Vídeo Jorge Pariente
Fotografía Jorge Pariente
Texto Laura del Río

LA DIRECCIÓN HA SUPERADO A OTROS ESCALONES EN CONCIENCIACIÓN

El mayor peligro reside en no conocer tu propia empresa

En una época en la que hasta los famosos robots aspiradora se pueden hackear para conseguir los planos de las casas y facilitar los robos a viviendas, entre otras cosas, nadie está seguro. Sin embargo, no podemos -y no queremos- renunciar a que la digitalización nos haga la vida más fácil. Por este motivo, la ciberseguridad está alcanzando altísimas cotas de importancia en el ámbito personal y profesional de las personas, pero que por diversos motivos económicos o de preparación, no son iguales en unos territorios que en otros. Sevilla, la capital de la segunda comunidad autónoma más grande de España y la más habitada, Andalucía, ha sido otra de las paradas efectuadas por el Tour de Ciberseguridad de Computing en la que se ha hecho un análisis sobre las luces y las sombras de los sectores público y privado del territorio sur.

La administración pública tiene un doble reto, por un lado, el de ser cada vez más digital para aquellos ciudadanos que demandan una relación telemática; por el otro, el de mantener los servicios para los ciudadanos que no son duchos en las nuevas tecnologías; y ambos canales tienen que ser 100% seguros. No obstante, en ocasiones un mismo ciudadano se relaciona con la AAPP por ambos canales y se corre el riesgo de que se creen documentos híbridos o copias, "hecho que hay que vigilar para tener un único documento auténtico". En la Junta de Andalucía, concretamente, están securizando a nivel de aplicativo, "antes de subir cualquier software a producción tiene que pasar unas auditorías mucho más severas que antes". A su vez, la mejor forma que ha encontrado la Junta para concienciar a sus trabajadores es a través de una plataforma de teleformación Moodle en la que suben píldoras informativas, "que, aunque en un principio a penas se leían, cada vez tienen mayor acogida".

Otro órgano público, el Consejo de Transparencia y Protección de Datos de Andalucía, lleva

la seguridad en su propio ADN por la propia función que realiza. "Tenemos que ser modélicos en el cumplimiento de la normativa por nuestro carácter garantista con el ciudadano", dijeron. Debido al pequeño tamaño de la institución, tienen externalizado el servicio informático con Sandetel, empresa que, al igual que todos sus proveedores, tiene que pasar unos exhaustivos controles de seguridad que en el Consejo han sido capaces de diseñar gracias al asesoramiento de una compañía de hacking ético. Pero el propio consejo también ha analizado su nivel de desprotección: "En la última auditoría que hicimos no salimos muy bien parados", lamentaron. "De una escala que va de L0 a L5, establecieron una calificación de L1", insuficiente para los tiempos que corren. Como resultado, han elaborado un plan de acción que les permita alcanzar un nivel L3 en este año, "tanto en la protección de los documentos en papel como digitales". En el Consejo, detectan más errores de protocolo y documentación que fallos técnicos, lo que lleva directamente a los empleados y a sus métodos. Uno de los problemas más graves a solventar es la suplantación de identidad, "nos han hackeado el portal web en varias ocasiones y han mandado correos a personas como si fuéramos nosotros", explicaron, "un tipo de incidencia que, además, es bastante difícil de detectar". Otra de las cuestiones en la que están haciendo hincapié recientemente es en la búsqueda de un sistema automático de anonimización de partes de texto y vídeo.

RAFAEL EXPÓSITO, GRANDES EMPRESAS TERRITORIO SUR DE TELEFÓNICA

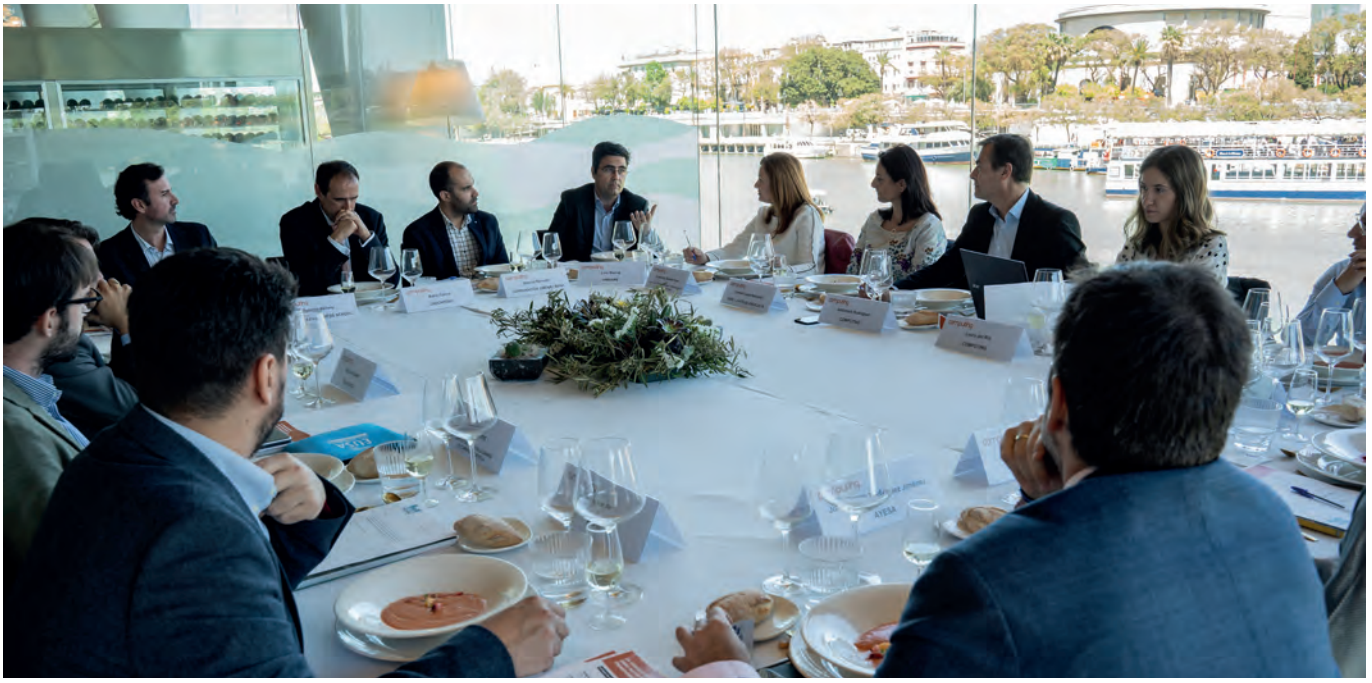
"LA SEGURIDAD SE BASA EN PREVENCIÓN, DETECCIÓN, MITIGACIÓN Y RECUPERACIÓN"

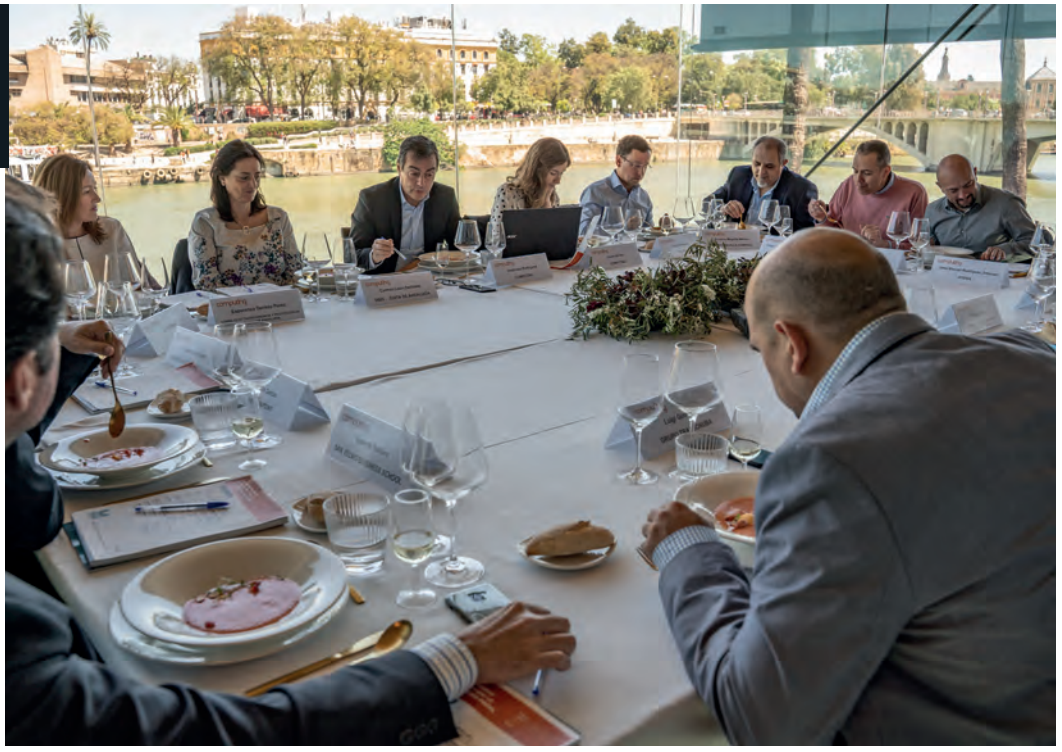
Las mejores medidas de seguridad giran en torno a cuatro puntos: la prevención, la detección, la mitigación, y como no, la recuperación una vez que se es víctima de un ataque. Para establecer las medidas oportunas en cada momento, es vital contar con las soluciones tecnológicas y con el soporte experto que permita identificar los patrones de comportamiento anómalo dentro de la red.

El ejemplo más representativo de las brechas que tardan en detectarse es el de Citrix, compañía de la que se extrajeron seis terabytes de información sensible durante los 10 años que pasaron desde que el grupo de cibercriminales Iridium consiguiera acceder a la red interna de la compañía. Fue el pasado mes de marzo cuando se descubrió el pastel. En este sentido, Zscaler recomienda invisibilizar la red interna controlando los accesos mediante lo que llaman "perímetro definido por software".

La falsificación de facturas también está a la orden del día. Sobre todo, en el caso de las pymes, que cuentan con menos recursos y equipo humano, muchas veces no revisan todos los pagos con la precisión que lo podría hacer una gran compañía y ha habido casos

"Dirección y empleados esperan que los de TI les garanticen que van a estar protegidos hagan lo que hagan"





Encuentro en el restaurante Abades de Sevilla, en el Tour de Ciberseguridad organizado por Computing.

1 Diego Camacho, Admiral | **2** José Manuel Rodríguez, Ayesa | **3** Francisco Leal, Cámara de Comercio de Sevilla | **4** Víctor Pérez, Campus Formativo de la Cámara de Comercio de Sevilla | **5** Esperanza Dorado, Consejo de Transparencia y Protección de Datos de Andalucía | **6** Alberto Bernabé, Corporación Jiménez Maña | **7** Carmen León, Junta de Andalucía | **8** Antonio Megolla, Grupo Sevilla Control | **9** Luigi Gutiérrez, Grupo Transonuba | **10** Diego Rodríguez, Migasa | **11** Roberto Bellany, San Telmo Business School

citados por los asistentes, en los que empresas han ingresado el pago en la cuenta bancaria de un proveedor falso, y cuando han querido recuperar su dinero, esta cuenta ya ni existía.

La conciencia de riesgo entra en la empresa

La dirección, "siempre un hueso duro de roer a la hora de invertir en tecnología, y más en ciberseguridad", ahora parece estar incluso más concienciada que otros escalones de la empresa. Iniciativas como cursos de formación han dado mejores resultados en las compañías de lo que se pensaba en un primer momento, "hay usuarios que siempre ven una pérdida de tiempo el hecho de reunirse con los informáticos, y tanto los jefes como los empleados aún esperan que los de TI les garanticen que van a estar protegidos hagan lo que hagan; sin darse cuenta de que la protección depende en gran medida de ellos mismos". A pesar de aprovisionarte con las más confiables herramientas de seguridad, de nada sirve si los usuarios no las utilizan o no lo hacen correctamente, "por eso es tan importante la colaboración de todas las áreas de la empresa". En este sentido, sería conveniente que las organizaciones midieran su nivel de buenas prácticas como lo hacen en algunas administraciones.

El golpe de realidad que se han dado muchas compañías que han sido atacadas, las ha llevado a abandonar su reticencia a ralentizar

o parar puntualmente el negocio para implantar herramientas de seguridad, en caso de que sea necesario. Sobre todo, las compañías que trabajan con clientes y proveedores de otros países, los cuales pueden tener una regulación más laxa o una menor conciencia en ciberseguridad, convirtiéndose así en un puente perfecto hacia la empresa para los ciberdelincuentes; de este modo, pueden hacer de la organización "otra manzana podrida capaz de infectar a las demás".

Otro medio que algunas empresas han encontrado eficiente a la hora de incentivar a la plantilla a seguir las medidas de seguridad consiste en lanzar pequeñas trampas para ver si los empleados caen en ellas, y premiar con bonus a aquellos que no cometan infracciones y consigan sortear el ardid. Perder el miedo a sacar a la luz los puntos débiles de nuestros equipos puede evitar desastres y daños reputacionales a futuro.

Un escenario con muchos actores

Siempre se habla del negocio a nivel de oficina, de la cadena de distribución y los proveedores, pero… ¿y la producción? La capa OT es igual de vulnerable que la de IT y, además, converge con ella. El nuevo modelo de Industria 4.0, capitaneado por el Internet de las Cosas, la robótica y los sensores, se ha transformado en un blanco al que los ciberdelincuentes pueden atacar cada vez por más flancos y que, sin embargo, parece que pasara de refilón por el tema de la ciberseguridad. Quizá por la complejidad que ha adquirido el panorama, cada vez más descentralizado, una brecha en un equipo de producción puede ser fatal para una organización que tenga en ella su core de negocio.

La movilidad es otro añadido al laberinto de la ciberseguridad en las conexiones. El teletrabajo está en auge, sin embargo, los empleados parecen preocuparse de la seguridad únicamente cuando trabajan desde sus propios dispositivos, por lo que las empresas optan por tenerlos lo más capados posible. Bloquear inmediatamente las cuentas y accesos de los empleados despedidos o que abandonan la empresa es otra medida urgente que las compañías no siempre se toman muy en serio. "Un trabajador descontento es lo peor que puede haber", dijeron, "y si es administrador de sistemas puede dejar muchas puertas abiertas, por lo que hay que estar vigilante".

Gobernance, normativas, seguridad de dominios, reglas de firewall, análisis, concienciación, resiliencia,... muchos pilares sustentan tanto la seguridad lógica como la física. Si uno de estos pilares se rompe y no se repara eficazmente puede acabar por caer toda la torre fortificada. Por eso, conocer y reconocer las debilidades propias e invertir en fortalecerlas es fundamental. Los problemas se presentan cuando "el plan de fortaleza es a tres años y solo se dispone de presupuesto para uno". ■

JOAQUIN GÓMEZ, REGIONAL SALES MANAGER PARA IBERIA DE ZSCALER

MELCHOR SANZ, DIRECTOR DE TECNOLOGÍA DE HP

MARIO GARCÍA, COUNTRY MANAGER DE CHECK POINT

LUIS BERNAL, ESPECIALISTA EN NSX DE VMWARE