NOTA DE PRENSA
15 / 04 / 2020

Trucos de ciberseguridad y mejores prácticas para teletrabajar

> Artículo escrito por Joseph Carson, Chief Security Scientist (CSS) & Advisory CISO en Thycotic

Dadas las inusuales y recientes circunstancias en las que nos encontramos, muchos empleados a nivel mundial están asistiendo a una situación nueva para ellos en la que tienen que teletrabajar.

He estado trabajando en remoto durante 15 años, y me gustaría ahora compartir con vosotros algunas de mis experiencias, así como aspectos importantes en ciberseguridad a los que me he enfrentado.

Tengo suerte de trabajar en Thycotic, una compañía global con trabajadores en remoto. La cultura de la compañía es que no importa en qué parte del mundo trabajemos, nuestra fuerza es nuestra gente, la colaboración entre nosotros y el trabajo en equipo. Nuestra tecnología ayuda a nuestros empleados, nuestros socios y nuestros clientes a disponer de un acceso a sus sistemas críticos y sus aplicaciones de manera segura independientemente de dónde se encuentren trabajando en ese momento. Nosotros permitimos la continuidad del negocio y de su crecimiento incluso en situaciones de emergencia, como la que vivimos actualmente.

Mi experiencia es haber estado trabajando desde los sitios más inusuales, como una isla remota. Una vez hace años, incluso estuve en cuarentena por una gripe porcina. Experiencia que me permite ahora compartir consejos en materia de seguridad y productividad para las personas y los negocios realizados en remoto.

Comenzaré con consejos para personas que estén trabajando remotamente, después proporcionaré recursos para negocios que necesiten controlar los riesgos de ciberseguridad mientras los empleados trabajan en remoto.

¿Cómo y a dónde me estoy conectando?

La primera pregunta que debemos hacernos es ¿cómo y a dónde me estoy conectando? Si al acceso es a una internet pública, o bien accedo a la conexión a internet de mi casa, a la conexión de internet de un hotel o, incluso, acceso a través de mi móvil, esto significa que la conexión de acceso a nuestro trabajo remoto es una cuestión crítica.

¿Cómo se mantendrá conectado con sus compañeros, sus socios y sus clientes? Actualmente, en la mayoría de los hogares, puede haber acceso ilimitado a internet y con una velocidad extremadamente rápida, algo que tuve la suerte de tener en Estonia, un país que priorizó la digitalización hace muchos años. Allí, se puede disfrutar de internet de alta velocidad en casi cualquier lugar, incluso en el bosque.

Conocer las limitaciones de su ancho de banda es importante. Es posible que desee deshabilitar las aplicaciones que demandan mucho ancho de banda. Habitualmente, internet funciona con rapidez, pero cuando muchos quieren conectarse en remoto a la vez, surge una tensión en las capacidades del ISP. También es decisivo saber cuándo conectarse con el internet del hogar y cuándo hacerlo con el internet del móvil. Si tiene una llamada o un webinar importante, puede que prefiera conectarse por el internet del teléfono porque durante las horas de mayor actividad pueda ser más rápido y seguro. Mientras que si viaja fuera de su país de origen, puede adquirir una tarjeta SIM de internet móvil para reducir gastos excesivos de internet.

Consejos para trabajar seguro usando acceso a internet

1. Apague las aplicaciones que exigen mayor ancho de banda cuando no las necesite
2. Use siempre un acceso VPN corporativo cuando sea necesario – permanecer seguro es vital
3. Utilice una red de internet doméstica separada para trabajar para aislar los dispositivos personales
4. Asegúrese de que la contraseña del router de internet de casa es larga y segura (y use un gestor de contraseñas)
5. Conozca las limitaciones de su ancho de banda
6. Utilice un monitor de ancho de banda de internet
7. Elija bien cuando conectarse al internet de casa y cuando al internet móvil

Recuerde que cuando se teletrabaja, las necesidades de comunicación con compañeros, proveedores, socios y clientes son las mismas que cuando lo hace desde su oficina, es decir, debe contar con un buen servicio de micrófono y sonido (ya sea por webcam o cualquier otro método). Para muchos trabajadores, teletrabajar incrementa el número de telellamadas, vídeo llamadas, webinars y presentaciones en remoto. Todo ello implica que debemos asegurarnos de que no hay ecos

inesperados, molestos ruidos de fondo o, simplemente, una mala calidad de audio.

Los cascos también previenen de que otros escuchen nuestras conversaciones. Algo que siempre nos debe preocupar cuando mantenemos una comunicación con información sensible; tenemos que asegurarnos de que contamos con la necesaria privacidad.

Trazar un plan de prioridades

Es importante trazar un plan de prioridades a la hora de teletrabajar, porque cuando no estamos trabajando en el lugar habitual, es muy fácil caer en el desorden. Así pues, debemos hacernos a comienzo de la semana una planificación de tareas, repartirlas durante los días de la semana, márcalas un grado de prioridad determinado, fijar las que podemos realizar nosotros solos y aquellas en las que necesitamos la colaboración de un compañero.

Y no olvidar que cuando teletrabajamos muchos, puede que no todos lo hagamos en el mismo horario laboral debido a nuestras diferentes horas locales. Utilizar Outlook nos permitirá contar un calendario donde planificar las reuniones de acuerdo con los horarios de los distintos empleados. Cree una rutina de trabajo y márquese un horario diario que deberá seguir fielmente.

Es clave entender la importancia de comunicarse frecuentemente y de saber utilizar las herramientas disponibles. No dude coger el teléfono y hablar con sus compañeros o clientes cuando otros métodos no funcionen. Pensemos que el teléfono, las herramientas de audio y vídeo, los webinars, los podcasts, las herramientas de colaboración, los meetings online y los diferentes sistemas de mensaje nos ayudan a hacer más fácil el teletrabajo. Y siempre hay que contar con una alternativa, la tecnología puede fallar.

La seguridad de la información no debe ser opcional

En el mundo conectado como el nuestro, con empleados teletrabajando, junto con proveedores externos socios y empleados conectados en remoto, la seguridad de la información debe estar entre nuestras principales prioridades. La mayoría de las organizaciones que tienen empleados teletrabajando utilizan proveedores externos para administrar sus sistemas, aplicaciones e infraestructura, o bien subcontratan algunos servicios, como soporte al cliente o desarrollo de productos. Algunas compañías podrían incluso estar utilizando Seguridad como Servicio (SECaaS) o Proveedores de Servicios de Seguridad Administrada (MSSP) para ayudarse en todo o en parte de la seguridad de sus Tecnologías de la Información.

En cualquiera de los escenarios anteriores, la prioridad es adoptar una estrategia de seguridad que

reduzca el riesgo de ciberataques al tiempo que se garantiza que se pueden realizar tareas enfocadas al negocio de modo productivo. Desde Thycotic, nuestra misión en ciberseguridad es entender cómo los empleados hacen negocio de manera exitosa utilizando nuestras herramientas de ciberseguridad enfocadas a reducir el riesgo de ciberataques en la medida de lo posible. La seguridad nunca debe ser compleja y debe ser fácil de manejar por los empleados.

La seguridad aplicada al teletrabajo abarca:

Un espacio de trabajo seguro: ¿Cómo accede a las aplicaciones de negocio de su compañía? ¿Utilizando su dispositivo personal (BYOD), con un portátil de la compañía o un tercer dispositivo? Dependiendo de cada caso, la seguridad de su espacio de trabajo puede variar sensiblemente. Debería aplicarse una política de Zero Trust (Confianza Cero). También debería coexistir un modelo de seguridad basado en Zero Trust con una Gestión de Acceso Privilegiados (PAM).

Comunicaciones seguras: Cuando los trabajadores acceden en remoto a las aplicaciones o sistemas, es importante que la comunicación entre dispositivos sea segura, ya sea mediante protocolos que cifran los datos como HTTPS o mediante una VPN corporativa.

Gestión de acceso e identidad: Para los trabajadores conectados en remoto, tener el acceso correcto a las aplicaciones correctas es fundamental. Una solución sólida de gestión de acceso e identidad ayudará a automatizar la capacidad de cambiar o aprovisionar a los teletrabajadores a los métodos y tecnologías de acceso adecuados.

Principio de Privilegio Mínimo: Dar el privilegio mínimo significa otorgar solo los permisos mínimos requeridos por un usuario final, aplicación, servicio, tarea o sistema para realizar los trabajos que se les han asignado. El objetivo de privilegio mínimo es evitar el "acceso con privilegios excesivos" por parte de usuarios, aplicaciones o servicios para ayudar a reducir el riesgo de explotación sin afectar a la productividad o involucrar a las TI.

La administración de acceso privilegiado asegura el acceso a los teletrabajadores

Muchas compañías tienen un escenario híbrido en el que algunas aplicaciones comerciales se encuentran en las instalaciones de la oficina o en el centro de datos de la compañía, mientras mantienen otras aplicaciones en una nube privada o pública. Sea cual sea el modelo seguido por la empresa, es esencial que, sin importar dónde se encuentre el empleado, éste pueda acceder de forma segura a las aplicaciones comerciales que necesite.

La administración de acceso privilegiado (PAM) no se trata solo de asegurar cuentas privilegiadas en

un pool empresarial cifrado. Se trata del uso seguro de cuentas privilegiadas y del acceso seguro a datos y recursos privilegiados desde cualquier ubicación, incluso para los empleados que teletrabajan.

A medida que más empresas adoptan soluciones PAM, se convierten en un importante habilitador de un enfoque de seguridad integral que impulsa la evolución de PAM. Esto incluye integraciones entre soluciones de seguridad, como conexiones a soluciones de administración de identidad, herramientas de administración de sistemas, autenticación multifactor, SIEM, soluciones de administración remota y DevOps.

Las soluciones PAM permiten a los trabajadores remotos acceder a las aplicaciones, ya sea en la nube o en las instalaciones, todo mientras se aplican las mejores prácticas de seguridad.

Es común que las empresas permitan el acceso a las soluciones PAM a través de Internet y combinen la autenticación con el inicio de sesión único y una autenticación multifactor robusta (MFA).

Asegúrese de que sus trabajadores remotos puedan mantenerse productivos y mantener un acceso seguro, ya sea que estén accediendo a sistemas remotos, aplicaciones críticas, infraestructura o datos mediante el uso de una solución PAM combinada con MFA.

Contacto de prensa:

JAVIER MODUBAR ALVAREZ
info@ingecom.net
944395678
http://www.ingecom.net