Coronavirus: La seguridad en internet, en el punto de mira de las empresas

La implementación del teletrabajo como medida para prevenir la propagación del coronavirus (COVID- 19) ha disparado las brechas de seguridad informática en aquellos países poco acostumbrados a esta modalidad laboral

Cuando el mundo se medía por aquello que podíamos ver y palpar, las principales amenazas para nuestros negocios eran los robos físicos o los atracos más o menos violentos que preveníamos con sistemas como alarmas de seguridad. Ahora el mundo es global y está al alcance del teclado de un ordenador o de nuestro smartphone. Por ello, los ataques se han profesionalizado y son invisibles, sobre todo si llegan a través de métodos como un correo electrónico. **El uso del Covid-19 como cebo ha generado un volumen de ataques por correo electrónico que representa la mayor colección de tipos de ciberataque** registrados bajo un mismo tema en años o incluso en la historia, según la empresa de ciberseguridad Proofpoint.

Qué es la ciberseguridad

La ciberseguridad es la práctica de defender y proteger los servidores, teléfonos móviles, sistemas electrónicos, redes, etc. de los posibles ataques maliciosos de virus creados para robar dinero o información. La experta Lucía Arias, Lead Advisor Técnico Sector Público en la consultora en ciberseguridad Govertis, define la ciberseguridad como la protección de los procesos de negocio que tienen o utilizan tecnologías de la información como herramientas para su ejecución. La ciberseguridad contempla el análisis de los procesos, la tecnología y las personas para tratar de asegurar que no ocurren incidentes que afecten a la seguridad de la información, es decir, que vulneren la protección de la confidencialidad, la integridad y la disponibilidad de los sistemas y datos.

Hay muchas formas de ciberataques, dependiendo de su naturaleza y de su misión, entre ellas **los malware, que son softwares maliciosos que infectan los ordenadores, o el phishing que es la táctica de suplantación de identidad.**

El riesgo creciente de sufrir un ciberataque

Como el mundo en la red corre a una velocidad vertiginosa los ciberataques se han convertido en todo un reto para aquellos que estudian la seguridad en Internet, de hecho, **la afección es muy elevada y su impacto económico es mayor que cualquier otra actividad delictiva, supone 600.000 millones de dólares en la economía mundial y genera más dinero que el narcotráfico.** En una sociedad inmersa en procesos de transformación digital donde todo emplea tecnología, la ciberseguridad debe garantizar la supervivencia de las empresas, explica Arias. En España, el coste asciende a 40 millones de euros al año y, según un informe elaborado por Acierto.com, quienes más lo sufren son las pequeñas y medianas empresas, que soportan casi el 70 % de los ciberdelitos. ¿Esto significa que cualquier empresa, sea como sea, debe preocuparse por la ciberseguridad? Sí, porque las empresas ya no tienen las TICs como un apoyo, tal y como ocurría antes, ahora son herramientas esenciales sin las que no se pueden realizar las actividades propias de cualquier negocio. **Quién no se preocupa por la ciberseguridad no tiene garantizada la supervivencia en un mundo interconectado donde todo pasa por Internet**, afirma tajante la experta.

Campañas masivas, el principal riesgo

Las principales amenazas que una empresa o una organización de cualquier tipo puede tener son campañas masivas de ataques que penetran en el corazón de la organización y pueden paralizar la actividad interna a cambio de la petición de un rescate. Estos ataques no siempre van destinados al robo económico, en muchas ocasiones lo que interesa es la información. También se desarrollan para bloquear un sistema o dejar inoperativa una entidad durante un tiempo.

Deepak Daswani, experto en ciberseguridad y autor de La amenaza hacker (Ed. Deusto), coincide con Arias al afirmar que todas las empresas y organizaciones son sensibles a estos ataques, y apunta que el problema es que las pequeñas y medianas empresas no disponen de sistemas de seguridad avanzados para hacerles frente, **un ecommerce puede sufrir un ataque automatizado para tumbar el sistema, que se paralice su actividad, y puede recibirlo de su competencia**. La protección es muy importante ya que, si una tienda online, una organización o un ayuntamiento no gozan de un buen sistema de seguridad el ataque puede extenderse mucho, a través de vulnerabilidades se puede atacar una web para comprometer a los usuarios. Todo depende de la motivación del ataque. Como los ataques van por delante, uno de los principales problemas es la detección, **lo difícil es adivinar y saber que tienes un ataque, porque en ocasiones los hackers se cuelan y permanecen durante mucho tiempo robando información sin que la empresa sea consciente de ello.**

En los últimos años se ha intensificado el fraude en la red y, de momento, no existe un patrón que defina los ataques ni sus motivos. Hospitales, organizaciones públicas y empresas han sido víctimas de ciberataques recientemente, de hecho, 2019 fue un año muy convulso. Ransomware, un tipo de malware, atacó una gran cantidad de empresas y organizaciones, entre ellas, varios ayuntamientos, centros sanitarios y compañías privadas como la Cadena Ser, Prosegur o Everis. Estos ataques son muy sofisticados y se van renovando cada poco tiempo, por lo que son muy difíciles de contener. Por ello, Daswani señala que lo mejor es la prevención, los retos a los que nos enfrentamos en esta materia van encaminados a prevenir los ataques. **Las empresas deben ponerse al día en materia de ciberseguridad, deben seguir el decálogo de buenas prácticas, actualizar los sistemas, someterse a auditorías de seguridad y preparar a sus trabajadores para que sepan a lo que se están enfrentando**.

Para la experta de Govertis, el plan de contingencia ideal debe contemplar varias cuestiones: En primer lugar debe identificar las necesidades y los tiempos máximos de supervivencia de una empresa frente a un incidente. Debe, por lo tanto, conocer cuáles son los procesos críticos, cuánta gente como mínimo es necesaria para realizarlos y cuáles son las aplicaciones necesarias. El plan contempla dos cuestiones básicas: Gestionar la crisis, valorar el suceso y tomar decisiones; y, la segunda, gestionar las actividades de contención, respuesta y recuperación, añade.

Pero la fase clave es la de la prevención: Toda buena continuidad comienza con el proceso de análisis de riesgos que trata de identificar situaciones potenciales y plantear medidas preventivas para evitarlas. Además, se debe realizar un análisis de impacto en el negocio para conocer, si finalmente ocurre la contingencia, qué es lo más urgente, lo que antes debe volver a la situación de normalidad. No todo es necesario desde el primer momento y, por tanto, las organizaciones deben saber qué, cómo y cuándo deben restablecerse los procesos de negocio.

Los peligros del phishing

Otro de los grandes fraudes online son los que se cometen a través del phishing, que es la suplantación de identidad que se destina al robo de credenciales a los usuarios y que permite tener un primer acceso para el robo, o para lanzar un malware. Esta técnica es muy común y se cuela en nuestra actividad diaria. Muchas veces recibimos un supuesto mail inofensivo de una empresa o de una entidad que nos solicita un cambio de contraseña, o información personal e incluso un pago para una campaña y es falso.

El estafador utiliza el logotipo de la empresa a la que está suplantando e incluso un enlace a la web original. En la campaña de Navidad del año pasado Correos fue víctima de estos fraudes, los estafadores enviaron mensajes vía sms y mail donde solicitaban una pequeña cantidad de dinero para enviar un paquete a los destinatarios, aprovechando la época de gran volumen de envíos. La organización lanzó un comunicado alertando de que los mensajes eran falsos y que el usuario podría distinguirlos por la dirección de emisor. **Para protegerse de esta estafa se recomienda no dar datos personales por correo electrónico, cerciorarnos de que la dirección desde la que nos han enviado el mail es la correcta e ignorar todos aquellos correos de los que dudemos.**

El fraude en internet y el robo de datos son, en la actualidad, dos de los principales problemas y desafíos globales. Según el informe anual The Global Risks Report 2019, ocupa la cuarta posición, solo un puesto por encima de los ciberataques.

La aproximación del sector ha cambiado, antes se trabajaba para intentar impedir los ataques y ahora las organizaciones asumen que en algún momento van a ser atacadas, por lo que trabajan para estar lo más preparadas posible.

Fuente: El Economista