Texto
Laura del Río

LA PANDEMIA HA ACTIVADO TODAS LAS ALARMAS DE LOS CISO

Más alerta que nunca

<< El ransomware y el phishing son las técnicas de ingeniería social más extendidas y las que han hecho el tándem más temido -pero más efectivo- en la Red junto con la Covid-19, el término que ha servido para poner la trampa.

Si algo ha quedado claro en los últimos años es que los hackers maliciosos ya no son "cuatro frikis" que van por libre, se organizan como lo puede hacer una compañía cualquiera y, muy posiblemente y a diferencia de las compañías, colaboran entre ellos en ciertos aspectos creando una industria potente de forma incesante, la del cibercrimen. Todo esto hace que sus ataques están muy bien dirigidos y sean cada vez más sofisticados. De la magnitud de las amenazas y cómo proteger

FEDERICO DIOS, PRESALES SENIOR MANAGER DE AKAMAI

"HAY UN CAMBIO EN LA DIRECCIÓN DE LOS ATAQUES Y UN AUMENTO DEL RANSOMWARE Y PHISHING"

La situación que ha dejado la llegada de la Covid-19 está marcada por una serie de cambios. En lo referente al cibercrimen, el primer cambio ha sido el de dirección de los ataques. El foco ha pasado de las infraestructuras o aplicaciones publicadas a los puntos de acceso de aplicaciones, servicios publicados para trabajo en remoto, VPN, etcétera. Un cambio impulsado por la movilidad. Por otro lado, los ataques de ransomware y el phishing se han intensificado notablemente en los últimos meses. También el trabajo en remoto ha propiciado la creación de un entorno híbrido en el que confluyen de manera directa la vida personal o del hogar con la vida profesional del usuario, contexto que está siendo aprovechado por los ciberdelincuentes para diseñar ataques mucho más encaminados a explotar la exposición que sufren los datos corporativos al mezclarse con la información, tecnologías y dispositivos particulares del empleado.

SERGIO BRAVO, REGIONAL SALES MANAGER DE BITDEFENDER

"ES PRECISA UNA SOLUCIÓN INTEGRAL QUE CUBRA EL CICLO COMPLETO DE SEGURIDAD"

La protección a las arquitecturas complejas que las compañías se han visto en la necesidad de desplegar tras la apertura del perímetro y las redes distribuidas ha supuesto un enorme reto para muchas de ellas. Para blindar la extensa superficie que es diana de los ciberdelincuentes y neutralizar los vectores de ataque, es precisa una solución integral de seguridad que cubra el ciclo completo: predicción, prevención, detección y respuesta. Bitdefender ofrece una solución que proporciona una cobertura completa del ciclo y que posee hasta 36 capas de tecnología, muchas de ellas basadas en machine learning. Esta herramienta unifica la protección a nivel de endpoint con un EDR innovador o incluso con servicios de Manager Detection and Response (MDR) en el caso de las empresas que opten por los servicios de DR gestionado de Bitdefender. Además, cuenta con tecnología de Risk Management adaptativa para identificar qué puntos necesitan reforzar sus clientes.

nuestras compañías han hablado los expertos en ciberseguridad en el encuentro virtual de Computing, organizado junto a Capgemini, Bitdefender, Akamai y Okta.

A raíz de la expansión del teletrabajo, el perímetro se ha extendido y se han multiplicado los dispositivos que acceden a la red W-LAN de la empresa, "aunque los vectores de ataque son prácticamente los mismos que existían antes de la pandemia, las compañías tienen que controlar un mayor número de endpoints y los atacantes son cada vez más listos y nos tienen más estudiados", dijo Javier Sánchez, CISO de Real HAYA Estate. Tecnologías como la IA y el machine learning han contribuido a hacer estos ataques más sofisticados y a dirigirlos, ya no a una empresa en general, sino a roles específicos de la misma. "No obstante, las personas estamos cada vez más preparadas y continuamente alerta".

El phishing comenzó a extenderse en el año 1996 con las entidades financieras como principal objetivo, pero hoy por hoy su espectro se ha abierto a todos los sectores. Por regla general -a no ser que el ataque vaya dirigido a un sector estratégico como Defensa o ciertos organismos públicos en los que se persigue obtener información y la recompensa es a largo plazo y se materializa de diferentes maneras, como el caso del ataque a SolarWinds-, los ciberatacantes suelen buscar una monetización rápida de su acción. Por este motivo, el ransomware o los ataques de denegación de servicio son los más comunes. "En ISDEFE solemos aplicar 'Threat Hunting', una estrategia de seguridad defensiva que permite reducir el tiempo de detección y respuesta ante un incidente", contó Óscar Pastor, gerente de Seguridad de ISDEFE (Ingeniería de Sistemas para la Defensa de

"Se está considerando la creación de un Centro de Operaciones de Ciberseguridad para la Administración General del Estado"

ANDRÉS DE BENITO, DIRECTOR DE CIBERSEGURIDAD DE CAPGEMINI ESPAÑA

"LAS EMPRESAS NO PUEDEN QUEDARSE ATRÁS EN LA CARRERA POR LA SUPERVIVENCIA"

Las organizaciones están permanentemente protegiéndose frente a continuos ciberataques, aunque solo salgan a la luz los que tienen éxito y, entre ellos, los de mayor impacto. Los ciberdelincuentes tienen la capacidad de identificar rápidamente al miembro más débil de la manada, o lo que es lo mismo, a la compañía más vulnerable del mercado. Si una organización se queda atrás en esa carrera por la supervivencia, caerá pronto en esa relación entre presa y depredador que hay entre empresa y hacker malicioso. Esta situación no va a mejorar, porque las empresas son cada vez más digitales, por lo que su dependencia de la tecnología va en aumento, exponiéndolas cada vez más a unas ciberamenazas cada vez más sofisticadas. Así las cosas, es necesario no bajar la guardia y estar preparados para reaccionar cuando ocurra un incidente, es la única manera de asegurar la supervivencia en la jungla digital en la que vivimos.

SAMIR ZERIZAR, CHANNEL SALES MANAGER DE OKTA

"RECOMENDAMOS APLICAR EL MODELO ZERO TRUST ENFOCADO EN LA IDENTIDAD DEL USUARIO"

La pandemia ha traído consigo un cambio radical en la forma de trabajar. Ahora los empleados desarrollan su actividad 100% de manera remota, fuera de la red corporativa, y las organizaciones se han puesto las pilas para securizar los accesos y e identificar claramente quién accede a qué datos determinados y durante cuánto tiempo.
Desde Okta recomendamos aplicar el modelo Zero Trust enfocado en la identidad del usuario, que es el que determina el nuevo perímetro de seguridad. La forma óptima de conseguirlo es implementando una solución céntrica que permita una gestión de identidades eficaz y el diseño de reglas más sólidas para saber en todo momento a qué aplicaciones se conectan los usuarios, tanto internos como externos a la compañía, con el objetivo de adquirir el control total sobre los accesos a los sistemas.

"El sector privado está mermando de profesionales al sector público porque les pagan salarios más altos"

España). Pastor también puso el foco en la cadena de suministro, "la gran olvidada, cuando es muy importante que tus proveedores estén igual de protegidos que tú".

Así las cosas, el entorno a proteger posee una cantidad de flancos difíciles de controlar. En este sentido, "se está considerando la creación de un Centro de Operaciones de Ciberseguridad para la Administración General del Estado. Un proyecto de varias decenas de millones de euros que puede estar financiado, en parte, por los fondos europeos, y mediante el que se desplegaría la infraestructura necesaria para monitorizar y automatizar a gran escala todos los organismos de la Administración Pública", explicó Pastor.

Proyectos ambiciosos como este son una muestra de "la importancia de aplicar la automatización en la prevención y detección de ciberamenazas", afirmó Juan Cobo, Global CISO de Ferrovial. "Las empresas dependemos cada vez más del mundo digital y tenemos que estar preparadas para reaccionar dentro de este entorno, nos venga lo que nos venga, ya sea una pandemia mundial, una crisis económica… Cualquier situación coyuntural no nos puede volver vulnerables". Cobo ve como un gran avance "la compartición de información entre compañías para defendernos y aprender de la experiencia de otros, al menos en situaciones extraordinarias como la que hemos vivido en estos últimos meses". Sin embargo, "los ciberdelincuentes siempre ganan más si vamos por libre", señalaron algunos expertos.

El cibercrimen es un negocio muy rentable, las compañías invierten más en protegerse que los ciberdelincuentes en atacarlas. "Aunque únicamente existieran cuatro atacantes, todas

ASISTENTES

1 Juan Cobo, Global CISO de Ferrovial | **2** Javier Sánchez, CISO de Real HAYA Estate | **3** Óscar Pastor, Gerente de Seguridad de ISDEFE | **4** Alberto López, IT & Cybersecurity Manager de Solaria Energía y Medio Ambiente | **5** Luis Ballesteros, CISO de WiZink Bank

las compañías del mercado tendrían la necesidad de protegerse frente a ellos", indicó Andrés de Benito, director de Ciberseguridad de Capgemini España. "Las organizaciones deben asegurarse, al menos a un nivel mínimo, para hacer frente a los ataques más básicos o más comunes. Para los malos, encontrar la brecha de seguridad más insignificante no supone un gran esfuerzo, sin embargo, para las empresas, confiarse y no protegerse hasta en lo más simple puede suponer su fin".

Las pesadillas del CISO

"No sé si los hackers maliciosos, o cibercriminales, dormirán bien por la noche, pero los hackers buenos -como todos los que hay en este encuentro- o CISO nunca descansan tranquilos", confesaba entre bromas Alberto López, IT & Cybersecurity Manager de Solaria Energía y Medio Ambiente. Todo sistema es vulnerable de una u otra manera, "si no ha sido atacado es porque aún no se ha descubierto su vulnerabilidad o no es lo suficientemente rentable hacerlo". Además, la crisis de la Covid-19 y el trabajo en remoto ha dejado relamiéndose a los cibercriminales de ingeniería social. "Ojalá la pandemia hubiera sido un simulacro para que todas las empresas analizaran sus infraestructuras y métodos. Por desgracia no ha sido algo programado, pero sí ha servido para que nos pongamos las pilas, aunque aún queda mucho por hacer. El trabajo nunca acaba".

Por lo menos, entre las preocupaciones del CISO parece que ya no está la de "luchar" con la alta dirección para establecer planes de ciberseguridad y presupuestos. "Los directivos están más concienciados y entienden mejor los riesgos de no securizar sus activos". Juan Cobo resaltó que "España es el séptimo país con una mejor calidad de ciberseguridad del mundo según el Global Cibersecurity Index de 2018". Habría que ver si las cosas han cambiado mucho en estos tres años.

Pero la concienciación no solo se da en el ámbito directivo de las empresas, sino también en los gobiernos y la sociedad. "Una de las primeras acciones que ha llevado a cabo Joe Biden en Estados Unidos es contratar a un comité de expertos en ciberseguridad para la Casa Blanca", contó Luis Ballesteros, CISO de WiZink Bank. Normativas como GDPR en Europa son el reflejo de esta sensibilización. No obstante, todos los dedos suelen apuntar a errores humanos en los casos de ataques más sonados, y no tranquilizan datos como que el 88% de los españoles estuvo dispuesto a ceder sus datos para asegurarse grandes descuentos en Navidad y que solo el 39% no compraría en un sitio web que pareciera ilegítimo, según porcentajes facilitados por Kaspersky. En este sentido, un usuario que no está concienciado en su vida personal, con los que considera sus propios datos, difícilmente lo estará en su vida profesional.

Por este motivo, porque aún queda mucho camino por recorrer, Ballesteros explica que "antes de autorizar a los empleados el acceso remoto a los sistemas allá por marzo de 2020, revisamos estos accesos y vimos que todos contaban con doble factor de autenticación y con un test de vulnerabilidades tanto automático como manual. Toda precaución es poca".

La siempre nombrada falta de presupuestos está dando paso a la falta de talento como principal quebradero de cabeza. "Los próximos dos años el dinero en el sector público no será un problema -sobre todo si invertimos bien el que nos llegue de los fondos europeos de recuperación-, lo que más falta hará será personal cualificado", apuntó Óscar Pastor. Aunque la calidad y el liderazgo de los profesionales en España es notable, "no hay suficientes hackers en el lado bueno. El sector privado está mermando de profesionales al sector público porque les pagan salarios más altos". La eterna demanda que, por el momento, no parece ser escuchada, la de la formación de profesionales en materias digitales, especialmente de ciberseguridad, para satisfacer las necesidades de todos los sectores. ¿Tardaremos tanto en generar este talento como en crear concienciación en seguridad o en destinar inversión a Tecnología? ■

"Todo sistema es vulnerable de una u otra manera, si no ha sido atacado es porque aún no se ha descubierto su vulnerabilidad o no es lo suficientemente rentable hacerlo"