Texto Andrea Gómez
Fotografía Santiago Ojeda
Vídeo J. Pariente

VEMOS MÁS AMENAZAS PORQUE CADA VEZ PODEMOS OÍR Y VER MEJOR

Las asignaturas pendientes en torno a la ciberseguridad

"La transformación digital o el GDPR se cuelan en los despachos de los directivos y estos empiezan a interesarse"

La carrera a contrarreloj por la digitalización de las organizaciones ha traído numerosos cambios positivos para la sociedad durante los últimos años, pero también ha abierto una ventana al crimen organizado, que ve en la red un espacio infinito de posibilidades para lucrarse a través del robo de datos de las compañías.

Los ataques informáticos contra empresas, gobiernos y usuarios individuales se multiplican a un ritmo alarmante, lo que hace que las organizaciones se preocupen cada vez más por proteger sus redes. El concepto de la ciberseguridad nació en 2005, alentado por la explosión de Internet, y ha ido evolucionando con la interconectividad de los dispositivos móviles y la era de los datos.

La cultura de la ciberseguridad es aún una asignatura pendiente para la mayoría de las organizaciones, las cuales relegan esto a un departamento y no lo entienden como algo intrínseco en la compañía. Con la intención de seguir concienciando sobre la importancia de la ciberseguridad, Computing organizó un encuentro en el que participaron T-Systems, Panda Security y Micro Focus, junto a diversos expertos en ciberseguridad de organizaciones, públicas y privadas.

"La lista de amenazas es interminable", así daba comienzo a la tertulia Juan Navarro, Security Sales Executive de Micro Focus. "Tratar de adivinar el futuro del cibercrimen es como mirar una bola de cristal", afirmaba.

"Durante los últimos años hemos hablado de un incremento exponencial de las amenazas, esto ha traído consigo mayor formación y concienciación dentro de las organizaciones con respecto a la ciberseguridad", comentaba María Campos, VP Sales Worldwide Key Account, MSSP y Telcos de Panda Security.

"La ciberseguridad empieza a ser algo sexy", señaló José Arias, Head of Security Sales de T-Systems. Según indicaba, "vemos cómo se está popularizando, en parte gracias a incidentes como WannaCry, la aplicación del GDPR, o el buen trabajo del CCN".

En busca del fallo humano

Las amenazas cada vez son más sofisticadas y difíciles de detectar, lo que ha provocado que se busque

JOSÉ ARIAS, HEAD OF SECURITY SALES DE T-SYSTEMS

"LO DIGITAL HA POPULARIZADO LA CONCIENCIACIÓN EN TORNO A LA SEGURIDAD"

La digitalización está siendo un driver interesante, cuanto más acercas lo digital a tu negocio, más importante es la seguridad; un ejemplo está relacionado con el tema de los coches conectados o la automatización, donde la seguridad es clave en áreas como el control de los sistemas industriales.

Sobre GDPR, considero que va a suponer un cambio sustancial en cuanto a concienciación. Los que trabajamos en seguridad sabemos que es clave. GDPR ha llegado a un nivel de popularidad muy alto, todos hemos recibido correos para renovar los acuerdos de confidencialidad, y ha supuesto un driver muy importante para el negocio el hecho de que sea una normativa europea. T-Systems tiene una alta concienciación en torno a la privacidad de los datos, vemos que estos no son una mercancía que se pueda comprar, sino un derecho como tal que ya teníamos embebido.

JUAN NAVARRO, SECURITY SALES EXECUTIVE DE MICRO FOCUS

"HAY QUE ESTAR PREPARADOS ANTE LA LISTA INTERMINABLE DE AMENAZAS"

Hay que estar preparados ante los ciberaquetes continuos. Es por eso que nuestra intención como proveedor es tratar de proporcionar herramientas a nuestros clientes para que puedan reaccionar de la mejor manera posible ante las nuevas amenazas que están surgiendo, y estar a su lado para ver qué necesitan en cada momento.

Sí quiero también abordar GDPR, que ha supuesto un cambio considerable. Hay muchas organizaciones que llevan ya mucho tiempo preparándose, no solo se trata de revisar lo que teníamos y tratar de adaptarse, sino que hay que añadir nuevos procedimientos y metodología, identificar información sobre los datos que manejamos, etc., y esto no ha sido sencillo. La gran empresa ha tenido tiempo y recursos dedicados a la adecuación, y yo creo que esto se está notando. Es un proceso de madurez que no es llegar a una fecha y ya está, sino que hay que seguir evolucionando.

MARÍA CAMPOS, VP SALES WORLDWIDE KEY ACCOUNT, MSSP Y TELCOS DE PANDA SECURITY

"NUESTRAS CLAVES SON PREDICTIVIDAD, PROTECCIÓN Y RESILIENCIA"

Panda es una empresa con una visión muy cloud, con soluciones basadas en servicios que apuestan por la proactividad. Ante las amenazas, nuestras claves son predictividad, protección y resiliencia.

En cuanto a GDPR, tenemos que recordar que afecta a todas las empresas que prestan bienes o servicios sobre ciudadanos de la Unión Europea independientemente de donde tengan sus oficinas o servidores. Sin embargo, vemos cómo todavía más del 40% de los profesionales de TI en Estados Unidos creen que no les afecta la regulación. Desde Panda llevamos muchos meses con diversas iniciativas para ayudar en esa adopción con guías, documentos o reuniones. Pero también hemos desarrollado el Data Control, dentro de la plataforma Adaptive Defense, un módulo para ayudar en el cumplimiento de GDPR que ayuda a descubrir, auditar y monitorizar en tiempo real ficheros de datos personales, para simplificar todos estos procesos.

Atento,
Óscar Sánchez

Centro Criptológico Nacional,
Pablo López

Codere,
Luís Miguel Brejano

el error en el fallo humano en lugar de en la red. Así lo ilustraba Pedro Pablo López, Gerente GRC & PIC (Compliance) de Rural Servicios Informáticos: "El timo de la estampita ha vuelto. Cada vez hay más sistemas de protección, lo que hace que los cibercriminales vuelvan a la ingeniería social, para ellos lo más sencillo es engañar al humano. Tenemos que trabajar mucho en ello, en lugar de limitarnos a aplicar parches cuando algo salte".

Juan Cobo, Global CISO de Ferrovial, coincidía con él. "Siempre hemos mirado más los sistemas, pero hoy nos centramos más en el comportamiento del usuario dentro de la red". Para el directivo, esto supone un cambio de paradigma dentro de la seguridad, "la formación, concienciación y la cultura de la ciberseguridad pasan a tener la misma importancia que el desarrollo de soluciones".

Juan Navarro, desde Micro Focus, quiso ilustrar la situación con un símil bastante acertado, "no todos podemos ser bomberos, pero todos deberíamos saber manejar un extintor". No consiste en tener controles externos sino "que los desarrolladores tengan en cuentan la seguridad en el propio desarrollo de los productos".

La palanca del GDPR

Pero sin duda, la entrada en vigor del GDPR o el impacto de incidentes tan mediáticos como WannaCry, han ayudado a que se visibilice una seguridad fuerte dentro de las organizaciones.

"El reglamento ayuda a implementar cosas que antes estaban un poco en el aire", comentaba Jorge Vidal, director del Departamento de Seguridad de Sistemas de Información y DPD de Fraternidad-Muprespa.

En España ya existía la LOPD, que regulaba el uso de datos personales, pero ahora, la entrada en vigor del nuevo reglamento de protección de datos europeo ha supuesto un cambio de modelo. "La diferencia entre la LOPD y el GDPR es el cambio de paradigma. La LOPD te tutelaba mucho más, te marcaba la forma en la que debías proteger tus datos. El GDPR nace en un entorno cambiante, te hace responsable de la gestión de los datos y la valoración del riesgo, pero no te dicta cómo has de protegerlos, tu eres libre de tomar las medidas que consideres oportunas", explicaba Luis Ballesteros, CISO de Wizink.

Por otro lado, gracias a la regulación se han creado departamentos de ciberseguridad dentro de la Administración Pública. Así lo narraba Rafael Santos, CISO de la Dirección General de Organización e Inspección del Ministerio de Fomento, "para nosotros la legalidad y normativa es lo que dicta que trabajemos o no sobre un tema. A medida que la normativa se va modificando da lugar a que haya gente que se dedique específicamente a temas de ciberseguridad, antes ni siquiera teníamos un CISO". Como en muchos otros temas digitales, la Administración Pública va a la carrera por detrás del sector privado, "hasta hace nada no existían presupuestos para la seguridad informática, pero ahora gracias a estas normativas sí. Pero de momento dependemos en gran parte del CCN, es más barato contratar sus servicios que cada ministerio gestione su propia seguridad".

Aunque Óscar Pastor, gerente de Seguridad de Isdefe, empresa perteneciente al Ministerio de Defensa, reconocía que "el GDPR puede ser una palanca, pero hace falta más. El talento es crítico, y la administración en esto no puede competir con el sector privado. Me llegan constantemente peticiones de talento desde la Guardia Civil o la Policía y son casi imposibles de suplir, y de retener una vez captado".

José Ramón Monleón, CISO de Orange, hizo una puntualización al respecto, "en mi opinión, el GDPR es algo beneficioso, pero no debe hacernos creer que está todo hecho. Puede haber empresas que ahora piensen: '¿tengo datos personales? No, pues entonces esto no va conmigo'. Y no es así. El GDPR está bien como punto de partida, pero no

Ministerio de Fomento,
Rafael Santos

Ferrovial,
Juan Cobo

Fraternidad-Muprespa,
Jorge Vidal

Guardia Civil,
Juan Sotomayor

perdamos el norte. La ciberseguridad afecta a toda la información y a todas las infraestructuras de una compañía. Hay problemas de ciberseguridad que no tienen nada que ver con los datos personales y aun así pueden poner en riesgo a tu empresa".

Presupuestos al alza

Pero de la misma, la normativa ha sido también un driver para el aumento de presupuestos dedicados a la protección informática dentro de las compañías privadas. "La legislación nos ayuda a que la seguridad se convierta en un tema estratégico, lo que hace que sea más fácil defender los presupuestos. Esto se mueve por impactos y gracias a temas como WannaCry o el GDPR, he visto cómo nuestro presupuesto se incrementaban año tras año", señalaba Óscar Sánchez, gerente de Tecnología de Atento.

"La transformación digital o el GDPR se cuelan en los despachos de los directivos y estos empiezan a preguntar", señalaba Luis Miguel Brejano, responsable de Seguridad de Sistemas de Codere. "Gracias a las multas millonarias que vemos en los periódicos, los consejos de dirección ven que realizar una inversión en seguridad y protección de datos quizás tenga rentabilidad". Añadió, "el GDPR nos trae madurez y la oportunidad de que ahora todas las empresas protejan los datos de sus negocios. Esto trae consigo la creación de soluciones que abaratan el coste de las analíticas, las cuales dan un valor diferenciador a tu compañía en el mercado. Estas palancas sumadas a un buen plan de seguridad hacen que los presupuestos sean recurrentes".

Al respecto, David Moreno del Cerro, director de Seguridad y Sistemas de TI de Tendam, quiso hacer una llamada de atención al resto de responsables: "Gran parte de los problemas con los que nos encontramos los hemos generado nosotros, no somos capaces de trasladar a los consejos nuestras necesidades de forma que ellos las comprendan, entonces, hasta que no han saltado temas como WannaCry ellos no se han visto para qué servimos. Con el GDPR, he tenido que explicar de nuevo procesos que llevaban años implantados, hay que cambiar el lenguaje de cara a los comités de administración y enfocarlo al negocio, hacia algo que ellos puedan cuantificar, como el impacto reputacional o el valor bursatil".

Aunque como muchos quisieron resaltar, esto no es nada nuevo, "hablamos de nuevas amenazas, pero luego, si nos fijamos en casos como Wannacry, vemos que no era nada nuevo; si hubiéramos prestado más atención habríamos podido reducir parte del daño que causó", aseguraba Ramón Ortiz, responsable de Seguridad de Mediaset.

Y es que, "no hay que prepararse para Wannacry, sino que hay que prepararse para un ransomware", como añadía Juan Sotomayor, jefe del Departamento de Delitos Telemáticos de la Guardia Civil. Explicaba que "uno de los grandes retos es la compartimentación de la seguridad en las compañías, los procesos de seguridad han de ser transversales dentro de la organización".

Por último, Pablo López, segundo jefe del Departamento de Ciberseguridad del Centro Criptológico Nacional, puso un punto positivo al estado de la ciberseguridad en España. "Cuando decimos que cada vez hay más amenazas no siempre implica algo malo, también significa que hemos alcanzado un grado de madurez mayor y ahora podemos ver y oír mejor, nuestras capacidades de detección están más desarrolladas. Estamos viajando mucho a Latinoamérica y quieren nuestras capacidades. Ahora vamos a Colombia a controlar que el proceso electoral se haga sin incidencias, y cuando el mercado latinoamericano quiere comprar algo es porque sabe que es bueno". Desde luego, "aún queda mucho por hacer, pero sí que hay madurez y cosas que se hacen muy bien". ■

"Hay que cambiar el lenguaje y enfocarlo al impacto directo de la seguridad en el negocio"

Wizink,
Luis Ballesteros

Tendam,
David Moreno del Cerro

Isdefe,
Óscar Pastor

Mediaset,
Ramón Ortiz

Orange,
José Ramón Monleón

RSI,
Pedro Pablo López