La ciberseguridad en tiempos de coronavirus

La seguridad: objetivo "común" de empresas y *hackers* durante el Covid-19

La seguridad se ha convertido en el objetivo principal de empresas y *hackers* durante el Covid-19. Las primeras, para brindarla y hacerla infranqueable a los ataques de los segundos. Los ciberdelincuentes son conscientes de los beneficios que pueden obtener de un contexto como el actual. "Es habitual que durante determinadas situaciones planeen campañas con el único objetivo de engañar a sus potenciales víctimas para obtener crédito económico sin importarles los daños que pueden provocar", ha explicado Marco A. Lozano, responsable de ciberseguridad para empresas del Instituto Nacional de Ciberseguridad (INCIBE).

Olga Romero

Actualmente los *hackers* se están sirviendo de la crisis sanitaria para crear ataques. Unas amenazas que se van adaptando a la evolución de la situación, "de tal modo que los mensajes progresan al mismo ritmo que la realidad del momento", ha afirmado Lozano. Porque, como ha matizado el responsable de INCIBE, "el propósito es engañar al mayor número de usuarios y empresas posible".

Está claro que la pandemia del Covid-19 está suponiendo un reto para las empresas y una gran oportunidad para los ciberdelincuentes. Por eso las principales compañías de seguridad han analizado cómo ven el panorama actual.

Principales carencias en la seguridad de las empresas

El teletrabajo ha sido la principal preocupación de organizaciones y empleados. Para Eusebio Nieva, director técnico de Check Point para España y Portugal, "el último mes ha supuesto un gran reto en términos de ciberseguridad, debido a que las empresas no contaban con la in-

fraestructura necesaria para teletrabajar de forma segura". La protección de los diferentes dispositivos conectados a la nube corporativa es, a su juicio, una de las principales carencias a las que se han enfrentado las compañías.

Esta opinión la comparte José de la Cruz, director técnico de Trend Micro Iberia. "El confinamiento ha supuesto un reto tecnológico para todas las empresas, ya que nunca nos habíamos visto en la situación de que toda la plantilla se encontrase trabajando remotamente".

Sobre esta cuestión, Jorge López, *systems engineer* en Fortinet para España y Portugal, ha valorado la importancia de realizar un análisis de riesgos. Mientras que las empresas que han llevado a cabo este estudio previo han estado preparadas para abordar esta situación, "el resto no ha tenido más remedio que actuar de la mejor manera posible, adaptándose a la nueva realidad". Son estos análisis de riesgos los que brindan a las organizaciones la información necesaria para reaccionar de la mejor forma posible.

A la gestión de riesgo también se ha referido María Campos, vp de Cytomic, quien aboga por la necesidad de contar con un plan de seguridad y de respuesta a incidencias que minimice los peligros más frecuentes a los que se enfrentan las organizaciones. "En las últimas semanas numerosas compañías han tenido que improvisar sobre la marcha. Mientras esto ocurre, los ciberdelincuentes aprovechan la situación para incrementar sus ataques", explica.

En este contexto Sergio Martínez, Iberia *regional manager* de SonicWall, ha puntualizado que este incremento inesperado del trabajo en remoto "se ha producido en un entorno en el que muchas empresas no tienen suficientes licencias de red privada (VPN) o capacidad en sus dispositivos de acceso remoto para atender este incremento de usuarios". Debido a esta situación los empleados se ven obligados a buscar otras maneras de conectarse a las aplicaciones y datos corporativos, "muchas veces de forma no segura".

Borja Pérez, *country manager* de Stormshield Iberia, identifica, como grandes carencias en cuanto a la seguridad en el teletrabajo, el hecho de que "en España culturalmente no estamos preparados para el trabajo en remoto, porque prima el trabajo presencial". Por ello, "las empresas no han visto la necesidad de invertir en seguridad, lo que se traduce en falta de preparación, aunque siempre hay excepciones".

La visión de INCIBE

Los expertos de INCIBE han detectado diferentes tipos de ataques que emplean principalmente técnicas de ingeniería social. Estas amenazas emplean principalmente el correo electrónico, pero también han observado casos que usan otro tipo de medios como el teléfono, la mensajería instantánea, los SMS o la creación de páginas web fraudulentas. Entre los principales argumentos empleados destacan la suplantación de servicios de logística, un falso servicio técnico, la recopilación ilegítima de datos, remedios y curas del Covid-19, servicios de difusión de vídeos, música o juegos y suplantación de entidades financieras o administraciones públicas, entre otras.

En cuanto al teletrabajo Lozano ha puntualizado que "no se trata de un riesgo, sino más bien de una nueva situación que nos expone a posibles peligros en el uso de las tecnologías en un entorno de trabajo fuera de lo común; o, al menos, no usado de manera convencional". Por eso desde INCIBE aconsejan:

- Acceder a los servicios de una empresa a través de VPN.
- Primar el uso de dispositivos corporativos frente a los personales.
- Uso de contraseñas robustas y del doble factor de autenticación.
- Cifrar el equipo y realizar copias de seguridad con frecuencia.
- Uso preferente del cable para la conexión a Internet.
- Vigilar el tipo de correos recibidos.

Para cualquier consulta, de particulares o empresas, INCIBE tiene disponible el teléfono 017, gratuito y confidencial.

Para Anastasia Sotelsek, *principal sales engineer* de CyberArk, "la principal carencia es que muchas organizaciones no protegen sus cuentas privilegiadas y solo una correcta gestión de las mismas ayuda a mitigar el riesgo que corren los datos y activos más valiosos de una organización", ha indicado.

Los ciberdelincuentes y sus "nuevas" fórmulas de ataque

El Covid-19 ha provocado una sensación de vulnerabilidad para todas las empresas. "El teletrabajo, las videoconferencias familiares, los videojuegos, las plataformas de televisión o el uso de las redes sociales han sido el "caldo de cultivo" idóneo para el *phishing*, que se ha constituido como una nueva forma de pandemia virtual", ha explicado Juanjo Galán, *business strategy* de All4Sec. Pero las VPN o la conexión remota de escritorios también han sido objetivo de los ataques. Sin olvidar la expansión de las *fake-news*, "una lacra que nos afecta a todos por igual y que nos conduce a menudo a comportamientos irracionales".

Borja Pérez, de Stormshield Iberia, coincide con Galán en la gran presencia de campañas de *phishing* que utilizan la pandemia como gancho. "También hay un incremento importante del

phishing por SMS suplantando la identidad de varias empresas; así como ataques a organizaciones de la salud a través de Netwalker", explica. "Aunque no tenemos la certeza de que sean ataques dirigidos, sino más bien una campaña masiva que ha impactado también en la sanidad".

Por su parte, Samuel Bonete, *regional sales manager* de Netskope Iberia, ha hablado sobre los ataques híbridos. Un tipo de amenaza "en la que los delincuentes utilizan la nube para la distribución de *malware*". Los *hackers* dejan un *malware* en una instancia de Office 365 comprometida y de esta manera el usuario cree estar accediendo a su aplicación pero, en realidad, lo que está haciendo es infectando.

Desde Cisco Talos, la división de ciberinteligencia de Cisco, han alertado de campañas de *malware* y *phishing* con temática sobre Covid-19, ataques contra organizaciones que realizan investigaciones, desinformación y sitios web fraudulentos que pretenden vender mascarillas médicas. Eutimio Fernández, director de ciberseguridad de Cisco España, ha confirmado que "España tiene el porcentaje más alto de incidentes de seguridad en Europa como resultado de abrir un email no deseado: un 54 % frente a la media europea del 41 %".

Bitdefender monitoriza constantemente la forma en la que las amenazas se adaptan a las nuevas realidades. Juan Grau, *regional sales manager* de la compañía, ha comentado que "los usuarios de dispositivos móviles se han convertido en un objetivo prioritario". Los expertos de Bitdefender han observado que los *hackers* se han "centrado en las aplicaciones que más se utilizan en esta situación como, por ejemplo, el rastreador de la OMS, las aplicaciones de interacción social, de productividad o las enfocadas al ocio", ha explicado Grau.

> "Los mensajes cambian al mismo ritmo que la realidad del momento", Marco A. Lozano, (INCIBE)

Alfonso Ramírez, director general de Kaspersky en Iberia, ha hablado de Ginp, "un troyano bancario que hemos identificado". Este *malware* tiene una elevada incidencia en España ya que el 83 % de las víctimas de este ataque procede del territorio nacional. "Usa la pandemia Covid-19 como cebo y solicita dinero a cambio de información sobre personas próximas e infectadas por coronavirus", ha matizado.

"Las situaciones de caos son perfectas para los atacantes ya que crean situaciones de incertidumbre nuevas que facilitan su tarea", ha comentado Daniel Varela, ingeniero especialista de seguridad para el sur de Europa en F5 Networks. Desde la compañía están observando el aumento de ataques de *phishing* para extraer información personal y que además sirven para ataques más complejos. Por eso Varela ha destacado que "es básico que recibamos educación en esta materia. Es la manera más efectiva de prevenir los ataques".

Cambio de tendencia para la ciberseguridad

La pandemia del Covid-19 ya forma parte de la historia española y mundial. Esta situación excepcional cambiará la vida de la población, pero aportará muchos conocimientos. Una idea que comparte José de la Cruz, de Trend Micro Iberia. "Marcará un cambio de tendencia en las empresas al permitir y/o fomentar el teletrabajo. Esto tendrá un impacto claro y directo en cómo las organizaciones protegen sus activos: infraestructuras, datos y usuarios".

Para Daniel Varela, de F5 Networks, "el teletrabajo ha venido para quedarse". Esta situación ayudará a perder los miedos a que la productividad pueda verse afectada y las empresas están invirtiendo mucho esfuerzo para implantar o mejorar las soluciones que lo permiten. "Garantizar la seguridad de estos entornos de teletrabajo va a sufrir una importante demanda".

La situación actual ha dejado clara la "gran dependencia que tenemos de estar conectados y, si no estamos preparados, reconocer los peligros a los que nos debemos enfrentar", ha comentado Josep Albors, responsable de concienciación e investigación de Eset España. Ante esta situación las empresas deben entender la importancia de proteger los equipos y trabajar de una forma segura. "Sin seguridad y conectividad, su negocio pende de un hilo".

En esta misma línea se manifiesta Iván Mateos, *sales engineer* de Sophos Iberia, que insiste en la importancia de la ciberseguridad en cualquier entorno y momento. "Si antes era de vital importancia para las organizaciones contar con sistemas de seguridad avanzados, ahora se ha hecho visible que la ciberseguridad no es un asunto de segundo nivel". Mateos recuerda que los ciberdelincuentes siempre están preparados para aprovechar cualquier situación con la que puedan crear campañas de *malware*.

"La sociedad tiene que aprovechar lo aprendido en relación a las nuevas formas de hacer las cosas, lo que trae consigo un notable incremento de la exposición y la necesidad evidente de contemplar la ciberseguridad como un factor de diseño de todos estos servicios", ha comentado Rafael Rosell, director comercial de S2 Grupo. Durante este tiempo de confinamiento no solo se ha aprendido a teletrabajar: también a realizar diferentes trámites en remoto o prestar servicios no presenciales.

Desde Check Point tienen claro que la pandemia del Covid-19 va a traer cambios, tanto en el ámbito del teletrabajo como en una mayor concienciación sobre la importancia de estar protegidos en el mundo virtual. "La prevención es la mejor estrategia de protección", ha afirmado Eusebio Nieva. Por eso recomienda a todas las empresas contar con herramientas para garantizar la seguridad de los datos y los dispositivos.

Sergio Martínez, de SonicWall, explica que "el cambio que estaba previsto para los próximos cinco años se ha realizado en tan solo 15 días". La transformación ha sido tan rápida que ha provocado numerosas disrupciones y problemas que han aprovechado los ciberdelincuentes para crear una lista de ataques como *malware*, troyanos o *phishing*, entre otros. Se trata de un cambio que "nos ha pillado desprevenidos", insiste.

El teletrabajo: ¿qué riesgos abre y de qué manera hay que protegerse?

Eutimio Fernández, de Cisco España, recomienda que "hay que pensar en los usuarios y en sus puestos de trabajo como si nunca trabajaran dentro de un perímetro". Es fundamental disponer de la misma protección en cualquier entorno. La conexión VPN, los mecanismos de verificación multifactor, la seguridad *cloud* y DNS y la protección de cualquier dispositivo o terminal son las cuatro soluciones claves para garantizar un teletrabajo seguro.

Con el teletrabajo el robo de credenciales de VPN o la seguridad de los dispositivos son nuevos vectores de ataques que los *hackers* pueden explorar. "Para mitigar estos riesgos, se recomienda proteger el acceso con privilegios a sistemas críticos como soluciones de Zero Trust, autenticación biométrica y aprovisionamiento *just-in-time*", ha explicado Anastasia Sotelsek, de CyberArk.

Pero las prácticas de teletrabajo también han generado "estrés tecnológico", recuerda María Campos, de Cytomic, lo que se traduce en un aumento de los fallos y de los riesgos asociados que no se pueden eliminar pero que "las empresas deben tener presente para determinar medidas razonables y prácticas para mitigarlos". Para conseguir este objetivo hay que disponer de soluciones avanzadas y actualizadas, así como el empleo de programas de detección y respuesta en los *endpoints*.

Guillermo Fernández, *sales engineer* del sur de Europa en WatchGuard Technologies, ha afirmado que "nunca ha sido más importante para los empleados tomar un papel activo en la lucha contra los ciberataques, ya que el teletrabajo ha ampliado la superficie de ataque". Para ayudar a las empresas a protegerse, desde la compañía comparten una serie de consejos como hacer que la red doméstica sea privada, emplear contraseñas seguras, vigilar los correos electrónicos y emplear una conexión VPN.

Sobre los riesgos que trae el teletrabajo Samuel Bonete, de Netskope Iberia, explica que "lo primero en lo que piensan los usuarios es en los riesgos derivados de la protección de un perímetro ya inexistente". Según datos de la compañía el 85 % del acceso a Internet va dirigido a aplicaciones SaaS en la nube. "Los dispositivos son personales y si rápidamente no se logra un control en tiempo real de lo que está pasando, realmente la exposición a fugas de información y amenazas es muy grande".

Para Jorge López, de Fortinet, "la protección del *endpoint* debe ser similar a la que se tiene cuando se está conectado a la red de la oficina". Desde la compañía aconsejan protegerlo con software de protección avanzado del *endpoint*,

que debería disponer de tecnología EDR capaz de detectar *malware* basado en firmas. López también opina que para el acceso remoto "se debería disponer de terminadores de túneles que cifren las comunicaciones y dimensionados para soportar la carga de todos los usuarios trabajando al mismo tiempo".

La sanidad: un sector crítico

Durante el estado de alarma el sector sanitario está recibiendo el reconocimiento por parte de toda la sociedad. Algo totalmente merecido por el gran esfuerzo que están realizando, junto a otros sectores de primera necesidad, para salir de esta situación lo antes posible. Pero los *hackers* también han puesto el ojo en el sistema sanitario, así como en otros servicios esenciales como la alimentación, la logística, la seguridad, los transportes o las telecomunicaciones. Ante esta situación el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) ha mantenido el nivel cuatro de alerta, para ser capaz de responder a situaciones de alto riesgo.

En Bitdefender son conscientes de que el sector sanitario siempre ha sido uno de los más expuestos a las ciberamenazas y esta crisis ha incrementado este peligro. "El número de ciberataques contra hospitales ha aumentado significativamente en los últimos meses", ha comentado Juan Grau. Uno de los ataques más utilizado es el *ransomware* que "consigue bloquear el acceso a los ordenadores, logrando detener la actividad normal".

Jospe Albors, de Eset, coincide con Grau en que el sector sanitario está pasando por el momento más crítico. "No podemos permitir que un ciberataque deje fuera de juego infraestructuras tan críticas como los hospitales", ha recordado. Asimismo, ha hablado sobre los ataques dirigidos y otros que han sido lanzados de manera indiscriminada y que han llegado a afectar a algún centro sanitario.

Según datos de un informe de Kaspersky, las vulnerabilidades en las organizaciones sanitarias proceden de dos situaciones. Por un lado, la falta de atención a los riesgos de la digitalización. Y, por otro, la falta de conciencia del personal sobre la importancia de la ciberseguridad. Con estas debilidades "el peligro que supone que los ciberataques en instituciones sanitarias tengan éxito es enorme", ha indicado Alfonso Ramírez. La información que manejan estas organizaciones es crítica y, si el ataque triunfa, se pone en riesgo la resolución del diagnóstico del enfermo, su cuidado y la evolución.

La crisis del Covid-19 aumenta la concienciación sobre la importancia de la seguridad para las empresas y organizaciones

Continuando el hilo de la información confidencial y sensible de la que disponen los hospitales, Iván Mateos, de Sophos, ha corroborado la opinión de Ramírez sobre el altísimo coste que puede suponer el robo, la pérdida o la simple alteración de dichos datos. Mateos ha puesto como ejemplo "un ataque de denegación de servicio que deje caído un sistema de citas o consultas o un médico que no pueda acceder al historial de un paciente hace que sistemas de seguridad perimetral con capacidades de IPS o WAF sean esenciales".

Guillermo Fernández, de WatchGuard, recuerda que el *phishing* y el *ransomware* siguen liderando el ranking de ataques. "Se está realizando un importante esfuerzo de concienciación para ayudar a los centros hospitalarios a ver los riesgos a los que están expuestos". El Gobierno, explica, a través del CCN, del CNI y de otros organismos, está trabajando para la protección de estos entornos tan críticos.

Por su parte, Rafael Rosell, de S2 Grupo, también ha destacado el elevado riesgo de los centros sanitarios y los delicados datos que guardan. Sin embargo, el directivo cree que la protección ha sido correcta. "Al menos no se han tenido noticias de compromisos relevantes o problemas graves en los entornos sanitarios".

Por último, Juanjo Galán, de All4Sec, ha hablado sobre los riesgos a los que se enfrentan las infraestructuras esenciales que vienen "catalogados en función del nivel de amenaza que suponen para la prestación de servicios básicos". En la lista de ataques, aparecen en cabeza los que afectan a la disponibilidad de los sistemas o al robo de información. "También se están viendo un gran número de intentos de suplantación de la identidad o manipulación de la información que reciben los ciudadanos".