Así se protegen las empresas ante los ciberataques

Noviembre de 2022

El número de **ciberataques** que sufren las empresas hace necesario que la seguridad sea un asunto de máxima importancia. Situar el concepto de ciberseguridad en todas las decisiones que toma la empresa a cualquier nivel es la tendencia actual para minimizar los riesgos e incrementar el nivel de protección de datos y sistemas informáticos empresariales.

El auge del teletrabajo, la implementación del *cloud computing* y el uso de internet como principal canal de comunicación de las empresas, ha disparado los ciberataques, poniendo de manifiesto la **necesidad de protección de cualquier empresa**, independientemente de su tamaño o del sector en el que opere.

Podemos ver cómo las empresas más importantes del mercado apuestan por **la ciberseguridad como uno de los cimientos de su negocio**. La inversión en dispositivos, *software* y formación en este aspecto se ha disparado durante los últimos años, siendo una clara muestra de la necesidad de situar la ciberseguridad en el centro del negocio.

Veamos cómo se están preparando y protegiendo las empresas ante los principales tipos de ciberataques.

Protección contra el *phishing*

El usuario es el punto débil de todo sistema informático y es el principal objetivo de los ciberdelincuentes para conseguir vulnerar sistemas y acceder a ellos de forma remota con objetivos maliciosos.

El ***phishing* o robo de identidad** es uno de los grandes problemas en ciberseguridad actualmente, pues los métodos que utilizan los ciberdelincuentes para engañar a los usuarios y conseguir sus credenciales de acceso son realmente sofisticados.

Las empresas se protegen de este tipo de ataques mediante la **aplicación de herramientas de *software* específicas, como filtros avanzados en las cuentas de correo** para eliminar de forma automática mensajes sospechosos. Sin embargo, la mejor alternativa para minimizar el riesgo de sufrir este tipo de ataques es la inversión en formación en ciberseguridad, preparando a los usuarios para poder defenderse ante esta práctica fraudulenta.

Incluso algunas empresas organizan **sesiones de ataques *phishing* como simulacros** para poder aprender de ellas y aplicar las mejores técnicas de defensa.

Protección contra el *ransomware*

Durante la etapa de pandemia fueron muchas las empresas que sufrieron ciberataques de secuestro o *ransomware*. El impacto de estos ataques en la empresa es realmente profundo, pues encripta toda la información impidiendo el acceso a los datos y sistemas informáticos, lo que **puede llegar a paralizar por completo un negocio**.

La defensa y protección contra esta gran ciberamenaza se encuentra en la apuesta por nuevos métodos como **continuidad de negocio (*disaster recovery)* y copias de seguridad o *backups* en la nube**.

La **defensa proactiva** es otra de las apuestas para defender a la empresa contra ataques de *ransomware* y de otro tipo de *malware*. Por ejemplo, empresas como Caixabank disponen de un equipo especial de respuesta que **monitoriza la red empresarial 24/7** con el objetivo de detectar cualquier patrón o comportamiento sospechoso, para así poder actuar incluso antes de que un ciberataque ocurra.

Protección contra los ataques de denegación de servicio

Otro de los riesgos de seguridad a los que se enfrentan las empresas actuales es el del ataque contra sus servidores. Los **ataques DDoS o de denegación de servicio consisten en saturar los servidores de la empresa con infinidad de peticiones de acceso**, que terminarán con un anómalo funcionamiento de los mismos, o de la propia caída de un servidor.

La apuesta por **proveedores *cloud* de garantía a la hora de confeccionar la infraestructura empresarial** es una de las mejores decisiones para que las empresas se protejan de este tipo de ataques. Apostando por proveedores en la nube de servicios *cloud* profesionales se dispondrá de un **mayor nivel de protección, ya que este tipo de empresas utilizan tecnologías y protocolos avanzados de seguridad**.

Si las empresas tienen sus servidores en la nube, difícilmente pueden ser afectados por este tipo de ataques por diversos motivos.

- Los proveedores disponen de las **tecnologías más avanzadas** para detectar y defenderse de los ataques DDoS.
- Con un proveedor *cloud* se dispondrá de una disponibilidad total de los servidores, ya que están **basados en tecnologías de virtualización**, es decir, si un servidor falla se implementa otro de manera inmediata (garantizan la continuidad del negocio).

Acciones proactivas y *backup* profesional

Las principales apuestas de las empresas en la actualidad, además de la formación de los usuarios, se centra en dos puntos fundamentales:

1. **Acciones proactivas**. Para poder garantizar el mayor nivel de ciberseguridad es necesario contar con sistemas proactivos de monitorización y defensa que permitan actuar de manera inmediata (incluso ante de que ocurra un ciberataque).
2. **Sistemas de *backup***. Contar con un sistema de copias de seguridad periódicas, automatizadas (sin intervención del usuario) y en distintos soportes es clave para garantizar la continuidad del negocio (siempre hay una copia actualizada y protegida de los datos y sistemas de la empresa).

La **ciberseguridad gestionada** por una empresa especializada del sector que cuente con un centro de operaciones de seguridad (SOC) es la mejor alternativa para proteger los datos y sistemas de una empresa.

Los **ciberataques** son una realidad a la que cualquier negocio debe enfrentarse hoy en día, por lo que la prevención y formación en ciberseguridad debe ser una prioridad para tu negocio.