Seguridad de la red: los nuevos retos del mantenimiento informático, por LQN SOLUCIONES

Multimedia

Las amenazas cibernéticas adoptan diferentes formas a lo largo del tiempo. Con el auge de la tecnología digital, también se están extendiendo cada vez más, provocando que las empresas sean las primeras en sufrir las consecuencias a través de la red informática

Los líderes empresariales deben ser conscientes de los nuevos problemas de seguridad en la red, esto permitirá encontrar y adoptar soluciones eficaces a través del mantenimiento informático.

¿Cómo garantizar la seguridad de la red informática de una empresa?
Tener presencia en Internet se ha convertido en algo esencial para cualquier negocio que quiera crecer. Les permite llegar a más clientes y abrir un mercado más amplio de consumidores.

Sin embargo, cuanto mayor sea la presencia online, mayor será el riesgo. Por ello, es necesario asegurarse de que la red informática es segura y protegerla de cualquier ataque.

Actualmente, las soluciones tradicionales de seguridad informática ya no son suficientes para hacer frente a las nuevas amenazas. Por lo tanto, es necesario reforzar el sistema corporativo adoptando las soluciones más adecuadas:

Disponer de un sistema de seguridad informática fiable
Un sistema de seguridad bien diseñado tiene todas las herramientas para preservar la integridad de una red contra cualquier intrusión.

Este sistema se encarga de proteger toda la comunicación de la empresa de los hackers. También ayuda a preservar el sistema de información controlando el acceso a todos los recursos. Sin embargo, este sistema sólo es fiable si es capaz de garantizar todas estas funciones.

Por lo tanto, hay que tener en cuenta que el mantenimiento informático, refuerza la seguridad permitiendo a la empresa protegerse a sí misma y a los clientes.

Para proteger el sistema de información, también se debe prestar atención a la composición de los equipos. Aquí hay que asegurarse de que haya uniformidad en el conjunto de ordenadores.

Por lo general, se recomienda que las empresas utilicen el mismo sistema operativo para todos los dispositivos si es posible. De este modo, las actualizaciones periódicas serán idénticas para cada dispositivo o servidor.

> *Un dispositivo antiguo en un parque informático puede ser una puerta abierta para los ciberdelincuentes.*

Realizar controles periódicos de los dispositivos
Además de establecer un sistema de mantenimiento informático, es necesario supervisar el sistema de seguridad regularmente de todos los dispositivos, esto requiere realizar pruebas de intrusión.

Este tipo de control debe ser dominado por todos los empleados que garantizan la seguridad de una red informática. Este control se realiza a través de determinadas herramientas como antivirus, cortafuegos y otras herramientas de detección de ataques cibernéticos.

Hay que tener en cuenta que no se puede confiar únicamente en un antivirus para proteger los datos. Por eso, es importante dirigirse a una empresa especializada en servicios de mantenimiento informático.

Estas empresas son capaces de ofrecer una arquitectura de red personalizada que se adapte perfectamente a las necesidades de cada empresa, asegurando el mantenimiento informático constante de la red.

Concienciar al resto del equipo
Tener un sistema de seguridad de red segura con actualizaciones regulares no es suficiente para tener una protección total. Hay que saber que la seguridad del equipo informático también depende en gran medida de cómo se utilice. Por ello, los expertos en seguridad informática recomiendan que las empresas eduquen a los empleados en las buenas prácticas.

> *Los empleados deben ser conscientes de que todo lo que hacen en los ordenadores implica la seguridad de la empresa.*

La formación sobre buenas prácticas es necesaria para prevenir cualquier fallo. En este contexto, algunas empresas incluyen estas buenas prácticas que permiten evitar cualquier mal uso de la herramienta informática que pueda provocar un mal funcionamiento del sistema.

Controlar el acceso a las redes
Para proteger los activos informáticos de los ataques externos, también es importante aumentar el control del acceso a los mismos. Por ello, es importante tener un control total sobre todos los usuarios de la red.

La empresa también puede comprobar regularmente todo el software o los programas instalados en un sistema. Además, debe asegurarse de que los

empleados no instalen ningún programa, aplicación o software que no haya sido verificado y autentificado, anteriormente.

Otra forma eficaz de verificar el acceso de la red es limitar el acceso al Wi-Fi. Para ello, es necesario poder restringir el acceso sólo a las instalaciones de la empresa y evitar cualquier intrusión desde el exterior.

¿Por qué subcontratar la seguridad informática a terceros?
Como se ha mencionado anteriormente, garantizar la seguridad de los activos informáticos no es una tarea que se pueda improvisar, ya que requiere formación y experiencia.

La externalización informática ofrece ventajas a las empresas:

- En primer lugar, esta supervisión de seguridad la llevan a cabo profesionales equipados con herramientas de alto rendimiento.
- Estos expertos pueden garantizar la seguridad de una red informática a diario.
- Realizan regularmente auditorías organizativas o técnicas, así como análisis de los riesgos de intrusión del sistema.
- Estos expertos también pueden asesorar a las empresas sobre cómo anticiparse y proteger la red de cualquier ataque.
- C o m o especialistas en ciberseguridad, estos expertos investigan constantemente los nuevos métodos utilizados por los hackers. Así, son capaces de encontrar soluciones para evitar cualquier intrusión.

Diferentes tipos de seguridad que hay que aplicar
Para garantizar la seguridad de una red informática, hay algunos dispositivos esenciales que hay que poner en marcha:

Cortafuegos
Los cortafuegos proporcionan una barrera entre los empleados y las redes externas. Estos cortafuegos utilizan un conjunto de reglas creadas por un experto en seguridad informática para permitir o bloquear el tráfico. Este dispositivo puede ser software, hardware o ambos.

Antivirus
A veces llamado antimalware, el antivirus está diseñado para bloquear todos los ataques contra la red informática. Protegen el ordenador de virus, troyanos, spyware, gusanos y ransomware.

Los hackers utilizan ahora técnicas más sofisticadas, por eso es importante contar con un excelente programa antimalware. Estos programas se encargan de escanear y eliminar todo el malware a medida que entra. También supervisan todos los archivos existentes en busca de posibles anomalías para eliminarlas y reparar los daños.

La nube

Antes de la llegada de la nube, las empresas almacenaban los datos internamente en soportes físicos. Actualmente, la mayoría de las empresas eligen la nube para almacenar información por sus múltiples ventajas.

Con la nube, los empleados pueden acceder a los datos de la empresa estén donde estén. La nube le protege del riesgo de robo de datos y piratería informática. Además, permite ahorrar dinero, porque ya no es necesario invertir en hardware. Al migrar el servidor a la nube, se disfruta de una mayor seguridad.
