Los ciberataques en empresas aumentaron un 150% y el principal vector de entrada de virus es el error humano

Expertos en ciberseguridad analizan los riesgos de ataques que existen para las empresas y desvelan las claves para proteger a tu negocio de cualquiera de estos fraudes: la lucha empresarial contra el phising, el ransomware y el malware

España **es uno de los países que más ciberataques sufre a nivel mundial**, teniendo en cuenta que las consecuencias que sufren las empresas son económicas, reputacionales y operativas. Cualquier negocio debe tener un buen sistema de protección, por consiguiente, necesitan el asesoramiento de profesionales para tener mecanismos de prevención.

El principal objetivo de los ciberataques es acceder a los datos privados de una empresa para impactar negativamente en su imagen y en la confianza de los clientes. Iosu Arrizabalaga (CEO de Factum) señala que "en los últimos años, los ciberataques han superado los porcentajes que conocíamos. **Solo en 2021 aumentaron en un 150% y cada vez son más las vías de entrada para aprovechar cualquier brecha de seguridad".**

Dichos ataques cibernéticos pueden suponer el cierre de la actividad empresarial porque los costes son inasumibles, además, **una falta de diligencia en el deber de protección supone sanciones.**

¿Estamos expuestos a los ciberataques?

Jesús Yanes (director de Desarrollo de Negocio de EnGenius) asegura que **"lo estamos, en mayor o menor medida dependiendo de la tecnología y el equipamiento WiFi que utilicemos**. Negarlo sería una ilusión, especialmente en un momento histórico como este, en el que el dato ha cobrado la relevancia actual. Sin entrar a pormenorizar las distintas consecuencias del robo de datos, sabemos que nuestra información depende del grado de seguridad personal o corporativa que hayamos interpuesto".

Las obligaciones de seguridad que tiene una empresa

El responsable de datos debe aplicar las medidas necesarias para impedir cualquier vulnerabilidad, de esta manera, **la empresa tendrá que justificar qué prevenciones ha tomado.**

Cualquier negocio tiene que ser capaz de gestionar los sistemas de información mediante medidas físicas y técnicas para mantener la confidencialidad, disponibilidad y la integridad de sus recursos. Asimismo, **tienen que llevar a cabo evaluaciones de riesgos y están obligados a asegurar la información de los trabajadores y clientes.**

A pesar de los grandes avances tecnológicos, Hervé Lambert (Global Consumer Operations Manager de Panda Security) afirma que "si bien hay entidades que certifican medidas de seguridad, vemos que **hay empresas que carecen de sistemas, profesionales y que siguen protegiendo sus activos de la peor forma posible**. A nivel de concienciación, tenemos mucho, muchísimo que hacer. Estamos mejor que hace diez años, pero hay mucho margen de mejora".

Mientras tanto, Mario García (director general de Check Point Software para España y Portugal) añade que “en el año 2021, a través del Boletín Oficial del Estado, **se regularon las obligaciones de determinados operadores a la hora de proteger sus redes y sistemas de información**. La nueva norma exige que el Responsable de Seguridad de la Información dispone de los medios adecuados para realizar sus funciones de una forma eficaz, con personal capacitado y los recursos necesarios”.

La importancia de protegerse para que un negocio funcione correctamente

Una empresa no puede defenderse de las campañas de violación de datos sin un programa de ciberseguridad, además, los lugares de trabajo deben incluir programas de concienciación sobre seguridad cibernética para educar al personal.

Carlos Borrego (Cybersecurity Service Delivery Manager de Bidaidea) señala que todas las organizaciones deberían tomar medidas para protegerse de un posible ciberataque. La protección no solo se basa en una serie de controles genéricos, sino que han de ser un conjunto de medidas adaptadas al contexto de cada organización. **La ciberseguridad no es un coste sin retorno, sino que es una inversión que permitirá la implantación de medidas y el entrenamiento del personal mediante la formación.**

Quién debe hacerse responsable del ciberataque

Jesús F. Rodríguez (CEO de IberBox) afirma que “el Reglamento General de Protección de Datos deja clara la figura del responsable del tratamiento de datos, que es quien recopila el dato. Por tanto, **si ocurre un ciberataque, la Agencia Española de Protección de Datos incidirá inicialmente en el responsable del tratamiento”.**

Por otro lado, **la responsabilidad recae en quien ejecuta la acción y en quien no actuó con la diligencia exigible**. Iosu Arrizabalaga añade que “la víctima es la empresa y la responsabilidad primera siempre es del delincuente, la realidad es que deber ser la misma entidad afectada la responsable de la toma de decisiones y de medidas paliativas”.

Javier Huergo (director de Watch&Act Protection Services) indica que “**en todas las empresas debe existir un responsable de ciberseguridad (CISO)** que ponga en marcha todos los mecanismos necesarios para mitigar lo antes posible un ciberataque y coordine todas las acciones necesarias para volver a funcionar en la mayor brevedad posible”.

Los riesgos que corre el cliente ante un posible ciberataque de la empresa

Sufrir un ciberataque puede suponer un parón temporal o el cese total de la actividad. Los ciberdelincuentes acceden a los sistemas y sustraen los datos privados externos, conllevando responsabilidades subsidiarias y dejando al descubierto vías de entrada para atacar a terceros, ya sean proveedores, colaboradores y clientes.

Los ataques cibernéticos pueden detener las operaciones en línea en solo unos minutos y demorar semanas en resolverse. José Carlos Márquez (Education Manager en OpenWebinars) señala que “**el principal riesgo es el robo de información**. Los datos robados podrían usarse para exponerlos públicamente, realizar chantajes o extorsiones, o ser ofrecidos a la competencia”.

Aquellos clientes con datos personales comprometidos deben ser informados por parte de la empresa, de forma que puedan tomar las medidas necesarias para evitar problemas inmediatos o futuros.

Francisco Valencia (director general de Secure&IT) afirma que **los riesgos “dependen del tipo de ataque y tipo de empresa**. Hay ataques que son capaces de paralizar la actividad durante un período de tiempo más o menos extenso y, en consecuencia, esto implica que el cliente puede dejar de recibir servicios o suministros más o menos críticos”.

¿La vulnerabilidad depende de la empresa o del empleado?

Javier Huergo indica que “**el principal vector de entrada de virus informáticos viene provocado por errores humanos**, por ello, una buena formación a empleados y directivos en materia de ciberseguridad puede evitar muchos problemas”.

Valentín Cortés (Campus Manager de Madrid y Barcelona de Ironhack) agrega que “**los empleados son la mayor debilidad de la seguridad informática de una empresa**. Si los trabajadores no están capacitados, será difícil proteger los sistemas contra la variedad de amenazas que los ciberdelincuentes utilizan para robar datos”.

José Carlos Márquez informa que **la culpa “depende en parte de la empresa**, dado que tiene que dar los pasos para facilitar la adopción de esa Cultura de Seguridad a los empleados, pero también en gran medida del trabajador, porque accede a los datos con distintos niveles de sensibilidad y debe hacerlo siempre con responsabilidad”.

Qué vulnerabilidades existen

El aumento de los ciberataques aumentó a raíz del teletrabajo, debido a que se ha puesto a prueba las barreras de seguridad de las empresas y dificultó la labor de control sobre la actividad.

Desde el inicio de la pandemia destacan los ataques de ransomware. Esta vulnerabilidad provoca la encriptación de la información y paraliza la actividad de la empresa. Asimismo, en la mayoría de los casos, el pago de un rescate es la vía más rápida para retomar el funcionamiento del negocio.

Otros de los **riesgos** son:

- Fraude por phishing: Se simula un correo legítimo para engañar al usuario y conseguir algún dato personal relevante, como las claves de su banca online.
- Malware: Un fichero malicioso que se ejecuta e infecta el dispositivo.
- Scam: Se envía un correo para cometer una estafa basándose en supuestos ingresos económicos.

Cómo protegerse

En primer lugar, cualquier negocio se tiene que poner en manos de profesionales que protejan los datos de manera privada. Posteriormente, es recomendable tener un alto nivel de formación para evitar los posibles errores humanos.

Los usuarios se pueden proteger de la siguiente manera:

- Establecer una política de contraseña fuerte, con al menos ocho caracteres, mayúsculas, minúsculas, números y caracteres especiales.
- No hay que pinchar en los enlaces que se reciban por correo electrónico.
- Desconfiar de las redes WiFi públicas.
- Proteger todos los dispositivos mediante un antivirus con herramientas extra de seguridad, como almacén de contraseñas y verificador de enlaces o conexiones.
- Usar perfiles de usuario con permisos restrictivos que no permitan acceder a ninguna información más que la estrictamente necesaria para el desempeño profesional.
- Mantener los equipos bloqueados con contraseñas.

Medidas para evitar un ciberataque

Valentín Cortés recomienda las siguientes medidas:

- **Establecer prácticas y políticas** para proteger a la empresa de ataques cibernéticos y brindar pautas para resolver problemas.
- **Formar a los empleados** sobre su papel en la seguridad y protección de la información de sus compañeros, clientes y la empresa.
- **Capacitar a los empleados** para que puedan reconocer mensajes de advertencia de antivirus falsos y alertar tan pronto como noten que ocurre algo cuestionable.

Los negocios tienen que **realizar evaluaciones detalladas del estado en el que se encuentran para conocer los posibles fallos**, establecer un protocolo, analizar la actividad, hacer copias de seguridad, elaborar un Plan de Ciberseguridad personalizado y contar con un buen software de protección.

Otros de los requisitos mínimos son los antivirus, actualizaciones de software, doble factor de autenticación y una buena política de contraseñas.

Fuente: 20Minutos