresas gestionan datos valiosos que almacenan en sus servidores físicos o en la nube, y empresas enteras dependen de las infraestructuras informáticas. El comercio electrónico, las bases de datos llenas de información sensible y datos confidenciales y los sistemas tecnológicos corren constantemente el riesgo de sufrir ciberataques.

Precisamente por eso, la ciberseguridad debe considerarse una partida importante en el presupuesto de TI: tanto los propietarios de las empresas como los clientes deben sentirse seguros, y también sus datos.

La infraestructura de TI debe defenderse de los constantes ataques y violaciones, y las plataformas tecnológicas deben permanecer online y funcionando las 24 horas del día para evitar ralentizaciones y caídas de las máquinas.

La importancia de este punto ha aumentado aún más durante esta pandemia mundial, y en 2021 hay una tendencia al alza de los ciberataques realmente preocupante.

Auge de los ciberataques

El Covid-19 provocó una repentina y frenética digitalización de los negocios y las empresas que se encontraron adoptando entornos tecnológicos sin la debida preparación y transición de un sistema a otro. La rápida modernización de las PYMES fue el escenario perfecto para un aumento exponencial de los ciberataques.

De hecho, muchas empresas carecían de sistemas de ciberseguridad adecuados, lo que los llevó a sufrir graves violaciones de la protección de datos.

Según algunos estudios realizados, una de cada tres operaciones en España está amenazada debido a infracciones de la cadena de suministro. El 26 % de las infracciones se produjeron en la cadena de

suministro, esto se debe a la facilidad con la que los hackers son capaces de infiltrarse en los vectores de ataque en dichas cadenas. También fueron altos los porcentajes de ataques a sistemas operativos, 18%, y a aplicaciones web, 14%.

Los datos restantes son alarmantes:

El 99% de las empresas españolas han afirmado haber sufrido un ciberataque en los últimos 12 meses y una posterior violación de datos
Ha habido una media de 2,2 infracciones por empresa
El 85% de las empresas ha confirmado que los ataques se han vuelto más sofisticados, y el 5% que se han vuelto significativamente más avanzados.
El 98% de los profesionales de la seguridad han confirmado un aumento del volumen de ataques.

En consecuencia, se puede afirmar que ha habido un aumento significativo de los ataques debido a la pandemia. Los ciberdelincuentes han aprovechado esta pandemia, ya de por sí nefasta, para lanzar ataques de forma aún más masiva. Alguna web de la administración pública ha sido hackeada, al igual que los sistemas corporativos y postales.

¿Por qué es tan importante la ciberseguridad?

No se puede pensar en la ciberseguridad como una partida más que añadir a los gastos de funcionamiento de una empresa.

Ni mucho menos: la ciberseguridad es una de las inversiones más valiosas para el futuro. Hoy en día, la seguridad informática de los datos y el tiempo de funcionamiento de los sistemas tecnológicos es vital.

De hecho, los costes de las filtraciones de datos sensibles o la interrupción de las máquinas y el entorno informático son mucho más caros que cualquier medida preventiva. Por eso se debería invertir en:

Gestión de identidades y accesos
Gestión de la vulnerabilidad
Gestión de riesgos y cumplimiento
Detección y prevención de intrusiones

No hay que subestimar, la protección que puede asegurar una copia de seguridad en la nube o una recuperación ante desastres, gracias a la cual se podrá recuperar los datos perdidos o robados durante una violación o un ataque de hackers, con el fin de limitar los daños sufridos.

El mercado de la seguridad de la información es tan importante que, según algunas estimaciones, superó los 1.300 millones de euros. Es evidente que las empresas lo consideran una inversión fundamental en innovación tecnológica. También se estima que en 2021 el gasto mundial en ciberdelincuencia alcanzará los 11,4 millones de dólares por minuto.

El reto de la ciberseguridad en 2021

A medida que aumentan las estrategias de trabajo inteligente y crecen los entornos de TI en todo el mundo, la ciberseguridad desempeñará un papel cada vez más importante y es una de las tendencias tecnológicas con más crecimiento.

Los ciberataques aumentarán, como prevén los expertos y también las violaciones de datos sensibles, a menos que las empresas confíen en soluciones de ciberseguridad que aseguren su infraestructura y los datos almacenados en ella. Las novedades informáticas adelantan que estas soluciones serán una de las partidas más importantes en inversión de las empresas.

El lanzamiento del 5G también podría aumentar significativamente las infracciones de los ciberdelincuentes. De hecho, el 5G aumentará el ancho de banda general, incrementará la cantidad de dispositivos IoT conectados y casas domóticas con tecnología para evitar robos y todos estos avances harán los ataques DDoS más frecuentes.

El reto será, por tanto, ayudar a las empresas a modernizar y digitalizar sus sistemas y, al mismo tiempo, garantizar que sus entornos informáticos estén protegidos de los ataques de los ciberdelincuentes con un adecuado mantenimiento y reparación de ordenadores. Esto incluirá también la concienciación sobre la tecnología.

Cómo defenderse de los ciberataques entrantes

Un primer paso clave es la evaluación informática. Esta evaluación examinará detalladamente el entorno informático de la empresa e identificará cualquier problema o carencia. De este modo, saldrán a la luz los fallos del sistema de seguridad que pueden solucionarse gracias a la asistencia informática adecuada.

Otra alternativa lógica es solicitar a una consultoría en seguridad informática que vaya a implementar nuevas y más eficaces soluciones para proteger el departamento de informática y garantizar a los clientes una gestión segura de los datos sensibles. Esto permitirá a la empresa una mejor gestión del tiempo, dedicándose a aspectos relacionados con el propio negocio y dejando a los especialistas todos los aspectos relacionados con la seguridad informática.

Para proteger una empresa de los ciberataques, se puede recurrir a un proveedor de servicios externos. Al externalizar la gestión del entorno informático, se podrá aumentar el nivel de seguridad,

gracias a un soporte proactivo que mantendrá los sistemas actualizados y seguros, e intervendrá al instante si fuera necesario.

Datos de contacto:
LQN SOLUCIONES
Comunicado de prensa de LQN SOLUCIONES
912 42 60 06

Nota de prensa publicada en: España

Categorías: Nacional Programación Madrid Software Ciberseguridad