Vídeo Jorge Pariente
Fotografía Jorge Pariente
Texto Laura del Río

ENTERARNOS DE QUE HEMOS SIDO ATACADOS TAMBIÉN ES UN RETO

La seguridad predictiva se convierte en ciberinteligencia

El Tour de Ciberseguridad de Computing sigue recorriendo las ciudades españolas. Si en pasados encuentros, proveedores, empresas e instituciones públicas y privadas se dieron cita en las ciudades de Barcelona y Bilbao, esta vez le toca el turno a Valencia. El restaurante Ricard Camarena LAB, ganador de dos Estrellas Michelín, fue el lugar encargado para recibir a los expertos en ciberseguridad en la tierra de la luz, el mar, la paella…. ¿y también de los negocios digitales seguros? ¿Están en las organizaciones de la Comunidad Valenciana preparados para competir en un mundo TIC lleno de peligros?

Los usuarios que tratan con la tecnología son muy heterogéneos, tienen habilidades y desempeñan funciones muy distintas, y esto les hace convertirse en "un punto débil" de la empresa en lo referente a ciberseguridad. La concienciación en este sentido "es vital", ya que muchos empleados piensan que con "respetar las normas de seguridad una vez o de vez en cuando, están inmunizados para siempre, que la suerte va a estar de su lado, el típico: no me va a tocar a mí"; pero, lamentablemente, nadie está fuera de peligro y "no aprendemos hasta que nos toca a nosotros". Sin embargo, a pesar de que todos estuvieron de acuerdo en la importancia de la formación del usuario, algunos señalaron que muchas veces no es una cuestión de conocimiento, sino de responsabilidad. Y pusieron un ejemplo: "A la hora de hacer una transferencia bancaria online, a los usuarios no les duelen prendas en hacer los cinco o más pasos que puede tener la operación, porque es su dinero el que está en juego; pero cuando se trata de una operación de la empresa les entra la pereza, porque no toman los recursos de la compañía como propios". Por este motivo, es fundamental tener una tecnología adecuada para respaldar al usuario en aquellos puntos

donde este no llega, ya sea por una cuestión de educación o porque el usuario tampoco es omnipotente. "Ni el usuario más preparado del mundo ni la tecnología más puntera garantizan al 100% no ser víctima de un ciberataque".

Adquirir e implementar tecnología desde un punto de vista de ayuda al usuario, esa es la clave. Las empresas no tienen que ver en la ciberseguridad un elemento que obstaculiza el negocio, sino que lo protege; y no un factor que interrumpe sus actividades diarias, sino que las securiza para que estas se puedan seguir llevando a cabo. "Pasarse escalando en seguridad puede hacer a las empresas incurrir en costes innecesarios y aumentar la complejidad; sin embargo, quedarse corto puede poner en riesgo nuestra actividad, hay que encontrar un equilibrio". No obstante, en el encuentro afirmaron que "no deberíamos hablar de ciberseguridad, sino de ciberinteligencia. La ciberseguridad es reactiva y la ciberinteligencia es predictiva, y la lucha está en ver quién va por delante, si los ciberdelincuentes o los usuarios; quien se anticipa tiene ventaja". En este sentido, "es la transformación digital la que tiene que servir de motor de la ciberseguridad, y no al revés".

Para conseguir este objetivo, es necesario hacer una labor de consultoría antes de comprar cualquier tipo de tecnología, para identificar, según la naturaleza de la organización, las posibles brechas de seguridad de los sistemas, los puntos flacos de los equipos, tanto humanos como técnicos; y las partes más sensibles del negocio. Para establecer las herramientas y las medidas adecuadas también hay que tener en cuenta las fases de prevención, detección, reacción y recuperación después de un ataque, que componen una estrategia de seguridad.

Detectar un ataque parece el paso más obvio, pero no todas las amenazas encienden las alarmas, "el tiempo medio que tarda una empresa en enterarse de que ha sido atacada es de 75 días", apuntaron en el debate. Un periodo del todo excesivo si consideramos que no reaccionar durante 75 días a un ataque es como tener una ventana abierta al corazón de la empresa para los ciberdelincuentes durante más de un mes: datos, operaciones, proyectos y objetivos quedan al descubierto para ser utilizados en beneficio de los ladrones. También cabe mencionar las ocasiones en las que los trabajadores extravían dispositivos de la organización y tardan días en notificarlo porque guardan la esperanza de recuperarlos perdiendo un tiempo precioso para bloquear estos aparatos.

JOAQUÍN GÓMEZ, REGIONAL SALES MANAGER DE ZSCALER

"SECURIZAR SOLO LA RED PROPIA CARECE DE SENTIDO"

Hoy en día, la movilidad y el IoT han potenciado la expansión del perímetro de conexión y han propiciado que la gran mayoría de las empresas suban su data center y aplicaciones a la nube. Por este motivo, securizar solo la red propia carece de sentido, hay que desarrollar una estrategia por la que las políticas de seguridad del negocio sigan al usuario allá donde esté y utilizar Internet para conectar a los usuarios con las aplicaciones alojadas en la cloud, controlando los accesos.

ALEXANDRE TOVAR, EXPERTO EN SEGURIDAD DE IPM

"EL ALCANCE Y LA RENTABILIDAD SON LAS GRANDES CLAVES"

Existen dos criterios básicos para determinar cuándo y en qué solución de ciberseguridad debemos invertir. Uno es el radio de alcance, o el potencial que el servicio o producto tiene para extender sus capacidades dentro de la organización; y el otro es el coste para el atacante, es decir, que al ciberdelincuente le sea menos rentable atacar a la compañía que a esta implementar la solución en cuestión. Estos dos criterios se resumen en alcance y rentabilidad.

MELCHOR SANZ, DIRECTOR DE TECNOLOGÍA DE HP

"FACILITAR LA TAREA AL ADMINISTRADOR DE SISTEMAS"

HP lleva invirtiendo muchos años en aspectos de seguridad del hardware. El primer paso ha sido fortalecer la BIOS para que detecte y notifique amenazas en tiempo real y los dispositivos se recuperen fácilmente en caso de ser atacados. La compañía también ha incorporado a sus ordenadores e impresoras filtros de privacidad, identificación y anonimización. Además, ha diseñado aplicaciones para gestionar todas estas herramientas y facilitar la tarea del administrador.

Una vez somos conscientes del ataque, se debe poner en marcha el plan de reacción, para tapar las brechas, y de resiliencia, para asegurarnos de que los sistemas vuelven al estado inicial, el de antes del ataque, y no han sufrido ningún daño. Sucede que, muchas veces, las empresas se focalizan en la prevención, para no

MARIO GARCÍA, COUNTRY MANAGER DE CHECK POINT

"EXTENDEMOS LA PROTECCIÓN A TERCEROS"

La solución de seguridad de Check Point toca todos los ámbitos de una posible incursión de amenazas en la empresa, desde el dispositivo hasta la nube pasando por la red, el perímetro del data center y el control de acceso a las aplicaciones; ya sea en un puesto de trabajo fijo o móvil. Yendo un paso más allá, el proveedor de seguridad ha extendido su protección a terceros, siendo capaz de detectar cuándo a los clientes de sus clientes les están robando información.

FRANCISCO VERDUGO, NETWORK & SECURITY EN VMWARE

"LA SEGURIDAD SE ABORDA DESDE LA RED Y LAS APPS"

La apuesta de VMware se basa en la capacidad de su plataforma de virtualización para entender el funcionamiento de las aplicaciones y abrir la puerta a elementos de remediación. A dia de hoy, la seguridad se aborda desde diferentes puntos de vista: el punto de vista de la red, desde el cual nos servimos de la microsegmentacion que nos proporciona la solución NSX, pero también desde el punto de vista de las aplicaciones en la nube, en el que contamos con la herramienta App Defense.

ser atacados, dejando un poco de lado las tácticas de recuperación, que se aplican una vez lo han sido; un paso que es tanto o más importante que los demás, ya que, cuando el ataque afecta a la continuidad del negocio, la pregunta más común es: "¿cuándo voy a poder volver a operar con normalidad?". Por esta razón las compañías hacen tanto backups y copias de seguridad.

Descentralizar la seguridad

El perímetro del data center es el ámbito donde las compañías han puesto el foco de la seguridad, algo del todo positivo si no fuera porque se han olvidado de securizar los distintos elementos que van más allá de su red en la época del Internet de las Cosas y la conectividad 5G. La vida personal y profesional de las personas gira cada vez más en torno al smartphone, y se pueden contar con los dedos de una mano las organizaciones que han diseñado de verdad una estrategia de movilidad segura. "Ya sea por falta de recursos o de conocimientos, las compañías van a remolque de los acontecimientos, y si las grandes organizaciones se topan con estos límites, imaginemos las pymes, que forman la mayor parte del tejido empresarial español", lamentaron en el encuentro.

Desde la dirección, pasando por los empleados hasta los canales de producción y distribución, toda la empresa debe estar involucrada de forma proactiva en la seguridad.

Afortunadamente, "los directivos han dejado de creerse que están por encima del bien y del mal, y no solo impulsan medidas de seguridad, sino que ellos también las aplican". En el caso de la administración pública, la concienciación de los altos mandos es más difícil, ya que estos son los políticos: alcaldes, concejales, diputados y presidentes del gobierno. Aunque la ciberseguridad y la ciberinteligencia están penetrando cada vez más en los programas de los partidos políticos, algunas instituciones dependientes de la administración están empezando a recibir ahora partidas presupuestarias para la seguridad, que únicamente se ejecutan si no sale del gobierno el partido que las aprobó, "en caso contrario, se echan para atrás y a empezar de nuevo". No obstante, algunos expertos señalaron que "los costes en seguridad no serían tan elevados si en vez parchear los equipos, incluyéramos la seguridad desde el diseño y contando con las capacidades y necesidades del usuario final".

La normativa de Seguridad ha endurecido los criterios a la hora de adquirir tecnología a los proveedores, obligando a estos a estar certificados si quieren trabajar con la AAPP; ha hecho que las entidades tengan que calificar su negocio según su nivel de criticidad para implementar una mayor o menor protección, y la ley europea de GDPR impone elevadas multas a las compañías que no respeten sus criterios. Aunque a rebufo, parece que en España las organizaciones "es están poniendo las pilas", aunque la palabra 'cumplimiento' se puede dividir curiosamente en dos palabras, en 'cumplo', pero también en 'miento'. ■

"Los costes en seguridad no serían tan altos si en vez de parchear los equipos, incluyéramos la seguridad desde el diseño y contando con el usuario final"

1 José Fernández, Autoridad Portuaria de Valencia | **2** Víctor Giner, Autoridad Portuaria de Valencia | **3** David Domínguez, Ayuntamiento de Sagunto | **4** Javier Mateo, Ayuntamiento de Valencia | **5** María Luisa Lloret, Ayuntamiento de Valencia | **6** Carlos de Cózar, Cámara de Valencia | **7** Alejandro Corell, Feria de Valencia | **8** Víctor Abraila, GD Energy Services | **9** David Dapena, Ribera Salud | **10** Andrés Pérez, SanLucar Group | **11** Manuel Esteve, Universitat Politécnica de Valencia