EL PAÍS

Publicación	El País Suplemento, 1	Fecha	14/02/2021
Soporte	Prensa Escrita	País	España
Circulación	164 804	V. Comunicación	277 618 EUR (336,486 USD)
Difusión	115 479	Tamaño	8,52 cm² (1,4%)
Audiencia	1 013 000	V.Publicitario	9454 EUR (11 459 USD)

Ciberseguridad Empresas y particulares siguen desprotegidos.

EL PAÍS

Publicación	El País Suplemento, 4	Fecha	14/02/2021
Soporte	Prensa Escrita	País	España
Circulación	164 804	V. Comunicación	277 618 EUR (336,486 USD)
Difusión	115 479	Tamaño	501,53 cm² (80,4%)
Audiencia	1 013 000	V.Publicitario	52 866 EUR (64 076 USD)

Escudos contra 'hackers' que atacan por varios frentes

La clave es tener sistemas actualizados, soluciones integrales de defensa y formar bien a la plantilla

Elena Sevillano

En diciembre de 2020, la compañía estadounidense SolarWinds sufrió un ciberataque "altamente sofisticado", "extremadamente dirigido" y realizado por "un estado nacional externo", según informó la propia víctima. El objetivo no era, en realidad, este proveedor informático en sí, sino sus poderosos clientes, entre los que se cuentan Microsoft, Visa, Ford, la NASA y el Pentágono. En total, casi 20.000 empresas y Gobiernos afectados, dedos señalando a Rusia (que lo niega) y un revuelo internacional que aún colea. Este "*Falcon Crest* de los ataques", como lo denomina algún experto a la vista de sus visos de culebrón al que no le faltan *hackers* infiltrándose, agencias gubernamentales buscando *software* espía, ramificaciones e implicaciones geopolíticas, visibiliza la necesidad de proteger la infraestructura de tecnología de la información (TI) de negocios digitalizados y conectados que viven, cada vez más, en la nube.

Por cada caso sonado que salta a las noticias se suceden, entre bambalinas, cientos de ofensivas y contraofensivas, vulnerabilidades solucionadas (a tiempo o no), fallos de seguridad en sistemas operativos y parches para esos fallos, en una suerte de guerra sorda, poco conocida por el gran público, que en 2019 se saldó con más de 120.000 ataques, según José Antonio Cano, director de Análisis y Consultoría de IDC Research España. Y que se ha recrudecido con la pandemia provocada por la covid-19. "En marzo de 2020 pasamos, de un día para otro, de acudir a nuestro trabajo a teletrabajar; la digitalización se ha hecho demasiado deprisa, con muchas concesiones a los empleados en materia de seguridad informática, lo que ha abierto puertas para que los malos ataquen", apunta Alejandro Ramos, director global de Operaciones de Seguridad de ElevenPaths, el equipo de ciberseguridad en Telefónica Tech.

"Los ataques informáticos cada vez son más, y más sofisticados, porque estamos más conectados y por el auge de herramientas colaborativas", coincide Cano, recordando que las empresas reciben más de 500 a la semana, y que no todos se convierten en brechas, porque las protecciones son cada vez mayores y mejores. Resalta el papel de la inteligencia artificial en los sistemas IDS/IPS (detección y prevención de intrusiones), y la demanda de productos como *firewall* (cortafuegos) o mitigación de DDoS, que consiste en bloquear y absorber picos maliciosos en el tráfico de red y el uso de aplicaciones causados por ataques DDoS o de denegación de servicio. Y cree que se está invirtiendo en medios y talento para salvaguardar infraestructura TI. El 55% de los ejecutivos encuestados en el Global Digital Trust Insights 2021 de la consultora PwC planea aumen-

EL PAÍS

Publicación	El País Suplemento, 5	Fecha	14/02/2021
Soporte	Prensa Escrita	País	España
Circulación	164 804	V. Comunicación	277 618 EUR (336,486 USD)
Difusión	115 479	Tamaño	508,09 cm² (81,5%)
Audiencia	1 013 000	V.Publicitario	53 354 EUR (64 668 USD)

UNIÓN PROFESIONAL

ERIK ISAKSON (GETTY IMAGES)

tar sus presupuestos en seguridad cibernética este año, y el 51% afirma estar fichando a expertos en este campo.

Además de la infraestructura TI, hay que tener en cuenta, cada vez más, la nube o *cloud*, donde están migrando muchos de los procesos de negocio. "La ciberseguridad ha de ser compañera en ese viaje", destaca Gabriel Treiband, director comercial de Excem Technologies. Proteger la integridad de una instalación *on premise* (en local) dentro de una empresa implica defender el perímetro: a un lado, Internet; al otro, los dispositivos de la red interna de la organización; interponiéndose, murallas de nombre *firewall* o UTM (gestión integrada de amenazas), que gestiona de manera centralizada las amenazas a golpe de antivirus, *firewall,* IDS/IPS, *antiphishing* (para evitar suplantaciones, normalmente mediante el correo electrónico, que buscan obtener datos sensibles), *antispam,* redes privadas virtuales o VPN, sistemas de protección de redes wifi, filtrado de contenido... "El movimiento hacia la nube está desplazando la ciberseguridad perimetral a la centrada en el dato", avanza Cano.

En agosto de 2019, la consultora TI Garnet publicó su informe *The Future of Network Security Is in the Cloud* (*El futuro de la seguridad de las redes está en la* nube), en el que proponía SASE (Secure Access Service Edge), un nuevo modelo de seguridad de Red basado en la nube que combina múltiples tecnologías —SD-WAN, SWG, CASB, ZTNA, FWaaS— en un paquete ofrecido como servicio; vaticinaba que el 40% de las empresas buscarían adoptarlo para 2024. Unos meses después, su vicepresidente de investigación, Andrew Lerner, saludaba este nuevo enfoque holístico, con base en la nube, en su *post Say Hello to SASE* (dile hola a SASE), subrayando la capacidad de la plataforma para controlar, cifrar, monitorizar y, en una palabra, proteger el dato; de paso, indicaba cómo pronunciar el palabro: *sassy*.

Consumo como servicio

La seguridad se está empezando a consumir como servicio, gestionado por proveedores especializados, según observa Cano. El proveedor asegura la nube; los servicios son responsabilidad de las compañías, que buscan "un *framework* unificado de seguridad", según prosigue, para andar protegidas por un nuevo territorio híbrido formado por las instalaciones propias; la nube, donde tiene aplicaciones, datos y servicios, así como un entorno externo que influye, compuesto por Internet de las cosas (IoT). Resulta cada vez más importante orquestar todo esto; un análisis de ciberseguridad, inteligencia y respuesta a amenazas. Algunas empresas están contratando grandes organizaciones de seguridad "que crean y fomentan relaciones con proveedores de seguridad más pequeños", construyendo ecosistemas mayores y completos como Broadcom, Cisco Security Technical Alliance "e incluso Splunk AppStore o AWS Security Competency Partners Network", según enumera Cano. Otras se decantan "por aumentar su gasto en plataformas multiproducto llave en mano, como Fortinet Security Fabric o Check Point Infinity", añade.

Si algo enseñó 2020 a las empresas fue que más les valía estar ciberprotegidas. Si la primera mitad del año discurrió algo tranquila, en el verano "vino la explosión", recuerda Ramos. El volumen de amenazas de *malware* observadas por McAfee Labs alcanzó un promedio de 419 por minuto entre abril y junio, 44 (un 12%) más que en el trimestre anterior, según informó en noviembre. No hay más que repasar la sucesión de incidentes que recoge el *Informe sobre el estado de la seguridad 2020* de Eleven Paths para comprobar no solo el cuánto, sino el qué. Fugas de información, ataques a webs corporativas, *phishing* con su variante del fraude del CEO (robar fondos de una compañía suplantando la identidad de un alto directivo), *smishing* cuando el engaño llega a través de una aplicación de mensajería instantánea, *botnets* o robots que controlan de manera remota los dispositivos inteligentes.

Y la gran tendencia de la temporada, el *ransomware* o secuestro de datos, que es un programa dañino que inutiliza un sistema y pide un rescate a cambio de devolverlo a la vida. "Si se produce en una fábrica, ésta, directamente, deja de producir", sentencia Ramos. "Es un delito que ha subido un 300%", revela. Antes de la pandemia, Telefónica Tech acudía a ayudar a sus clientes frente a ataques *ransomware* un par de veces al año; desde el verano lleva cuatro incidentes internacionales. Los *hackers* han comenzado por chantajear a multinacionales, pidiendo rescates de hasta más de cuatro millones de dólares. Un ataque *ransomware* a Garmin dejó incluso barcos a la deriva hasta que el fabricante de dispositivos de GPS pagó, según varios medios estadounidenses. Estos asaltos, poco a poco, irán bajando hasta las medianas y pequeñas empresas, advierte Ramos, con exigencias de rescate proporcionales. El experto concede que se está creciendo en ciberseguridad, sí, pero no lo suficiente, ni lo suficientemente rápido. "Las grandes compañías están concienciadas, de hecho son las que impulsan una subida del 20% anual del negocio global; las medianas empiezan a hacerlo; quedan las pequeñas y los particulares", señala. Tres de cada siete ciberdelitos están dirigidos contra pymes, según el comparador de seguros Acierto.com, que, arrimando el ascua a su sardina, resalta la aparición de ciberseguros para cubrir, en caso de ataque, el asesoramiento legal, la investigación de la filtración, la restauración del equipo y recuperación del *software* o las posibles multas de la Agencia Estatal de Protección de Datos.

"Los ciberdelincuentes necesitan un medio de comunicación para propagar sus campañas fraudulentas, siendo el correo electrónico su preferido; esto se debe principalmente a que la gran mayoría de pymes y autónomos utilizan habitualmente el correo electrónico como herramienta de trabajo. Esta frecuencia en su uso es lo que vuelve a esta herramienta peligrosa, ya que en muchas ocasiones las tareas se realizan de forma mecánica, lo que puede provocar infecciones por *malware* o accesos a páginas web fraudulentas", afirma la guía *Ciberamenazas contra entornos empresariales,* publicada por el Instituto Nacional de Ciberseguridad (Incibe) en enero para desgranar los principales ciberataques que puede sufrir una empresa y ofrecer consejos sobre cómo enfrentarlos.

Comprobaciones necesarias

"Las pymes, donde casi todo está subcontratado, incluido el *e-mail,* han de comprobar que sus proveedores tengan un sello de ciberseguridad", avisa Gabriel Treiband. Cualquier corporación, da igual su tamaño, no puede limitarse a asegurar la infraestructura TI propia, sino que ha de comprobar que la de su cadena de suministro esté igualmente defendida. "Imagina que quien hace el reparto de tus artículos tiene una brecha de seguridad, y todos los datos de tus clientes quedan expuestos", alerta Treiband. Excem Technologies cita a Accenture para advertir de que el 40% de las violaciones de seguridad son indirectas, "ya que los ciberatacantes se dirigen a los eslabones débiles de la cadena de suministro o del ecosistema empresarial", y de que "los programas de ciberseguridad sólo protegen activamente alrededor del 60% del ecosistema de una organización".

Una empresa ha de tener continuamente actualizados sus sistemas de ciberseguridad, tanto en *software* como en *hardware,* según aconseja Excem Technologies. Mantenerse al día en cuanto a innovaciones. Y realizar simulacros. "En ocasiones, la teoría se queda solo en eso y, cuando llega la hora de la verdad, la plantilla no sabe cómo reaccionar ante un ataque real", expone. "Son importantes desde el punto de vista técnico, porque muestran los puntos débiles y enseñan a reaccionar mejor, pero también desde el punto de vista de la comunicación", argumenta Treiband. "Si el *e-mail* está muerto y la Intranet no funciona, ¿cómo le dices al personal que no encienda el ordenador? ¿Qué le cuentas a un cliente que llama por teléfono para preguntar qué está pasando? Esa parte de comunicación externa, reputacional, de gestión de crisis, es fundamental", enfatiza.

YUICHIRO CHINO (GETTY IMAGES)

El factor humano

Junto a las medidas legales y técnicas, la guía *Ciberamenazas contra entornos empresariales,* de Incibe, resalta la importancia de las organizativas, que incluyen "llevar a cabo acciones de formación y concienciación en ciberseguridad". El factor humano es clave a la hora de prevenir o evitar una agresión. Pero el 86% de las 50 compañías de ámbito nacional consultadas por PwC España entre junio y septiembre de 2020 admitían no tener una cultura de ciberseguridad en su organización, o bien que esta debería mejorarse. El informe del estado de cultura de ciberseguridad en el entorno empresarial de PwC muestra poca madurez en este terreno, especialmente en lo concerniente al comportamiento de la empresa y de sus empleados.

"La gran mayoría de incidentes de seguridad que afectan a las empresas tienen en común dos factores: el correo electrónico y comunicaciones que utilizan ingeniería social", explica la guía de Incibe, que define ingeniería social como el uso de diferentes técnicas de manipulación psicológica con el objetivo de conseguir que las potenciales víctimas realicen cualquier tipo de acción que pueda beneficiar al ciberdelincuente, como revelar información confidencial o instalar *software* malicioso. "En la mayoría de ocasiones, los ciberdelincuentes atacan al eslabón más importante en la cadena de la seguridad: los empleados", concluye.

"La tecnología hay que activarla, y somos nosotros quienes lo hacemos; es mucho más importante la gente que la tecnología", insiste Gabriel Treiband. Cuidado con los *e-mails* que abres, cuidado con no actualizar tu sistema operativo, cuidado cuando te conectas a una wifi abierta. "Un empleado trabaja en remoto desde casa, con una wifi segura o una VPN que le ha instalado su empresa, pero baja al bar a tomar un café y aprovecha para mandar un *e-mail* de trabajo utilizando una wifi gratuita, y por ahí se cuelan los malos", pone como ejemplo.

Es cada vez más importante orquestar todo: un análisis de seguridad digital, inteligencia y respuesta a amenazas

La protección crece, pero no lo suficiente ni a la velocidad necesaria. Las pymes y los particulares siguen muy expuestos