CIBERSEGURIDAD EN TIEMPOS DEL COVID-19: CLAVES PARA ADOPTAR (Y PROTEGER) UNA PLANTILLA DE TELETRABAJADORES

11 marzo 2020 | Michael Sentonas | Punto de vista ejecutivo

La declaración del día de hoy de pandemia mundial por parte de la Organización Mundial de la Salud pone de relieve lo que todos venimos observando: la enfermedad bautizada como COVID-19, provocada por una variante del coronavirus, va a provocar un nivel de conmoción socioeconómica sin precedentes en tiempos modernos. Nuestros clientes ya nos han expresado su preocupación ante los importantes desafíos repentinos que supone dotarse rápidamente de políticas corporativas que permitan a los empleados desalojar las oficinas y los campus corporativos, y empezar a trabajar desde casa. Garantizar la seguridad ante este éxodo de las oficinas a nivel mundial presenta riesgos importantes para la mayoría de las empresas.

RETOS DE LA ADOPCIÓN RÁPIDA DE UNA PLANTILLA DE TELETRABAJADORES

Según un informe del International Workplace Group, el 50 % de los empleados en todo el mundo trabajan fuera de sus oficinas centrales principales, al menos 2,5 días a la semana. Sin embargo, el COVID-19 empuja a más empresas (incluso a todas) a adoptar un modelo de teletrabajo de forma inmediata. Al margen de la presión que esta salida masiva de las oficinas ejerce sobre los equipos de TI, las arquitecturas de red e incluso los proveedores de equipos, existen desafíos de seguridad reales que las empresas deben tener en cuenta.

Seis factores que pueden ayudar a garantizar la ciberseguridad de los teletrabajadores:

- **Asegúrese de que cuenta con una política de ciberseguridad actualizada que incluya el trabajo a distancia.** Es posible que ya disponga de políticas de seguridad robustas, pero es importante revisarlas y asegurarse de que son adecuadas cuando su empresa realice la transición hacia un modelo con más empleados trabajando desde casa que en la oficina. Deben incluir la administración del acceso para el trabajo a distancia, el uso de dispositivos personales, así como consideraciones actualizadas acerca de la privacidad de los datos, para el acceso de los empleados a documentos y otra información. También es importante considerar el aumento de uso de dispositivos de las TI en la sombra y la tecnología de nube.
- **Planifique el uso de dispositivos propiedad de los empleados (BYOD) que se conectan a su empresa.** Los empleados que trabajen desde casa pueden utilizar dispositivos personales para llevar a cabo sus funciones, sobre todo si tienen acceso a un dispositivo suministrado por la empresa debido a la posible escasez de suministros. Los dispositivos personales deberán disponer del mismo nivel de seguridad que los de la empresa. Además, deberá considerar las implicaciones en cuanto a privacidad, de los dispositivos de los empleados que se conectan a una red empresarial.
- **Es posible que se acceda a datos confidenciales a través de redes Wi-Fi no seguras.** Los empleados que trabajen desde casa podrían acceder a datos empresariales sensibles a través de redes Wi-Fi domésticas que no dispongan de los mismos controles de seguridad (como firewalls) que las oficinas tradicionales. Se realizarán más conexiones desde ubicaciones remotas, lo que obligará a hacer especial hincapié en la privacidad de los datos, así como reforzar la caza de intrusiones desde un número mayor de puntos de entrada.

- **La visibilidad y la higiene de ciberseguridad serán fundamentales.** No es raro que los dispositivos personales tengan una higiene de ciberseguridad deficiente. El teletrabajo puede provocar que una empresa pierda visibilidad de los dispositivos y de su configuración, corrección e incluso protección.
- **La formación continua es crucial, en un momento en el que se intensifican los timos relacionados con el coronavirus.** La Organización Mundial de la Salud (OMS) y la Comisión Federal de Comercio de EE. UU. (FTC) ya han advertido sobre campañas de timos y ataques de phishing con temas relacionados con el coronavirus. La comunicación y la formación continua de los usuarios son extremadamente importantes, y es recomendable garantizar que los trabajadores a distancia puedan ponerse en contacto rápidamente con el departamento de TI para recibir asistencia. Las empresas también deberían plantearse la implementación de medidas de seguridad del correo electrónico más estrictas.
- **Es necesario que la plantilla remota sea capaz de poner en práctica los planes de gestión de crisis y respuesta a incidentes.** Un ciberincidente que se produce cuando una empresa ya está operando fuera de las condiciones normales tiene mayores posibilidades de descontrolarse. Con las herramientas de colaboración remota —como los puentes de conferencia fuera de banda, las plataformas de mensajería y las aplicaciones de productividad—, un equipo diseminado puede crear una "sala de operaciones virtual" desde la que gestionar las acciones de respuesta. Si los planes de su empresa dependen del acceso físico o del desplazamiento de técnicos para tareas específicas (por ejemplo, la recreación de imágenes o la sustitución de máquinas comprometidas), puede que sea prudente explorar métodos alternativos o recursos locales.

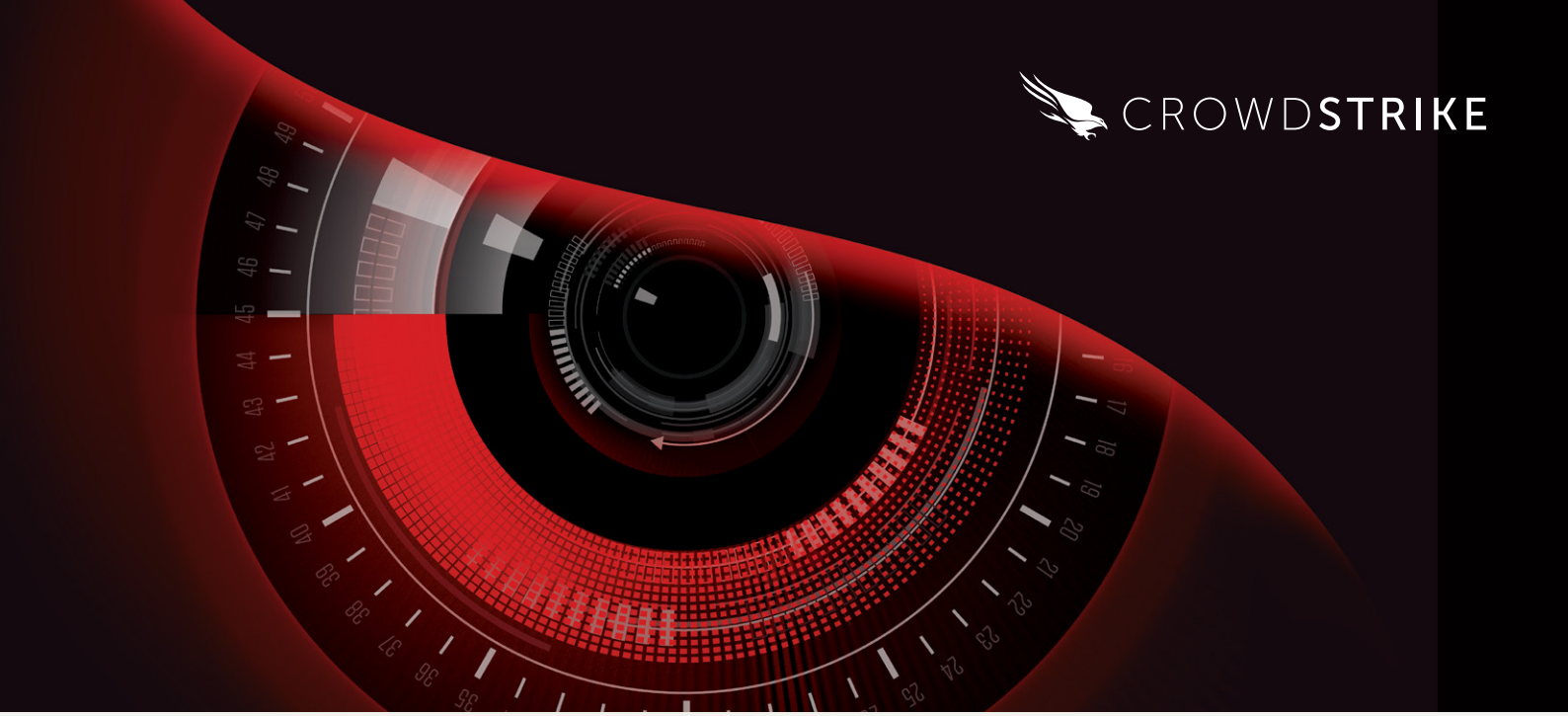
CÓMO GARANTIZAR LA SEGURIDAD DE SU PLANTILLA REMOTA

CrowdStrike se encuentra en una posición privilegiada para proporcionar asistencia a empresas que se enfrenten al cambio rápido al teletrabajo por dos razones: una es que nuestra plataforma a través de la nube y nuestra arquitectura de agente ligero son ideales para la asistencia y, especialmente, la protección de los teletrabajadores; la segunda es que nosotros aplicamos nuestras propias recetas, ya que nosotros mismos nos hemos dotado de una plantilla remota amplia y muy dispersa, por lo que contamos con un profundo conocimiento institucional sobre cómo adoptar este modelo de forma segura y eficaz.

A continuación incluimos varias funciones que le ofrece la plataforma CrowdStrike Falcon®, nativa de la nube, para facilitar una rápida transición y garantizar la seguridad cuando su plantilla pase a trabajar en casa:

Aproveche la escalabilidad y la rentabilidad de la nube. La arquitectura diseñada completamente para la nube se adapta a las exigencias de los clientes y proporciona un enorme poder de almacenamiento y computación para hacer posible la protección en tiempo real, independientemente del lugar desde el que se conecten los empleados. Trabajar con una arquitectura de seguridad de nube garantiza el aprovisionamiento de recursos adicionales cuando sea necesario. Y en un momento en que se dispone a adoptar el teletrabajo, no hay necesidad de planificar, preparar y adquirir hardware ni software para mantenerse al día.

Consiga el máximo nivel de seguridad con independencia de dónde estén ubicados los empleados. Disponer de una arquitectura de seguridad completamente ofrecida a través de la nube garantiza su capacidad para proteger cualquier carga de trabajo, en cualquier lugar, incluidas las que estén fuera del firewall, incluso si están offline, y además proporciona una funcionalidad de seguridad en tiempo real con el máximo nivel de eficacia, junto con información sobre el estado de cumplimiento. Es fundamental poder cazar amenazas en todos los dispositivos, especialmente en aquellos conectados a la red. Para conseguir esto fácilmente —con datos accesibles inmediatamente y desde cualquier lugar— es imprescindible contar con una solución nativa de la nube.



Confíe en una arquitectura de seguridad sencilla que ofrece visibilidad total. Saber quién y qué está conectado a su red es esencial para la administración proactiva de la seguridad. Resulta fundamental disponer de visibilidad total de cada uno de los dispositivos que se conectan a la red, con independencia del lugar desde el que se conecten. Gracias al agente único y ligero de CrowdStrike® Falcon, no hay necesidad de reiniciar para instalar; hay un impacto mínimo en el rendimiento en tiempo de ejecución; no se producen "oleadas de análisis" ni actualizaciones de firmas invasivas que afecten a la experiencia del usuario final; y se puede proteger a los usuarios en cuestión de segundos. La supervisión y descubrimiento completos y permanentes de las cargas de trabajo de la plataforma Falcon ofrecen a los equipos de seguridad visibilidad total de cada dispositivo: esto incluye los dispositivos in situ, los dispositivos domésticos y de oficina a distancia, y las cargas de trabajo de la nube. Esta visibilidad también extiende la protección a los contenedores y dispositivos móviles.

Garantice la seguridad sin preocupaciones, con protección de endpoints como servicio. Con CrowdStrike Falcon Complete™, los clientes pueden confiar la implementación, administración y respuesta a incidentes de su seguridad de endpoints al equipo de expertos en seguridad acreditados de CrowdStrike. El resultado es un enfoque de seguridad optimizado de manera instantánea sin la carga, los gastos generales ni el coste de administrar un programa de seguridad de endpoints global, liberando recursos internos para trabajar en otros proyectos. Falcon Complete es una solución de protección de endpoints completamente gestionada que proporciona las personas, los procesos y la tecnología necesarios para gestionar todos los aspectos de la seguridad de endpoints, desde la incorporación y la configuración hasta el mantenimiento, la gestión de incidentes y la corrección, ya sea una carga de trabajo in situ o un trabajador a distancia.

CONCLUSIÓN

Es probable que la crisis del COVID-19 esté con nosotros durante algún tiempo. Las empresas y sus empleados se verán obligados a tomar decisiones complicadas rápidamente, y habilitar una plantilla de teletrabajadores es una de ellas. Poner en marcha este modelo rápidamente conlleva riesgos, pero la seguridad de sus redes, dispositivos y datos no debería estar entre ellos.

Llame a su representante de CrowdStrike para obtener información sobre los programas especiales para clientes de CrowdStrike, que se enfrentan a aumentos masivos del número de teletrabajadores. CrowdStrike se ha comprometido a eliminar los obstáculos para tomar decisiones y garantizar que todos los usuarios tengan acceso a la tecnología y los profesionales que necesitan para trabajar con seguridad dondequiera que se encuentren.

NO SE PIERDA UN IMPORTANTE WEBCAST

Únase a los expertos de CrowdStrike el miércoles 18 de marzo para analizar las claves para adoptar y proteger una plantilla de teletrabajadores. **Regístrese hoy.**

Recursos adicionales

- Más información sobre la **plataforma CrowdStrike Falcon.**
- Regístrese en este webcast: **Ciberseguridad en tiempos del COVID-19: Claves para adoptar (y proteger) una plantilla de teletrabajadores.**
- Visite la **página web de Falcon Complete** para obtener más información sobre la protección de endpoints completamente gestionada.
- **Consiga una prueba gratuita totalmente funcional de CrowdStrike Falcon Prevent™** y descubra cómo actúa un verdadero antivirus de nueva generación contra las amenazas más sofisticadas de la actualidad.