Texto Laura del Río
Fotografía Santiago Ojeda
Vídeo Jorge Pariente

COLABORACIÓN Y CONCIENCIACIÓN POTENCIAN LA SEGURIDAD

<< 2017 ha sido un mal año para la seguridad, y no solo por la profusión de ataques masivos como WannaCry o Petya, sino porque, debido a ellos, entre otros factores, las empresas se han puesto frente a un espejo para comprobar que, aunque cuenten con las mejores tecnologías, la inversión en talento para gestionarlas es aún insuficiente.

Los problemas crecen para el CISO

Tras este golpe de realidad, muchas compañías han dado un vuelco a sus políticas de seguridad, pero el tiempo corre en su contra, ya que las amenazas no dan tregua. Para medir el estado de la ciberseguridad profesional en España, Computing ha organizado un executive lunch que ha servido de termómetro para los CISO y encargados de seguridad de empresas de diversa índole, tanto del sector público como privado, en el que han colaborado algunos de los principales fabricantes de seguridad: Check Point, Hewlett Packard Enterprise (HPE), Kaspersky Lab, Sophos y VMware.

Los expertos afirmaron que, asombrosamente, los usuarios continuamos cayendo en los errores de seguridad más básicos, como no cifrar la información o las comunicaciones, establecer configuraciones predeterminadas o dar permisos de acceso a los programas a usuarios no autorizados. Así, urge sensibilizar a los empleados con que "la tecnología que pone la empresa a su disposición es para uso exclusivamente empresarial y no personal, del mismo modo que no deben utilizarse aplicaciones personales para compartir documentos profesionales".

Los representantes del sector público sentados a la mesa admitían que, en su área, no se parchea con la suficiente celeridad. "Solo en el mes de marzo de 2017 hubo entre 30 y 40 organismos públicos con problemas de actualización de los equipos", afirmaron. Este

Centro Criptológico Nacional,
Javier Candau

Ferrovial,
Juan Cobo

Grupo Cortefiel,
David Moreno

Grupo Recoletas,
José Bardallo

hecho se debe a que las entidades programan herramientas de software libre y sin un desarrollo de código seguro "donde prima la disponibilidad por encima de la seguridad". Como consecuencia, el administrador deja de actualizar el sistema, el cual no está preparado para admitir las actualizaciones, por lo tanto, si se producen, deja de funcionar. No obstante, los miembros del sector privado presentes pronto se sumaron a reconocer que sufren la misma problemática.

Menos máquinas y más talento

En la mesa se admitió que ataques como WannaCry que, aunque no fue especialmente peligroso, sí se convirtió en uno de los más mediáticos; se podían haber evitado si se hubiera actuado a tiempo. No obstante,

> **"El mayor error es no integrar la seguridad de forma nativa en la arquitectura y los procesos"**

para reforzar la prevención es necesario invertir en recursos humanos y, sobre todo, en la correcta designación de personas preparadas para cubrir puestos específicos, ya que, en ocasiones, "las organizaciones cuentan con demasiados profesionales de un perfil concreto y escasean de otros". Sin embargo, algunos responsables de seguridad lamentaron que no encuentran ingenieros que cumplan sus requisitos en las universidades y que, muchas veces, contratan empleados en los que valoran "más la actitud que los conocimientos" y a los que preparan ellos mismos en el seno de sus empresas.

A pesar de que algunas voces alegaron que las entidades cuentan con tecnología "suficiente y de calidad" para protegerse, la queja de otras sonaba en torno a la "falta de sistemas maduros y sin fisuras". No obstante, en lo que coincidieron todos los profesionales es en que el principal problema se halla en "no integrar la seguridad de forma nativa en la arquitectura y los procesos desde el principio". Trasladar a la totalidad de la organización la responsabilidad de la seguridad también se considera una parte crucial del cambio. "Los encargados de seguridad de las empresas tendemos a culpabilizarnos cada vez que algo sale mal, -se quejaron,- por lo tanto, el reto consiste en hacer ver que la seguridad forma parte intrínseca del negocio, y por consiguiente, el compromiso es global; desde el último eslabón de la cadena hasta la dirección".

El papel del CISO y los intermediarios

"Los CISO jugamos un papel un tanto extraño y equívoco en las organizaciones", confesaron en el encuentro. Con la trasposición de la Directiva NIS de la Unión Europea y la entrada en vigor definitiva de GDPR, han surgido nuevas figuras como la del Delegado de Seguridad (DPO); muchas veces, actúan como interlocutores entre el departamento de seguridad y la dirección o el resto de la empresa, añadiendo capas intermedias a la función del CISO. "Este tipo de intermediarios hacen de asesores o consultores, pero, a fin de cuentas, la responsabilidad siempre recae en el responsable de seguridad".

Asimismo, en relación a la importancia del encargado de seguridad, en el encuentro reclamaron la presencia de esta figura a la hora de cerrar cualquier tipo de pro-

Intervención General de la AAPP del Estado,
María Jesús Casado

Mediaset,
Ramón Ortiz

Ministerio de Fomento,
Rafael Santos

MARIO GARCÍA, DIRECTOR GENERAL PARA ESPAÑA Y PORTUGAL DE CHECK POINT

"LAS EMPRESAS CUENTAN CON UNA PROTECCIÓN 2,8 PARA DERRIBAR ATAQUES DE NIVEL 4 Ó 5"

En los últimos tiempos se ha producido una revolución en el mundo del cibercrimen generando malware inteligente y predictivo, lo que llamamos ataques de nivel 4. No obstante, el desarrollo de las amenazas no tiene techo, y ya se predice la llegada de la 5ª generación de ataques, globales y multidimensionales. Este tipo de software malicioso no va dirigido a una única herramienta, puedes recibirlo por todas las vías de conexión imaginables o verte afectado de manera colateral por él. Según estadísticas de Check Point, hoy por hoy, las empresas cuentan con una protección de nivel 2,8; por lo que, una vez más, no estamos preparados para lo que nos espera.

Los ciberdelincuentes no están movidos por ningún motivo romántico, su único motor es el dinero, justo lo que les falta a las empresas para invertir en la seguridad que nos pondría a su mismo nivel, o mayor.

FÉLIX MARTÍN, SECURITY STRATEGIST, GLOBAL SECURITY COE, HPE POINTNEXT ADVISORY SERVICES

"CUANTO MÁS DEPENDEMOS DE LA TECNOLOGÍA MÁS EXPUESTOS ESTAMOS A LOS ATAQUES"

Desde hace 15 años hasta nuestros días, la tecnología ha ido evolucionando e inundando todos los aspectos de nuestra vida. Este hecho ha llevado aparejado, inevitablemente, el desarrollo de una nueva modalidad criminal que persigue apoderarse de nuestra vida digital, tanto a nivel personal como profesional. En este sentido, la securización de la tecnología se ha convertido en un quebradero de cabeza para las empresas, ya que, hoy por hoy, no existen procesos corporativos que no sean tecnológicos y, cuanto más dependemos de la tecnología, más expuestos estamos a los ataques.

Ante este cambio de paradigma, las empresas tienen que aprovechar su conocimiento, que es su 'propiedad intelectual', para abordar los procesos de seguridad confiando en una arquitectura referencial en este campo con soluciones end to end, como las de Hewlett Packard Enterprise.

BOSCO ESPINOSA DE LOS MONTEROS, KEY PRESALES MANAGER DE KASPERSKY LAB

"LOS ATAQUES MÁS SENCILLOS Y CONVENCIONALES SIGUEN SURTIENDO EFECTO"

Promover una cultura colaborativa entre los actores del sector de la seguridad es vital para fortalecer la protección frente a los ciberatacantes; no obstante, para crear un entorno de cooperación eficiente se necesita un organismo internacional neutro, que unifique las reglas y vertebre todas las fases y proyectos enmarcados en este contexto. Aun así, diseñar un protocolo de este calibre se antoja complicado cuando, no solo las empresas, sino que los gobiernos de los países desconfían unos de otros a la hora de aportar información.

A pesar de existir amenazas cada vez más sofisticadas, los ataques más sencillos y convencionales siguen surtiendo efecto debido a que el usuario se muestra despreocupado a la hora de dar sus datos por Internet. Además, las trabas legales a realizar una defensa activa frente a ataques a gran escala, ralentizan los tiempos de reacción y recuperación.

RICARDO MATÉ, COUNTRY MANAGER DE SOPHOS

"SE HA MONTADO UNA INGENIERÍA DE LA CIBERDELINCUENCIA EN TORNO AL HACKING AS A SERVICE"

El mundo de la seguridad se está tornando cada vez más complejo. Los hackers acceden a nuestra información por vías cada vez más diversas y se ha montado una ingeniería de la ciberdelincuencia en torno a la comercialización de herramientas para desarrollar software malicioso, lo que se conoce como Hacking as a Service. El periodo que pasa entre que se lanza una nueva herramienta de hackeo y otra es gradualmente más corto y, por tanto, la monetización de los ataques es más rápida. A pesar del progresivo perfeccionamiento de las amenazas, los usuarios demandan una protección completa, pero a la vez, simplificada. Por este motivo, el lema de Sophos es 'Security made simple'; lo hemos materializado en la herramienta Sophos XG Firewall, actualizada con tecnología de Business Intelligence para detectar el malware en milisegundos y gestionar una seguridad sincronizada.

PABLO TEIJEIRA, ENTERPRISE MANAGER DE VMWARE

"LA SEGURIDAD TIENE QUE SER NATIVA DE LA TECNOLOGÍA, NUNCA APLICARSE A POSTERIORI"

A la hora de embarcarse en un proyecto de transformación digital, las compañías implementan herramientas de movilidad, cloud… pero la securización siempre está la última de la lista cuando debería estar integrada desde el principio. Las organizaciones tienen que adquirir la conciencia de que la seguridad debe ser nativa de la tecnología, nunca aplicarse a posteriori. El cibercrimen ha llegado a ser una industria colaborativa, algo de lo que tenemos que aprender los fabricantes de seguridad para, de forma real y efectiva, remar todos en la misma dirección en la lucha contra la ciberdelincuencia. Actualmente, existen cerca de 2.500 proveedores de seguridad en el mundo, y esta cifra continúa subiendo; si avanzamos hacia un modelo de cooperación, también con otras industrias como la de canal, multiplicaremos nuestro poder frente al 'eje del mal' del mundo digital.

yecto con un proveedor. "Desde licitaciones a contratos con fabricantes de IoT, la asistencia de, al menos, un integrante de la división de Seguridad de las corporaciones participantes en el acuerdo debe ser demandada para supervisar el proyecto". Si bien, los CISO reconocen que prácticamente "ninguna empresa lo hace".

El dilema de la colaboración

"La ofensiva tiene libertad de acción, el atacante decide cuándo, cómo y dónde ataca, pero la potencial víctima debe estar siempre preparada". Además, los CISO afirman reconocer en "el obsesivo celo por la privacidad", a veces, "a nuestro peor enemigo". Esto se debe a que las entidades temen compartir cualquier tipo de información sobre un ataque recibido y detectado por miedo a que se filtre algún dato privado de algún usuario y que esto tenga consecuencias en materia de cumplimiento de regulación. Aun así, "la compartición de este tipo de información puede ser muy útil para formar un frente común contra el cibercrimen". De esta manera, los participantes del debate celebrarían la creación de una asociación de seguridad, "como la de Alastria sobre Blockchain", para "contraatacar mediante la unión de nuestras herramientas y conocimiento", ya que por separado "nuestros efectivos se encuentran en una clara minoría numérica".

"La empresa privada y el sector público podemos tener los mismos problemas, pero los

"Los CISO jugamos un papel un tanto extraño y equívoco en las empresas"

Prosegur,
Angélica Zamora

Renfe,
Francisco Lázaro

Rural Servicios Informáticos,
Pedro Pablo López

Seur,
Ricardo Martín

abordamos de distinta forma y vamos a distinto ritmo", destacaron ciertos expertos; sin embargo, apuntaron al efecto positivo que puede tener una "adecuada simbiosis entre ambos". A su vez, algunos de ellos resaltaron que "el conocimiento debe residir en las instituciones públicas, aunque estas se apoyen en la tecnología de las empresas privadas". Pese a que muchos solo ven ventajas en esta centralización de recursos, otros profesionales se muestran más reticentes a ceder determinada información core de sus empresas, por lo que encuentran fundamental "definir los términos de esta compartición". En este punto, algunos profesionales quisieron remarcar que hay que "asumir que cada una de nuestras organizaciones es una pieza del puzle que colabora en la seguridad global" y desterrar la idea de que "somos el centro del ecosistema y, por tanto, esperamos recibir toda la información para la propia seguridad sin aportar nada".

Centrarnos más en la prevención que en las consecuencias de un ciberataque una vez se ha efectuado es vital para estar mejor preparados antes las amenazas. Para ello, no solo debemos mantener un adecuado nivel de protección en nuestro entorno de trabajo, sino también asegurarnos de que nuestros socios lo tienen. "Los modelos de comercialización de la tecnología han cambiado, ahora están muy orientados a servicio". Esta casuística hace que los sistemas de las compañías dependan tanto de terceros, "por lo que debemos contar con la garantía de nuestros partners de que cuentan con unos buenos elementos de control de sus productos".

La lucha contra la ciberdelincuencia no ha hecho más que empezar, y todos, tanto de manera colectiva como individual, estamos implicados en ella. Desde las generaciones nativas digitales, sorprendentemente menos preocupadas por la seguridad; pasando por los medios

"La ofensiva tiene libertad de acción, pero la potencial víctima debe estar siempre preparada"

de comunicación, que en ocasiones generan una alarma social innecesaria y obligan a los departamentos de seguridad de las empresas a pronunciarse ante ciberataques que no han sufrido o sobre los que aún no tienen la suficiente información; hasta las instituciones públicas y privadas y cada uno de los profesionales que aportan a ellas su inteligencia; están llamados a tomar partido. En definitiva, los problemas crecen, pero no podemos permitir que las soluciones mengüen. ■