La interconectividad creciente en la supply chain multiplica los efectos de los ciberataques

Las nuevas tecnologías y la creciente interconectividad que permiten entre los agentes de la cadena de suministro se presenta como una oportunidad para el sector, pero también como un riesgo potencial de cara a posibles ciberataques. Según la Organización Empresarial de Logística y Transporte (UNO), el 99,8% de las empresas no se considera a sí misma un objetivo atractivo para este tipo de crímenes, pero cuando ocurren, el coste medio para las pymes es de 35.000 euros. Asimismo, el presidente de la patronal, Francisco Aranda, ha señalado que "el 60% de las pymes cierra seis meses después de haberlo sufrido".

En unas jornadas celebradas en Barcelona, el director general de la consultora Aronte, Alex Barnadas, ha explicado que "dependemos muchísimo del correo electrónico y de la inmediatez de las cosas" y que, al utilizar esta tecnología "relativamente frágil», gran parte de los ciberataques entra por esta vía. "El

producto lo podemos volver a enviar", ha recordado a su vez el director Comercial y de Marketing de la empresa Ingram Micro, José Luis Nuño. "Pero si perdemos información, perdemos la confianza de nuestros clientes".

Otras estadísticas aportadas por UNO muestran que solo el 36% de las empresas dispone de protocolos básicos de seguridad, que el 14% actualiza sus contraseñas regularmente y que el 21% realiza copias de seguridad. Concretamente, según la patronal, en los últimos años se han multiplicado los ataques ramsonware, es decir, la encriptación de archivos para pedir un rescate económico. "Primero se empezó por encriptar un ordenador, luego la red, después la nube y ahora hasta los dispositivos móviles", ha advertido el teniente de la unidad técnica de la Policía Judicial en el área de Cibercrimen de la Guardia Civil, Carlos Vico.

Aunque el sector logístico no es una víctima específica de estos crímenes, el socio fundador de la agencia especializada en ciberseguridad Leet Security, Antonio Ramos, ha recordado que "todos somos el objetivo, el cibercriminal busca hacer dinero y, allí donde lo hay, va", especialmente ante la vulnerabilidad que supone una cadena de suministro cada vez más digitalizada. No obstante, Vico ha puntualizado que las nuevas tecnologías no suponen en sí una amenaza, pero que "cuanto más se modernicen, el nivel de seguridad deberá ser igualmente proporcional".

"Tenemos que pasar de una seguridad convencional con muchísimos puntos ciegos a un enfoque moderno, donde todos los sistemas implantados en las compañías se apoyen en la inteligencia artificial", ha afirmado el gerente territorial de cuentas de la empresa de ciberseguridad SonicWall, Joaquín Fernández. El director de Organización de la empresa de transporte Ader, Jorge Cruz, ha añadido que «el sector logístico puede construir esta tecnología de manera diferente" a otros ámbitos donde ya están más desarrolladas, como en el de la banca, de forma que "en vez de añadir seguridad a un sistema, podemos desarrollar el sistema a partir de la seguridad".

Otro crimen recurrente es el ataque conocido como 'fraude al CEO', en el que el ciberatacante se hace pasar por un empleado o directivo para conseguir un beneficio económico. Esta técnica requiere de sofisticación y preparación: comprobar dónde se encuentra la persona, mirar sus redes sociales y cómo se expresa, con el objetivo de realizar ataques de phishing relacionados con estafas. Ante esta situación, la Guardia Civil recomienda no compartir más información personal en internet y sospechar si se reciben correos donde piden el envío de dinero de forma urgente.

"Tenemos que estar continuamente alerta porque lo que nos esperamos que va a pasar, no pasa", ha opinado el responsable de Negocio _b first de Bytemaster, Javier Álvarez. "Estamos abocados a derivar una parte de nuestros beneficios a ciberseguridad, porque si no, los costes que tendremos serán muchísimo más altos". Concretamente, Álvarez ha explicado que se dan tres tipos de costes cuando se produce un incidente. A corto plazo, se tarda entre una y dos semanas en recuperar los datos que han sufrido el ataque; a medio plazo, la restauración total de los servicios; y a largo plazo, la estabilización y consolidación del nuevo entorno. No obstante, en último término, el coste más grande es la pérdida de clientes. "La seguridad es tan fuerte como el eslabón más débil", ha concluido Ramos. "Aplicado en el mundo de la seguridad, basta con encontrar un punto débil para acabar con una prestación del servicio".