Nota de prensa
24/10/2024

Expertos de Orange, Fortinet, AON y Cuatrecasas explican los retos en ciberseguridad que afronta el sector de la logística

En la jornada "Retos de la ciberseguridad en el sector de la logística" se dieron las claves para que las empresas puedan proteger sus infraestructuras, a nivel físico, jurídico y legal, de todo tipo de ciberataques.

Barcelona-Catalunya Centre Logístic (BCL), Orange Empresas y Fortinet, junto con la colaboración de Cuatrecasas y AON, han organizado hoy jueves 24 de octubre una jornada para desgranar desde diferentes disciplinas los retos que afronta el sector de la logística en materia de ciberseguridad.

La apertura de la jornada ha estado a cargo de Santiago Bassols, director general de BCL, Víctor Vera, director Empresas Territorial Cataluña de Orange, y Lluís Planas, Sales Manager de Fortinet. Todos ellos han coincidido en la necesidad que tienen las empresas del sector logístico de minimizar los riesgos ante los ciberataques y de fijar pautas de seguridad para proteger todas sus infraestructuras y comunicaciones confiando para ello en especialistas en ciberseguridad.

Seguidamente, Daniel Pastor, Cibersecurity Business Development de MASORANGE ha explicado las soluciones de ciberseguridad y EDR que la compañía ofrece al sector de la logística, las cuales permiten proteger las cadenas logísticas. En este sentido ha ofrecido dos datos relevantes: por un lado, que los ataques a la supply chain han crecido un 60% respecto al año 2023 y, por otro, que en el 93% de los casos los usuarios son el origen de los ataques. Por todo ello, las empresas "necesitan proteger sus puestos de trabajo y contar con especialistas", dado que el incremento de la información digital, la existencia de arquitecturas tecnológicas heterogéneas y un mundo más interconectado provocan que las empresas y las personas "estén más expuestas" a los ciberataques.

Daniel Pastor ha añadido que el cibercrimen "es un negocio muy lucrativo y profesionalizado" constantemente en aumento y con tendencia a "sofisticarse", utilizando para ello la Inteligencia Artificial, para atacar las cadenas de suministro donde la principal amenaza es el 'ransomware', cuyo objetivo es atacar sus dispositivos impidiendo el acceso a toda la información para, posteriormente, solicitar una cuantía económica por devolverlos a su estado original.

En este sentido, la propuesta de Orange ofrece asesoramiento integral y personalizado junto con una plataforma EDR (Endpoint Detection and Response) que ayuda a proteger los dispositivos de las empresas de forma automática. Esta plataforma realiza un análisis continuo por comportamiento, reduce la superficie de ataque a través del descubrimiento de dispositivos y

parches virtuales, detectando amenazas y protegiendo frente a ataques en tiempo real además de permitir la recuperación y restauración de los datos existentes antes del ataque, así como ofrecer una respuesta ante los incidentes personalizada para cada empresa.

A continuación, ha intervenido Marta Rofés, Directora Speciality Lineas Financieras y Cyber de AON, para hablar de las coberturas que las empresas tienen actualmente a su alcance para protegerse de la que ya es su primera preocupación y principal riesgo: "el ataque cibernético".

Ha destacado que el primer paso que hay que dar es el de "medir el grado de madurez en seguridad que tiene una empresa y saber cómo está respecto a su competencia" para poder "cuantificar el riesgo" antes de fijar un seguro. Para la experta de AON, "un ataque cibernético causa pérdidas económicas y reputacionales en una empresa, pero también puede causar daños a terceros", motivo por el cual conviene disponer de una póliza que cubra toda la cadena; desde el propio incidente, pasando por la posible filtración de datos, la extorsión, las multas o sanciones de las autoridades o los daños a terceros.

La siguiente intervención ha sido la de Ramón Badarat, Abogado de Cuatrecasas, que ha dado unas pinceladas sobre el marco legal y las nuevas normativas en materia de ciberseguridad, haciendo referencia a dos de las regulaciones europeas más importantes en vigor.

Por un lado, la Directiva NIS2 que refuerza los requisitos de seguridad que han de cumplir las entidades esenciales (de más de 250 trabajadores y más de 50 millones de euros de facturación) y las entidades importantes, ya sean públicas o privadas. Esta reglamentación determina "la gestión del riesgo y la ciberseguridad", obligando a las empresas a analizar los riesgos, a "asegurar la cadena de suministro y las relaciones con los proveedores", a notificar y reportar los ataques cibernéticos, a establecer medidas de formación tanto para empleados como para directivos, entre otras cosas. Asimismo, también establece pautas de gobernanza, de la que puede llegar a trascender que "un directivo sea considerado responsable y, por ello, se sancione a la empresa o, incluso, se releve al directivo de la organización".

La segunda normativa que ha destacado Ramón Badarat es el Reglamento de Ciberresiliencia, CRA por sus siglas en inglés, que obliga a los fabricantes y comercializadores de productos digitales (los conectados directa o indirectamente a otro dispositivo o a una red) a mejorar la seguridad de estos. Es decir, "tienen que garantizar que los productos con elementos digitales sean seguros de usar, resistentes a las amenazas cibernéticas y proporcionen suficiente información sobre sus propiedades de seguridad". No cumplir el CRA puede conllevar la imposición de elevadas sanciones entorno a los 15 millones de euros o el 2,5% del volumen de negocios global del infractor.

David García Cano, Manager Sales Specialist en Fortinet, ha cerrado la jornada exponiendo el estado actual de la ciberseguridad, destacando que las soluciones de detección y respuesta ante un ciberataque "llegan tarde" y es necesario "ir hacia modelos de predicción", aunque "no sepamos qué estamos buscando".

El experto de Fortinet ha recalcado que las motivaciones para atacar a una organización pueden ser de distinta índole: financieras, de espionaje industrial, de sabotaje o de control para atacar a otras empresas. Por esta razón, los procesos y productos que desarrollan sirven para "predecir, detectar, dar respuesta y protegerse de lo que puede llegar a pasar". Para ello, se simulan sistemas y "se crean señuelos para engañar a los cibercriminales".

La jornada ha terminado con un turno de preguntas del público que han sido contestadas por los cuatro expertos y que han permitido resolver dudas y dar respuesta a necesidades concretas que tienen las empresas del sector de la logística.