Para la ciberdelincuencia no hay vacunas: así es la pandemia que sacude a las empresas

Los ciberataques explotan todas las rendijas que compañías, empleados y directivos les ofrecen

Las **amenazas de ciberseguridad** hacia empresas se han incrementado en todo el mundo. La irrupción de la pandemia y los modelos de teletrabajo han facilitado el auge de los ataques en la red, y los hackers han sabido aprovechar que millones de empleados de organizaciones y administraciones públicas no tenían los **conocimientos y medios tecnológicos adecuados para el cambio de modelo.**

Entre 2020 y 2021 los ciberataques no sólo han crecido en número, sino también en variedad y calidad, buscando explotar todas las rendijas que les ofrecen las empresas, sus empleados y directivos. De esta manera, **la ciberseguridad ya no es algo nuevo y sus herramientas se han vuelto imprescindibles** en toda empresa que busca proteger sus sistemas, dispositivos y redes.

Un simple envío a un listado de direcciones email puede provocar el caos. Los ataques cibernéticos se presentan en diferentes niveles y consisten en una invasión a los sistemas informáticos de una empresa, entidad o persona con el objetivo de hacer daño, secuestrar datos o tomar el control del ordenador. **Entre los más sofisticados se encuentra el ciberchantaje o ransomware**. Convertido en el riesgo estrella, se trata de un programa de software dañino que restringe al acceso a determinadas partes del sistema operativo y exige el pago de una cantidad de dinero a cambio de eliminar la restricción.

Según el informe *Panorama actual de la Ciberseguridad en España de Google*, 7 de cada 10 ciberataques de ransomware son a pymes. Así, **los ciberdelincuentes siguen teniendo como principal objetivo las pequeñas compañías**, porque son las más vulnerables al no disponer de mecanismos de protección adecuados en la mayoría de los casos.

Una de las debilidades clave de la pandemia ha sido el uso de equipos personales compartidos con el resto de la familia, que pueden desvirtuar las medidas de protección empresarial si otra persona hace un uso inadecuado del mismo equipo. El **espacio familiar como entorno de trabajo puede ofrecer mucha información a ciberdelincuentes**, al igual que ocurre con la información que pueden obtener de las redes sociales una vez que han identificado el hogar del empleado o directivo y al resto de su familia.

Por otro lado, la **amenaza deepfakes no puede faltar como una de las grandes novedades** que comienza a ofrecer usos ilícitos. Se trata de técnicas de edición de vídeo que sustituyen a una persona por otra mediante la inteligencia artificial alcanzando resultados altamente realistas. Así, ofrecen a los cibercriminales nuevos recursos para sofisticar sus procesos de hackeo social y quebrantar contraseñas.

Según los datos de la compañía informática Kaspersky, España es el sexto país que más **ataques de phishing** sufre. Y no es de extrañar, porque **cada vez son más las noticias sobre este tipo de estafas por correo electrónico**. Tanto es así que en España, el Instituto Nacional de Ciberseguridad (INCIBE) ha detectado varias campañas de envíos de correos fraudulentos reemplazando a importantes entidades nacionales e internacionales. Desde bancos, empresas de tecnología, telefonía, financieras o eléctricas, todas han sido suplantadas por los cibercriminales.

Robar credenciales o acceder a las cámaras y micrófonos de los equipos son algunos de los nuevos métodos. Las técnicas se han sofisticado, **aprovechando fenómenos coyunturales como el incremento del uso de los correos electrónicos durante la pandemia** o saltándose los mecanismos de protección a través de nuevos canales de phishing como son el SMS o el uso de PDF infectados que, inconscientemente, se pueden relacionar con una actividad empresarial.

EMPRESAS Y BITCOINS: EN EL PUNTO DE MIRA

Si bien hasta ahora los ciberdelincuentes utilizaban el ransomware principalmente para estafar a particulares, en los últimos años su **atención se ha desplazado hacia las organizaciones.**

Con los nuevos métodos, los atacantes envían una solicitud de transferencia en bitcoin por valor de unos 4.000 euros a las **direcciones públicas de la empresa o mediante el formulario de comentarios en su página web.** Además, si se rechaza, amenazan con enviar cartas supuestamente firmadas por la víctima a través formularios de contacto de hasta 13 millones de sitios, así como spam agresivo en nombre de la empresa a 9 millones de direcciones postales. De esta manera, se identifica el sitio de la persona dañada como spam y se bloquea para siempre.

¿CÓMO SALVARSE?

No importa si la empresa es pequeña o grande. Todas tienen información valiosa y, para seguir con el negocio, resulta imprescindible establecer unas medidas básicas para evitar ciberataques. Esto ha provocado que el trabajador tenga que asumir el rol de **combatir la ciberdelincuencia y protegerse en su propio entorno laboral.**

La extraordinaria amenaza que supone la ciberdelincuencia ha puesto en valor los **sistemas de compliance de las empresas, como la herramienta más adecuada para formar y concienciar al personal** sobre estas graves amenazas, impulsando así comportamientos mucho más seguros en contextos de teletrabajo, afirma Francisco Bonatti, socio director de Bonatti Compliance.

Tal y como recoge el documento 10 amenazas de ciberseguridad que las empresas deben integrar en sus sistemas de compliance, de la compañía Bonatti Compliance, la solución pasa por **implementar protocolos, políticas y sistemas necesarios** en el equipo informático, de almacenamiento de datos y de comunicación.

En primer lugar, utilizar herramientas de protección contra malware en los distintos dispositivos y servidor, como software antivirus o programas antiespías, puede prevenir las pérdidas económicas y la desconfianza en la marca. El correo electrónico, por otro lado, es fuente de muchos ciberataques al tratarse de uno de los medios de comunicación online más utilizados por las empresas. **La encriptación de los mensajes, combinada con contraseñas seguras**, permite asegurar que no haya acceso de terceros a su contenido.

Pero **quizás la más importante de todas las medidas de seguridad es la de realizar copias de seguridad de los datos**. Realizando esta acción a través de un servicio profesional, se puede garantizar que la misma se ejecute de forma automática y externamente a la empresa. En caso de algún problema, ataque o pérdida, los datos y sistemas de la empresa podrán ser recuperados en un periodo corto de tiempo, minimizando las posibles pérdidas.

Fuente: Bolsamanía