**Texto** Laura del Río
**Fotografía** Jorge Pariente
**Vídeo** Jorge Pariente

PROTECCIÓN = CONCIENCIACIÓN + RESILIENCIA

# La mayor brecha de seguridad: el usuario

<< A la hora de señalar el mayor punto débil en un plan de seguridad, muchos se señalan a sí mismos, es decir, a las personas que día a día utilizamos la tecnología y que, en ocasiones y de manera inconsciente, no lo hacemos de la mejor manera.

La ciberseguridad dejó de ser una commodity hace tiempo para pasar a ser un elemento de valor añadido fundamental para que un negocio no solo crezca, sino que no se hunda. Los ataques cibernéticos ya no son algo tan lejano a nosotros como el argumento de películas de ciberespionaje y guerras cibernéticas entre gobiernos y grupos de poder. Ahora el objetivo somos cualquiera y estamos en la diana de delincuentes cada vez más profesionalizados en su tarea: la de tener acceso a todos nuestros datos. El Tour de la Ciberseguridad ha hecho su segunda parada en una de las regiones más prósperas en negocios e industria de España, el País Vasco, más concretamente en Bilbao. ¿Qué consideran importante las empresas vascas en una estrategia de seguridad y por qué?

Existe un tipo de ciberdelincuente por cada tipo de negocio, "igual que existen carteristas y atracadores", los criminales en la Red están cada vez más especializados. Por ejemplo, la última tendencia es utilizar el cryptojacking para la minería de datos, ya sea en teléfonos móviles, ordenadores. La ciberdelincuencia se ha convertido en un negocio en sí mismo, solo el ransomware estaba valorado el pasado año en un billón de dólares. Incluso se han creado "una clase de mercados donde venden datos robados y credenciales, para entrar hasta la cocina de las empresas, a los interesados o a otros ciberdelincuentes".

La estrategia de seguridad tiene que ir desde la nube o data center hasta el dispositivo y su interfaz de acceso. "Ya no vale con proteger solo nuestra propia casa", con la movilidad y la

computación en el edge, "el recorrido del dato ha extendido su perímetro" y la protección debe abarcar el viaje completo. No obstante, una óptima estrategia de seguridad tiene que incluir al usuario, que continúa siendo "el punto débil en esta historia". No en vano, uno de los principales problemas de seguridad que se han acusado últimamente es el robo de credenciales, "nos registramos en tantos sitios y sin el mínimo cuidado que luego vienen los disgustos". Los ataques de día cero son también de los más detectados, -hasta 7.000 al día a nivel global confesó sufrir una empresa-, pero no dejan de surgir nuevas amenazas y crecen exponencialmente.

### Educar en ciberseguridad

A pesar de que las amenazas cada vez son más elaboradas y van más dirigidas, en el encuentro lamentaron que "las personas solo aprendemos a base de palos. Cuando atacó WannaCry todos nos blindamos frente al ransomware, pero con el paso del tiempo se nos va olvidando y nos vamos relajando; hasta que suceda otra vez algo parecido o peor", dijeron. La alerta debe ser continua, "a veces se detectan comportamientos anómalos a los que no damos mayor importancia porque no se presentan bajo la apariencia de amenaza, o lo que nosotros tenemos concebido como amenaza; sin embargo, las amenazas se disfrazan cada vez más de formas distintas".

Muchas veces, los empleados no son conscientes de realizar malas prácticas que ponen en peligro los sistemas de la empresa, "si se les preguntara si hacen algo incorrecto, probablemente la mayoría respondería que no", contaron, pero algo tan simple como esperar a descargar cualquier programa o contenido de interés personal en la oficina en vez de en casa, con la excusa de que "allí hay mayor seguridad", ya supone un riesgo.

La concienciación no solo se debe contar en las empresas, la educación en el plano tecnológico debe darse de forma transversal en el sistema educativo, "desde el colegio". En este sentido, sería beneficioso fomentar los acuerdos entre empresas TIC y de ciberseguridad con los centros educativos para desarrollar proyectos de formación, "tanto para el alumno que quiere emprender una carrera técnica como para el que no, ya que la tecnología la utilizamos todos desde cualquier rama". Esta no es una cuestión baladí, de hecho, muchos ataques, -"entre ellos el famoso WannaCry"-;

**FRAN MORALES,** ÁREA GRANDES CLIENTES DE TELEFÓNICA

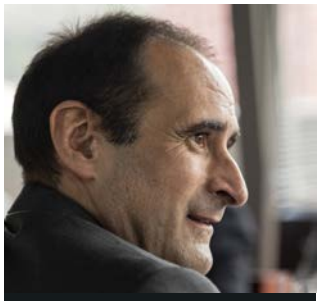
## "PARA SECURIZAR DEBEMOS HACER UN SEGUIMIENTO DEL DATO"

Para definir una estrategia de seguridad se debe analizar, no solo la infraestructura tradicional, sino dónde está el dato y hacia dónde va. Este seguimiento del dato es fundamental en un momento en el que el recorrido del mismo pasa por distintos dispositivos, (smartphones, ordenadores, tablets, …); y puede estar alojado en diferentes plataformas, tanto en la nube como on premise. Para ello se necesita una solución de ciberseguridad transversal.

Networking durante el cóctel del encuentro del Tour de Ciberseguridad en Bilbao.

**JOAQUIN GÓMEZ,** REGIONAL SALES MANAGER PARA IBERIA DE ZSCALER

**MELCHOR SANZ,** DIRECTOR DE TECNOLOGÍA DE HP



**MARÍO GARCÍA,** COUNTRY MANAGER DE CHECK POINT

**LUIS BERNAL,** ESPECIALISTA EN NSX DE VMWARE


se hubieran evitado con un buen uso de la tecnología, "sin necesidad de poseer una pieza ultramoderna".

### Partnership empresa-proveedor

No se trata de adquirir mucha tecnología o la más puntera, sino de adquirir la adecuada según nuestras necesidades. Los proveedores de seguridad afirmaron preferir "que nos compren menos pero que nos compren lo correcto", porque esta es la manera en la que "de verdad se ayuda al cliente, y su satisfacción hace que vuelvan a acudir a nosotros la próxima vez".

> **"Los proveedores de seguridad preferimos que nos compren menos, pero que nos compren lo correcto"**

Por este motivo, es importante realizar tests y pruebas que permitan saber dónde se encuentran las partes más vulnerables de los sistemas y dejarse asesorar por los proveedores, "para no realizar gastos innecesarios", ya que "ahora no se adquiere solo hardware o software, se adquieren servicios". Las compañías también demandan que los proveedores les faciliten la actualización, el cambio de equipos cuando estos se quedan obsoletos, "situación que se da cada vez con mayor frecuencia" por lo rápido de la evolución TI, y en la que las organizaciones se encuentran "un poco desamparadas".

Por mucho que el Esquema Nacional de Seguridad o GDPR dicten unos mínimos, son las empresas las que definen su propio plan de contingencia acorde al potencial peligro que corren. Los recursos no son infinitos, por eso, cuando escasean se tiende a aplicar una seguridad más laxa, "sin tener en cuenta que a veces se gasta más poniendo parches en equipos que comprando equipos seguros desde su diseño". Esta es la forma en la que "proteger tu empresa se convierte en una inversión, y no en un gasto". Nunca se está 100% a salvo, pero estarlo en un 99% depende de las soluciones de seguridad y, sobre todo, de cómo las gestione la empresa.

Pero elevar los niveles de seguridad no solo afecta a la organización, sino a todos los partners y proveedores que trabajan con ella, incluidos los de seguridad. Ser exigente con la seguridad puede pasar "por restringir o acotar el acceso a los sistemas a toda persona externa a la empresa, incluso interna, únicamente dando la dirección IP a los estrictamente necesarios", propusieron; "porque la mejor estrategia de seguridad es estar oculto". No obstante, algunas voces se alzaron contra esta propuesta alegando que, en épocas de gestión transversal y rotura de silos, no puedes poner


**1** Iñigo Carrión, IMQ Prevención | **2** Juan Luis García, IMQ Prevención | **3** Imanol Sauto, Lantik S.A.M.P. | **4** Joseba Maruri, Laboral Kutxa | **5** Izaskun Onandia, ITP Aero | **6** Juan Carlos Ávila, Consulmar | **7** Enrique Pascual, Ayuntamiento de Basauri | **8** Asier Martínez, Basque Cibersecurity Centre | **9** Manu Viota, Ertzaintza | **10** Alberto Rodríguez, Hospital San Juan de Dios | **11** Alberto Palacios, Bolsa de Bilbao | **12** José Antonio Gutiérrez, Hospital de Galdako | **13** Raúl Lozano, Minersa | **14** Aitor Ibarra, Universidad de Deusto | **15** Antonio Vasco, Grupo Acha Movilidad | **16** Guillermo Unamuno, Grupo SPRI Taldea | **17** Carlos Ortiz, Athletic Club de Bilbao | **18** Jorge Eskoin, Euskotren | **19** Jesús Lizarraga, Mondragón Universitatea | **20** Luis Pablo Elvira, Museo Guggenheim | **21** Iñaki Varela, Norbolsa Sociedad de Valores | **22** Aitor Arrondo, Orkli | **23** Igor Lacalle, Ulma Construction

barreras, "sería negativo en términos organizativos y de eficiencia".

La estrategia de seguridad debe ser integral. En el caso de la Industria 4.0, por ejemplo, "se pone el foco en proteger los canales de producción y difusión olvidando otros dispositivos de gran relevancia como el teléfono móvil". Además, los planes de resiliencia y de gestión de crisis, aunque pocas veces son nombrados, son una parte fundamental en toda estrategia de seguridad, ya que es imposible garantizar la impenetrabilidad antes los ataques. Si no consideramos los métodos de reacción estamos planteando una "seguridad falsa", ya que, se filtren ataques o no, "lo que realmente importa es la continuidad del negocio". Dentro de estos planes de resiliencia se contemplan los ciberseguros, cada vez más contratados por las organizaciones. Siempre asociamos las grandes pérdidas a los bienes materiales, pero hoy por hoy, lo más valioso que puede perder una compañía son sus datos. ■