TELETRABAJANDO BAJO LA AMENAZA DEL COVID-19

La nueva situación, que obliga al teletrabajo, requiere una especial aproximación que la mayoría de los despachos y profesionales de la abogacía están cuidando y, de la que, a su vez, están informando para instruir a sus clientes y a la población en general sobre las precauciones y recomendaciones a seguir, en este caso, para salvaguardar, entre otras, la salud de los sistemas informáticos.

por desiré vidal

El 19 de marzo, el equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, alertaba del repunte de las campañas de malware que emplean temáticas relacionada con la pandemia del Coronavirus/COVID-19 para infectar a individuos y organizaciones de todo el mundo a través de un comunicado.

"En estos momentos -refiere dicho comunicado- existen registrados más de 24.000 dominios en Internet que contienen los términos: 'coronavirus', 'corona-virus', 'covid19' y 'covid-19'. De ellos, más de la mitad, 16.000, han sido creados en este mes de marzo (10.000 en la última semana). Algunos de ellos tienen fines legítimos y otros están dedicados a realizar campañas de spam, spear-phishing o como servidores de mando y control, C2. También se ha detectado que algunos troyanos como

Trickbot y *Emotet* han evolucionado sus TTP para evadir la detección, utilizando las noticias relacionadas con el coronavirus".

En este vírico contexto, ¿cómo se controla la seguridad de la información?
El coronavirus ha obligado al teletrabajo no sólo en los despachos de abogados, sino en multitud de empresas de todo tipo. "El coronavirus ha hecho que las empresas deban habilitar el teletrabajo y la movilidad en su grado más alto. Por supuesto garantizando el mayor grado de seguridad y eficacia. Es comparable a la situación de inutilización de un centro de trabajo y esto pondrá a prueba todos los planes de continuidad de negocio de todas las compañías; tenemos por delante un difícil examen que pasar y del que debemos aprender independientemente de los resultados", dice **Manuel Asenjo**, IT director de Eversheds Sutherland Nicea.
Jesús Yáñez, socio de Risk & Compliance, Ciberseguridad y Privacidad & Protección de Datos de Écija Law & Technology, nos cuenta que, "desde el lunes 16 de marzo de 2020, ÉCIJA dejó activado el plan de teletrabajo obligatorio para todos sus profesionales. No obstante, cabe recalcar que en la firma tenemos una política de libre teletrabajo, es decir, nuestros profesionales pueden teletrabajar todos los días que requieran. En este aspecto, somos uno de los primeros despachos que apostó por teletrabajo en la abogacía de los negocios en España, por tanto, nuestros sistemas de Ciberseguridad ya contemplan un sistema de mucho teletrabajo y no esperamos mayores riesgos de ciberataques fuera de lo habitual. Nuestro equipo de Ciberseguridad continua su actividad normal y no se conocen casos relacionados con el Covid-19. Otra iniciativa es que hemos puesto a disposición de los clientes un *helpdesk*; un equipo multidisciplinar compuesto por socios de diferentes prácticas, para responder a cualquier pregunta que nuestros clientes puedan tener. Por último, también hemos elaborado un decálogo de Ciberseguridad ante el teletrabajo que las empresas deben tener en cuenta".
Los ciberdelincuentes, conocedores de las vulnerabilidades que conlleva el teletrabajo, ya han empezado a sacar ventaja de esta situación, nos dice **Francisco Pérez Bes**, socio de derecho Digital de Ecix Group: "cuando trabajamos fuera de la oficina, somos todavía más vulnerables a ciberataques por lo que debemos extremar


JESÚS YÁÑEZ


FRANCISCO PÉREZ BES


MANUEL ASENJO

las precauciones acerca del tipo de información que enviamos, así como ser cautos a la hora de acceder a según qué ficheros o enlaces. Lo estamos viendo con la crisis del coronavirus, donde los

›››

JOAQUÍN MUÑOZ

criminales (en ocasiones terceros que buscan la desestabilización social, y que puede acarrear un verdadero problema de seguridad nacional), difunden noticias y páginas falsas con el fin de aprovecharse de la preocupación de los usuarios, y de las mayores posibilidades de que aquellos accedan a esos recursos comprometidos, con fines delictivos. Este tipo de prácticas les permite difundir rápidamente malware, como -entre otros- el temido ransomware *Emotet*. Ahí es donde se demuestra que la prevención y la concienciación son herramientas efectivas para garantizar la Ciberseguridad de empresas y personas".
Lo mejor es estar formados y prevenidos. **Joaquín Muñoz**, responsable de IT & IP Law de Ontier

> EXISTEN MUCHAS MEDIDAS A IMPLEMENTAR EN FUNCIÓN DE LA OPERATIVA DE CADA EMPRESA, PERO LO PRIMERO ES UTILIZAR SOLAMENTE AQUELLOS EQUIPOS QUE LA EMPRESA PONE A DISPOSICIÓN DE LOS TRABAJADORES Y QUE CUENTAN CON LOS PROGRAMAS DE SEGURIDAD
>
> JOAQUÍN MUÑOZ DE ONTIER

lo explica así: "en estos días en los que la mayoría de profesionales, también abogados, estamos trabajando en remoto, hay una serie de cuestiones que podemos recordar para mantener un acceso seguro a los servidores y un tratamiento seguro de la información. Existen muchas medidas a implementar en función de la operativa de cada empresa, pero lo primero es utilizar solamente aquellos equipos que la empresa pone a disposición de los trabajadores y que cuentan con los programas de seguridad. En este sentido, es recomendable que toda la actividad laboral se lleve a cabo en un ámbito controlado por el despacho, siendo la forma más sencilla habilitar un acceso remoto y directo contra el servidor, evitando conservar documentos en local. Si es necesario que el trabajador acceda desde un dispositivo particular, será recomendable determinar unas credenciales únicas que le identifiquen en los accesos a la documentación corporativa y crear accesos seguros a la misma, a través de VPN, por ejemplo. Por otro lado, la asignación de roles y limitación de accesos en función de esos roles cobra mayor relevancia en situaciones de acceso remoto y siempre es importante poder conservar los logs de acceso para monitorizar la actividad llevada a cabo. Lo anterior, y sin perjuicio de otras muchas medidas de seguridad que se pueden implementar, puede no funcionar si la empresa no invierte tiempo y recursos en crear una cultura en la que todos los empleados sean conscientes de su responsabilidad y están comprometidos para cumplir con las obligaciones que la empresa impone en esta materia".
Pero los peligros no son exclusivos de la situación provocada por el COVID-19. Francisco Pérez Bes explica que "el abogado, por la propia naturaleza de su profesión, debe desplazarse fuera del despacho en numerosas ocasiones, lo que supone que la tipología de riesgos que deben ser atendidos, es diferente. Así, los despachos deben concienciar a sus abogados sobre cómo actuar durante un viaje de negocios, durante el cual se va a conocer una gran cantidad de información sobre operaciones y contratos, que pueden tener un gran valor comercial. Y es responsabilidad de este profesional proteger el secreto y la confidencialidad de tales extremos. No proteger las pantallas de nuestros terminales cuando trabajamos en público, revelar información en conversaciones telefónicas, utilizar redes wifi públicas (que pueden haber sido vulneradas), o perder un simple móvil o USB sin la información no va cifrada y protegida por contraseña, son negligencias que, además de poner en peligro la

NOEMÍ BRITO

confianza del cliente, están sancionadas legal y deontológicamente. También el teletrabajo es habitual en esta profesión. Por ello, los despachos deben disponer de accesos a sus sistemas desde el exterior, bien protegidos (mediante contraseñas robustas) y cifrados (mediante VPN, preferiblemente). Y concienciar a dichos empleados que adopten cautelas acerca de la información que incluyen en sus mensa cuando trabajan fuera del despacho, ya que existen más probabilidades de sufrir algún tipo de incidente de seguridad (por ejemplo, una interceptación de comunicaciones). No necesariamente porque un ciberdelincuente logre acceder al canal de comunicación, sino porque el profesional tiende a bajar la guardia y a utilizar terminales que pueden haber sido vulnerados en algún momento (por ejemplo, tener instalado algún tipo de malware), o que tienen instaladas aplicaciones inseguras. En tal caso, un tercero podría acceder a información sensible antes de que se produzca su envío a través de los sistemas del despacho, sin ser detectado".

Además de incidir en todo lo expuesto, **Noemí Brito**, socia responsable del Área de Tecnología de Ceca Magán advierte que: "es importante considerar las recientes recomendaciones dispuestas al efecto, tanto por el Instituto Nacional de Ciberseguridad (INCIBE) como por el Centro Criptológico Nacional (CCN), y que pueden resumirse en la necesidad de adoptar e implantar una política coherente y razonable de acceso remoto seguro. Las soluciones van, desde la implementación de una solución basada en la nube con la suficiente seguridad, a un sistema basado en sistemas locales, on-premise, en el que se extienden los límites de la organización más allá de sus instalaciones. El objetivo principal de esta política sería, en todo caso, prever las medidas de seguridad pertinentes para este tipo de accesos, así como la articulación de sistemas seguros de videoconferencias, conexiones con proveedores y clientes. Sin perjuicio de lo anterior, que sería lo deseable, en todo caso, se deberán asegurar ciertos parámetros en situaciones de teletrabajo (con apoyo de la empresa si fuera factible o posible), en particular, si el equipo, red o dispositivo es aportado por el trabajador".

Conocedores de los riesgos añadidos que supone la situación generalizada de teletrabajo, desde el equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, han elaborado un Informe de Buenas Prácticas: *CCN-CERT BP/18* Recomendaciones de Seguridad para situaciones de teletrabajo y refuerzo en vigilancia y las medidas de seguridad para acceso remoto.

Recomendaciones de seguridad para teletrabajar vía NOEMÍ BRITO

- Asegurarse de la seguridad de sus credenciales, en particular, utilizar claves o contraseñas robustas y, si fuera posible, activar el doble factor de autenticación.
- Mantener los sistemas operativos y aplicaciones actualizados (asegurando la mayor seguridad posible conforme a las correspondientes actualizaciones).
- Si fuera posible, usar dispositivos y soportes que permitan el cifrado o encriptación de la información, de forma que, en caso de brecha de información personal, los datos resulten ininteligibles para terceros minimizando los riesgos asociados a una posible falta de confidencialidad.
- Realizar copias de seguridad periódicas utilizando sistemas que ofrezcan garantías suficientes en atención a las políticas de seguridad corporativas.
- Evitar el uso de aplicaciones de escritorio remoto que pueden crear puertas traseras y alentar el uso de redes privadas virtuales (VPN) seguras.
- Asegurarse de que la configuración del Wifi es correcta y segura. Conservación y borrado/supresión segura de la información en consonancia con las políticas de seguridad corporativas.