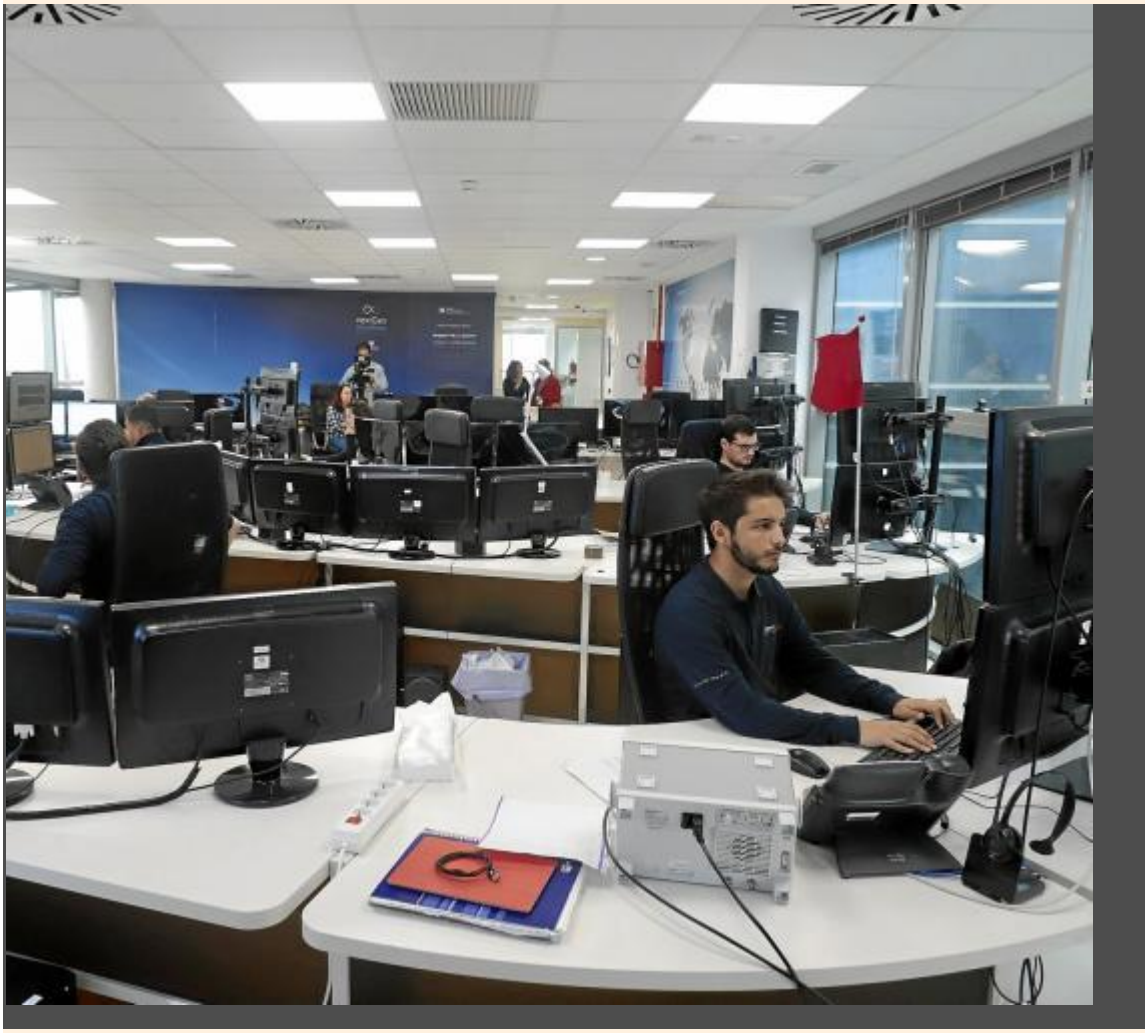
https://www.ultimahora.es/noticias/economico/2021/09/24/1303555/ciberataques-empresas-disparan-pandemia.html

Noticias | El Económico

Los ciberataques a empresas se disparan con la pandemia



Un incidente supone un perjuicio equivalenente al coste de proteger el sistema durante diez años. | **Pere Bota**

Aina Ginard24/09/21 11:27

Balears contaba el pasado mes de agosto con 43.347 empresas inscritas en la Seguridad Social. La inmensa mayoría no escapa de la amenaza de un ciberataque. El phishing, el ransomware y el secuestro del CEO son tres de los delitos a empresas más comunes, que además se han disparado desde el inicio de la pandemia. Una buena protección especializada así como la precaución individual a la hora de actuar son los principales mecanismos de defensa ante

estos ataques que pueden causar una debacle en un centro de trabajo, aunque los expertos dejan claro que la protección 100% no existe.

Alrededor del 10% de empresas tiene ataques que les causan grandes perjuicios. Es una cifra que proporciona Juanjo Fuster, gerente de Intec, una empresa mallorquina especializada en ciberseguridad con sede en el Parc Bit. “Calculo que un 10% de empresas tiene ataques que hacen desastres. Luego hay otras que no lo dicen, y otras que están protegidas y, en consecuencia, el ataque no llega a buen puerto”, señala.

La irrupción de la pandemia provocó un incremento del número de ataques que continúa este 2021. El teletrabajo improvisado con sistemas que no estaban preparados y organizado con prisas, el acceso de ciertos colectivos a servicios digitales por primera vez y la incertidumbre que se vivía por el desconocimiento de la COVID-19 fueron las causas principales.

“Desde nuestra perspectiva el número de ataques se ha disparado al menos un 50%. Hemos atendido incidentes millonarios a empresas de Balears que no son multinacionales. A algunas pymes les han robado más de un millón de euros. Hay casos de autónomos que han tenido que pedir préstamos o directamente cerrar por el perjuicio causado por el cibercrimen. O a algunos particulares les han robado los ahorros de toda la vida. Hablo de casos que he tratado”, añade Fuster.

TIPOS DE ATAQUE. El ransomware es uno de los ataques más frecuentes a empresas. Se trata de un secuestro de datos con la petición de un rescate económico a cambio de quitar las restricciones que impone el atacante. “Pueden pasar muchas cosas: que infecten con ransomware, que miren a quién envías correos y cambien números de cuenta... Entra un malware en tu red y empieza a cifrar equipos. Puedes perder toda la información que tienes y encima te cifran el Windows y no puedes trabajar, tienes la empresa parada. Pueden pasar meses hasta poder restaurar el sistema”, señala el experto.

El phishing también es común. Es a la vez un ataque y una técnica. “Si yo te quiero hackear, te envío un email haciéndote creer que soy otro para que abras un fichero adjunto o abras un enlace, y luego te infecto el equipo, te meto un ransomware y te lo cifro todo”, cuenta Fuster.

Mientras que en el secuestro del CEO alguien intercepta el ordenador y hace un seguimiento de rutinas y contactos. Cuando tiene la oportunidad, envía un email solicitando el pago de una cantidad o modifica de los documentos oficiales el número de cuenta corriente, de manera que el pago se efectúa donde no toca. Así se han llegado a robar decenas de miles de euros.

De acuerdo con la empresa multinacional de ciberseguridad Sophos, las empresas de distribución y transporte, los medios de comunicación y las compañías de ocio y entretenimiento están más preparadas para evitar que los atacantes cifren archivos. En cambio, los gobiernos locales y centrales, las entidades públicas independientes y la sanidad están más expuestos a un

cifrado de datos. Sin embargo, Fuster pone esta información en cuarentena. “No hay un ataque específico por sectores, están recibiendo por igual. El objetivo principal son autónomos y pymes de hasta 200 trabajadores porque no tienen seguridad”, explica.

PROTECCIÓN. ¿Qué puede hacer las empresas para evitar los ciberataques, sobre todo las pymes, que tienen menos recursos? Lo más fácil es la prevención. Es necesario contar con profesionales informáticos especializados en ciberseguridad, que no son los mismos que hacen páginas web o gestionan redes. “Un incidente puede suponer de media un perjuicio equivalente al coste de proteger el sistema durante diez años, según nuestros datos”, menciona el gerente de Intec. “Un atacante utiliza programas de software millonarios y funcionan según su retorno de inversión. Si no te pueden hacer nada en 24 horas, se van a otro”, comenta Fuster.

Además de proteger los equipos y las redes, hay una cuestión de precaución personal que no se puede obviar a la hora de clicar en enlaces o al abrir emails, mientras que otros ataques son inevitables. “Atacan con cualquier cosa. A través de wifi, a través de programas que puedas tener instalados, por una impresora, en el internet de las cosas... Solo un robot que barre me pide la clave del wifi, mi email y el teléfono y si consiguen entrar saben dónde vivo, cómo es mi casa, a qué horas no estoy...”, explica.

Preguntado por si deberíamos cerrar las sesiones abiertas, considera que no vale la pena. “No es solo cerrar las sesiones. También es tener la ubicación conectada, lo que dices en cualquier red, conectarte a redes inseguras, en ordenadores que no controlas... Los fallos no son de los sistemas, son de las personas. El delincuente siempre va por delante de nosotros”, concluye.