La escasez de talento, principal desafío de la ciberseguridad

Los expertos piden colaborar a todos los niveles para luchar contra los ataques

De izq. a dch.: Ricardo García Gómez (Correos Express), Manuel Serrano (Atresmedia), Daniel Zapico Palacio (Globalia), Lourdes Ruiz (Oracle), Rubén Esteller ('elEconomista'), Javier Zubieta (GMV), Alberto Rosa Gámez (CaixaBank) y José Antonio Sánchez (Viesgo). NACHO MARTÍN Y ALBERTO MARTÍN

elEconomista MADRID.

La aplicación de las nuevas tecnologías en el día a día de las empresas y organizaciones públicas se ha traducido en una gran oportunidad para ganar en eficiencia y en eficacia en los procesos de éstas, pero también en una mayor vulnerabilidad al estar muchísimo más expuestos que hace años. Durante el *II Foro Ciberseguridad: La protección de las infraestructuras críticas en España*, organizado por *elEconomista* con el patrocinio de GMV y Oracle, los expertos han apuntado a la necesidad de concienciación de los riesgos que conllevan las nuevas tecnologías y la importancia de hacer una labor pedagógica a todos sus niveles para un buen uso. Sin embargo, el principal problema que señalaron todos los expertos fue la dificultad de captar talento en el sector.

En palabras de Javier Zubieta, director de Marketing y Comunicación de Secure e-Solutions de GMV, "en el mercado de la ciberseguridad estamos viviendo un momento de gloria, hay bastante alegría, se están moviendo en torno a 1.200 millones de euros, con un crecimiento del 7-10 por ciento interanual. Sin embargo, tenemos un serio problema relacionado con la escasez de talento, la demanda de profesionales no se cubre".

Lourdes Ruiz, responsable comercial de Ciberseguridad de Oracle, añadió que "esta situación no es exclusiva de España, está extendida en toda la Unión Europea (UE). Hay que motivar a los más pequeños desde la más tierna infancia para que se inclinen por profesiones tecnológicas y abrir esta nueva economía digital".

Capacidades de reacción

Por su parte, el CIO de Correos Express, Ricardo García Gómez, apuntó a que desde su empresa "trabajamos en la concienciación, el CISO no puede estar solo, los ejércitos con los que cuenta son los programadores y cada una de las capas de la compañía. La ciberseguridad tiene que venir de todos. Las empresas hemos actuado por miedo, ahora tenemos que actuar por convicción".

En esta línea, el director corporativo de Security & Governance de CaixaBank, Alberto Rosa Gámez, explicó que "es muy importante poner el foco en la capacidad de reacción, hay que ser ágiles para aislar el impacto de los ataques. Tenemos que asumir que éstos van a ocurrir, pero has de tener las capacidades bien engrasadas para aislarlos y eliminarlos".

Sobre si las organizaciones están preparadas para los ciberataques, el CISO y director de Seguridad de Viesgo, José Antonio Sánchez, argumentó que "nunca estás totalmente preparado, cada vez tenemos más medios y más tecnologías, pero fuera hay mucha más gente con mucho más tiempo que puede dedicar a preparar esto".

"Es fundamental tener un equipo dentro para controlar estas incidencias y tener una auditoría que nos permita saber quién nos ataca y qué sistemas utiliza. Cuando recibimos un ataque, lo principal es restablecer el servicio, pero el estudio de ese ataque es fundamental, porque nos da patrones para prevenir otros", dijo el CISO de Atresmedia, Manuel Serrano.

De esta forma, para el CISO de Globalia, Daniel Zapico Palacio, lo importante es descubrir estos vectores. "Personalmente no gasto esfuerzos en atribuir quién ha realizado un ataque, incluso hay mucha gente que se publicita después, lo que me importa son los vectores y aprender cómo lo han hecho para prevenir los ataques", explicó.

"El apoyo de la alta dirección en este sentido es clave, al igual que incorporar la ciberseguridad como parte de la estrategia de la compa-

"Hay que animar a los pequeños a que se inclinen por profesiones tecnológicas"

Lourdes Ruiz
Responsable comercial de Ciberseguridad de Oracle

"Si tienes un euro que invertir en seguridad, hazlo en la gestión de vulnerabilidades"

Javier Zubieta
Director de Marketing y Comunicación de Secure e-Solutions de GMV

"Es muy difícil saber quién te ataca, pero es fundamental saber los vectores"

José Antonio Sánchez
CISO y director de Seguridad de Viesgo

"Las soluciones son importantes, pero tienen que ir con gente que sepa aprovecharlas"

Daniel Zapico Palacio
Chief Information Security Officer (CISO) de Grupo Globalia

"Es clave incorporar la ciberseguridad a la estrategia de la compañía"

Manuel Serrano
Chief Information Security Officer (CISO) del Grupo Atresmedia

ñía. Hay que verlo como una inversión, no como un gasto", añadió Serrano.

Consejos a seguir

La mesa de debate concluyó con diferentes consejos de los expertos en esta materia. Por ejemplo, el CISO y director de Seguridad de Viesgo recomendó a las organizaciones "probar las medidas que tenéis aplicadas, ver si funcionan y cumplen la labor que buscáis. A nivel personal, algo que parece obvio, no se os ocurra mandar las claves de usuario a nadie".

El directivo de GMV apuntó a que "si tienes un euro para invertir en seguridad, hazlo en gestión de vulnerabilidades. A título particular lo que recomendaría es que no hagas en el mundo cibernético lo que no haces en el mundo real".

Por su parte, la responsable de Oracle concluyó explicando que "la seguridad y los responsables de la seguridad de la información debemos ser facilitadores para el negocio, así como cubrir las demandas que nos están haciendo, muy centradas en servicios *cloud*".

"Hay que ser ágiles para aislar el impacto de los ataques en las empresas"

Alberto Rosa Gámez
Director corporativo de Security & Governance de CaixaBank

"La concienciación es clave, todos los empleados deben saber los riesgos que existen"

Ricardo García Gómez
Chief Information Officer (CIO) de Correos Express

Fernando J. Sánchez Gómez Director del CNPIC

"Cuando se creó Internet, no se tuvo en cuenta la seguridad"

elEconomista MADRID.

En la apertura de esta jornada, celebrada en el Hotel Silken Puerta de América de Madrid, el director del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), Fernando J. Sánchez Gómez, explicó que lo que une los conceptos de ciberseguridad e infraestructuras críticas es la dependencia. "Dependemos de una serie de servicios fundamentales que damos por sentados, como la electricidad, el agua, los transportes, etc., que son esenciales en el día a día", explicó el responsable del CNPIC.

"Estudios realizados en el tiempo y a gran escala demuestran que una interrupción, por ejemplo, del servicio eléctrico provocaría un efecto cascada, que en tan solo 24 horas se verían afectados gravemente los sistemas de transporte, distribución, agua y telecomunicaciones. En 36 horas, el sistema sanitario, energético e industrial. A partir de las 48 horas, el sistema alimentario, financiero y el resto de servicios esenciales. A partir de 72 horas, se producirían pérdidas de servicio irrecuperables, afectando de forma muy negativa en la seguridad pública y en las propias capacidades de gobierno", argumentó Sánchez Gómez.

En este sentido, destacó cómo estos servicios esenciales para los ciudadanos están muy relacionados con las tecnologías de la información. "El ciberespacio ha pasado a ser un sinónimo de Internet,

tiene un uso universal, su espacio va más allá de lo puramente tecnológico: tiene implicaciones sociales, culturales y organizativas. Internet cuando se concibió era un espacio para comunicarse y compartir información de manera inmediata, pero no tuvo en cuenta la seguridad", continuó el responsable del CNPIC.

Sánchez destacó así varios datos relevantes en esta materia, como que en 2018 se produjeron 111.000 ciberdelitos, casi el doble que en 2016, cuando se contabilizaron 66.000, según datos del Ministerio del Interior. "Un informe del Foro Económico Mundial señaló los ciberataques como la quinta amenaza mundial más probable, la sexta más negativa y la séptima más peligrosa para la Humanidad, después de las armas de destrucción masiva, cambio climático, desastres naturales, etc. El impacto de los ciberataques a nivel mundial tendrá un coste de 8.000 millones de dólares en los próximos cinco años", destacó el responsable del CNPIC.

Por otro lado, Sánchez también hizo especial hincapié en la importancia de diferenciar entre tecnologías de la información (TI) y tecnologías de la operación (OT). "Cuando se habla de ciberseguridad lo identificamos con sistemas de TI pero, ¿qué pasa con OT? La principal diferencia entre unos y otros es la interacción humana, mientras que en los primeros es fundamental, en los otros no es necesaria. Desde las empresas, debemos ser conscientes de la importancia de los activos informáticos, pero también que el vector más utilizado en los ciberataques es el ser humano", apuntó.

"La ciberseguridad no es solo tecnología, ni hay que abordarla solo desde ésta porque afecta a todos los procesos de seguridad y de negocio de una empresa. Hay que entender la ciberseguridad desde una perspectiva holística y como parte de la seguridad en mayúsculas", añadió el responsable de este organismo público.

Pedro Colmenares Soto Subdirector general de la Inspección de Datos de la AEPD

"Comunicar las brechas al sistema nos ayuda a aprender de nuestros fallos"

eE MADRID.

El *II Foro de Ciberseguridad* de *elEconomista* fue clausurado por Pedro Colmenares Soto, subdirector general de la Inspección de Datos de la Agencia Española de Protección de Datos (AEPD), que destacó también la importancia de concienciar sobre la seguridad a todos los niveles, especialmente en el ámbito de la privacidad, tanto por parte de los organismos públicos como de las empresas.

Sobre la nueva normativa sobre protección de datos, Colmenares apuntó que "desde que se aplicó el reglamento, nos han podido comunicar unas 1.000 brechas y

creo que no llega al 1 por ciento las que han pasado a ser investigadas. De la mera comunicación y de la guía que tenemos publicada, ya hacemos un primer juicio. El reglamento establece un principio de responsabilidad activa, lo que nos interesa es saber si eso lo tenía previsto. Las organizaciones deben tener en cuenta desde el primer momento los derechos de privacidad. Lo que nos importa es la autocrítica. No me preocupa tanto el ataque, sino cómo lo hacen, es una forma de aprender y tomar medidas a futuro".

"Me gustaría quitar un poco de hierro y de miedo a la hora de comunicar. Hay que hacer un ejercicio de responsabilidad a la hora de comunicar las brechas de seguridad para aprender de los propios fallos", concluyó.