Vídeo Jorge Pariente
Fotografía Jorge Pariente
Texto Laura del Río

LA CIBERSEGURIDAD ES UNA GUERRA PERMANENTE

El tridente de la seguridad: tecnología, procesos, personas

<< Las organizaciones tardan en darse cuenta de que han sido atacadas, de media, en torno a 101 días; demasiado tarde para ponerle remedio o minimizar los daños.

Poner el foco en la seguridad está empezando a ser algo de primera necesidad para las empresas, en general, y para las personas, en particular, también impulsado por el eco que están comenzando a generar los medios de comunicación. Prueba de ello es la caída que experimentaron los ataques de ransomware en 2018, tras el 'boom' de WannaCry. Para revisar estos y otros muchos temas celebramos el Tour de Ciberseguridad, que tuvo su primera parada en Barcelona con un completo éxito de asistencia. 26 CISO, proveedores y expertos en ciberseguridad se reunieron en la ciudad condal para tratar un tema que nos ocupa a todos.

"Vivimos en un mundo de salvajes digitales", fue la controvertida frase que abrió el debate. Internet es un terreno cuyas posibilidades vamos explorando día a día, y al no haber sido educados digitalmente, no tenemos reglas a las que ajustarnos. "Aprendemos a base de errores, pero a veces, los errores se pagan caros", argumentaron. Al contrario que en el ámbito físico, en el cual nuestro instinto nos avisa de cuándo hay peligro, en el ámbito digital esta intuición natural no existe, "el peligro no se percibe de la misma manera, y aunque a base de práctica estamos aprendiendo, la velocidad a la que vamos en el mundo actual no nos permite pararnos a pensar en muchas ocasiones".

Por este motivo, la formación y la concienciación del usuario no iniciado fue uno de los temas estrella del encuentro. La necesidad de educar a los niños desde la escuela para que desarrollen sus capacidades digitales "es fundamental", aunque "muchas veces son ellos, los nativos digitales, los que nos enseñan a los que no lo somos". No obstante, las cosas cambian cuando se trata de formar y concienciar al empleado. "Transformar la mentalidad y la forma de trabajar de las personas a ciertas alturas es muy difícil, y más por una amenaza que no sienten como real", lamenta-

ron; "por eso, el usuario se convierte en carne de cañón". En este sentido, el apoyo de la dirección y una acción ejemplarizante por su parte se torna esencial, "si el subordinado ve que su propio jefe no cumple los requisitos de seguridad, él se va a relajar el doble".

La tecnología, enemiga o aliada

La anteriormente citada rapidez con la que vivimos hoy en día nos ha convertido en seres impacientes que buscan un acceso fácil e inmediato a páginas, contenidos y, por supuesto, a los datos. De esta manera, el ritmo actual se presenta como uno de los principales enemigos de la ciberseguridad. En el caso de datos de carácter sensible, como el historial clínico de los pacientes, la gestión resulta particularmente complicada. "Nos debatimos entre dar un servicio eficiente al usuario y cumplir los protocolos de seguridad, que a veces ralentizan el acceso", confesaron algunos. Sin embargo, voces discordantes alegaron que hace cincuenta años esta discreción con los datos y la necesidad de su identificación para acceder a ellos ya existía, aunque de forma analógica. "Quizá antes no éramos tan impacientes, pero estábamos mucho menos preparados para evitar el robo de la información", dijeron.

No hay duda de que "la tecnología ha acelerado y repartido el conocimiento", tanto para los que la utilizan para bien como para los que lo hacen para mal, "esa es la pega". Así, hay que tomarles la delantera a "los malos" y estar preparados, y no vale con poner parches. "Se deben repensar los procesos y añadir la seguridad desde el diseño y la arquitectura de las aplicaciones y herramientas". Esta tarea se presenta compleja en el panorama actual, en el que la tecnología está cada vez más descentralizada. Cada usuario se conecta desde varios dispositivos diferentes, la movilidad, la cantidad de endpoints, Internet de las Cosas, las redes 5G, etcétera; son factores que nos facilitan la vida a nosotros, pero también a los ciberdelincuentes, convirtiéndose en "puertas de entrada hasta la cocina de nuestros datos si no están bien securizados". Sumar sinergias, romper silos dentro de las compañías y crear comunidades fueron algunas de las fórmulas propuestas para generar una lucha más activa contra el cibercrimen: "En esto ninguna empresa es rival de otra, todas debemos ser aliadas".

Al igual que ciertos avances tecnológicos han añadido complejidad a la seguridad, han surgido otros que la benefician, como la inteligencia artificial y el machine learning, "para las amenazas de ingeniería social"; o el big data y analytics para recabar y analizar la información sobre los ataques, "ya que la mayoría son de día cero". No obstante, incidieron en la importancia de saber utilizar estas tecnologías correctamente para sacarlas el máximo partido, "si no, se convierten en una herramienta más".

MELCHOR SANZ, DIRECTOR DE TECNOLOGÍA DE HP

"LAS CIBERAMENAZAS CRECEN Y, SOBRE TODO, EVOLUCIONAN"

Las ciberamenazas están creciendo, pero, sobre todo, están evolucionando. Hasta ahora, los ataques estaban dirigidos al data center, sin embargo, en los últimos tiempos se ha detectado que estos están cada vez más dispersos debido a la multitud de dispositivos desde los que nos conectamos, la variedad de puntos de acceso, la movilidad y a tecnologías como Internet de las Cosas. Todo ello supone nuevas oportunidades para los hackers malos.

ALEX TETERIS, TECHNOLOGY EVANGELIST DE ZSCALER

"UN 70-80% DE LOS DATOS DE INTERNET ESTÁN ENCRIPTADOS"

Hace unos años, solo el 20% de los datos de Internet estaban encriptados. Hoy en día, el porcentaje ha aumentado a un 70-80%, y dentro de uno o dos años, estará en torno al 100%. Por este motivo, es primordial que seamos capaces de desencriptar este tipo de tráfico para identificar malware oculto, de lo contrario, conectarse será como subirse a un avión en el que solo un pequeño número de maletas han sido escaneadas: reinará la inseguridad.

ALEXANDRE TOVAR, EXPERTO EN SEGURIDAD DE IPM

"HAY AMENAZAS QUE BUSCAN DESTRUIR LO MÁXIMO POSIBLE"

En la actualidad, todavía estamos sufriendo las amenazas producto de la guerra cibernética entre gobiernos que comenzaron en los años 90. También somos víctimas de las amenazas relacionadas con la actividad económica. Sin embargo, en los últimos cinco o seis años venimos sufriendo un tipo de amenaza más perjudicial, ya que no tiene una motivación económica clara, sino que persigue destruir lo máximo posible y hacer daño reputacional.

MARIO GARCÍA, COUNTRY MANAGER DE CHECK POINT

"LA FALTA DE PROTECCIÓN NO ES POR FALTA DE TECNOLOGÍA"

Aunque se ha avanzado mucho en términos de seguridad, en España hay muchas empresas que se han quedado atrás, y no es por falta de tecnología. No se trata de qué va primero, si el escudo o la lanza, la protección o los ciberatacantes. Existen sistemas de protección tan modernos y preparados como los utilizados para el cibercrimen, el problema es que las compañías no cuentan con ellos y, si los tienen, los tienen mal instalados.

LUIS BERNAL, ESPECIALISTA EN NSX DE VMWARE

"LOS CIBERATAQUES VAN HACIA UN MODELO DISTRIBUIDO"

Los ciberataques se han transformado al igual que lo han hecho las aplicaciones de negocio, yendo desde el centro de datos tradicional hacia un modelo distribuido, desde el core al edge y a las distintas cargas en las nubes públicas y privadas. Así, las organizaciones están aumentando el perímetro de protección más allá de los CPD y las sedes remotas para evitar los movimientos laterales de los ciberdelincuentes.

La adquisición de esta tecnología, obviamente, requiere de una inversión, -"que no un mero gasto como antes era considerado"-, y no solo en el software, sino en "la captación de talento cualificado y la formación de las personas para utilizarlo". Sin embargo, a veces es más importante que el personal aprenda a utilizar correctamente las herramientas con las que ya cuenta que comprar la última tecnología. Pero no todo es cuestión de concienciación, "sino también de responsabilidad". Muchas veces, los empleados consideran el dinero o la reputación de la empresa como algo ajeno a ellos, por lo que no toman las mismas precauciones que si les afectara a sus bienes personales, "y no se dan cuenta de que, más directa que indirectamente, lo que le suceda a la empresa también les afecta a ellos". Para demostrar a estos profesionales lo fácil que es caer en una trampa cibernética hubo compañías que confesaron haber puesto a prueba a sus empleados, "para que vean que no deben despreocuparse".

Cuando hablamos de tecnología no nos referimos únicamente al software, a veces el hardware es el gran olvidado en este asunto. Dispositivos como las impresoras, por las que se extrae gran cantidad de información en papel, pueden ser, aún hoy en día, un punto débil; sin olvidar el puerto USB de los ordenadores. "Desde 2012 existen mecanismos para encriptar el puerto USB y que solo sirva para enchufar el ratón, no para meter ni extraer información del PC", explicaron; sin embargo, "las empresas o desconocen estas posibilidades o pasan de emplear tiempo en configurarlas". Por eso es tan importante que la seguridad se incluya desde el diseño y se aplique automáticamente.

A pesar de mantener los sistemas críticos en el modelo analógico, una opción comentada en el encuentro, la mayoría lo descartó ya que "de aquí a unos años convivir con el legacy va a suponer más esfuerzo que arriesgar a digitalizarlo". Un ejemplo es cómo la nube ha pasado en poco tiempo de considerarse un riesgo a "un lugar casi más seguro donde alojar los datos que en un CPD propio".

El poder del cibercriminal

El gran pecado que cometemos es subestimar el poder de los ciberdelincuentes, "lo subestimamos hasta que somos sus víctimas, claro". "Los hackers maliciosos se pueden organizar en compañías como las nuestras, -e incluso más potentes-, y con nuestros mismos fines, buscar el coste de oportunidad y la retribución económica", explicaron. Ya sea un ataque masivo a una o varias empresas o individual a una sola persona, debemos ver estas acciones como lo que son: "delitos", y "no tener dejadez para denunciar". Aunque muchas organizaciones renuncien a denunciar por temor a que se sepa que han sido atacadas y sufrir un daño reputacional, "esto juega en su contra, ya que dificulta la investigación de estos delitos y la asunción de las penas", a lo que hay que unir

1 Roger Martínez, UCIBER – Mossos d'Esquadra | **2** Emili Torres, CCOO | **3** José Vázquez, Barraquer | **4** Esther Sánchez, Axa | **5** Afons Sánchez, Casaviva | **6** Iñaki Sainz, CCCB | **7** Laia Porcar, TSB | **8** Eduardo González, Sabis | **9** Roger Cuadras, ARAG | **10** Manel Rodríguez, Aramark | **11** Alonso Flores, ATL Ens d'Abastament d'Aigua Ter-Llobregat | **12** Ramiro Cid, Abelló Linde | **13** Sergio Juárez, Cuatrecasas | **14** Pere Solé, Cuatrecasas | **15** Joan Centellas, Penguin Random House | **16** Marc Novo, Miguel Torres | **17** Albert Orriols, Grup Serhs | **18** Jesús Soro, CNMC | **19** Marcos Sancho, Clínica Sant Jordi | **20** Javier Martínez, A. Menarini Diagnostics | **21** Víctor Huerta, Universidad Politécnica de Cataluña

"la laxa normativa de algunos países y la falta de recursos de las autoridades para perseguirlos", al final nada frena a los ciberdelincuentes. Sin contar la falta de datos oficiales en materia de ciberseguridad que se acusa por parte de empresas e instituciones, "algo que debería ser obligatorio".

Los ataques cada vez son de más diversa naturaleza y pueden perseguir objetivos económicos, sociales o políticos. "Incluso existen intereses individuales de miembros de las propias compañías que propician los ataques o las brechas de seguridad desde dentro, para hacer daño reputacional por venganza o para ascender de posición". Lo que es seguro es que nada es seguro. Por este motivo, "más que un plan de prevención, -que también-, hay que tener uno efectivo de resiliencia o recuperación después de un ataque". Tanto para la protección como para la reacción es necesario "tener a punto el tridente: tecnología, procesos y personas".

Que tenemos que aprender a convivir con los conflictos de seguridad es innegable, no en vano, los seguros de riesgos en ciberseguridad están creciendo exponencialmente y las aseguradoras ya los colocan en nivel de alerta "por encima de los conflictos geopolíticos o los desastres climáticos". Además, el CISO, una figura de relevancia menor hace no tantos años, ha pasado a depender, en muchos casos, directamente del CEO, en vez de del departamento TI. Con todo, algunos expertos se mostraron pesimistas arguyendo que, de momento, estamos perdiendo la batalla contra los cibercriminales, aunque otros difirieron con que "no importa perder alguna batalla, esta es una guerra permanente donde lo que prima es la resistencia". ■