Consejos para un teletrabajo seguro

Por Iván Mateos, Sales Engineer de Sophos Iberia

La ciberseguridad, una prioridad

La movilidad laboral ha pasado estos últimos días de ser una opción de flexibilidad, o un proyecto futuro, a ser lo habitual en muchas empresas tecnológicas y no tecnológicas. Debido a los últimos acontecimientos y a la urgencia del momento, muchas compañías han comenzado a desplegar todo tipo de opciones para facilitar a los empleados la continuidad del negocio.

Si bien es cierto que el teletrabajo se está mostrando como una herramienta eficaz de cara mantener la productividad, es muy importante no tomar decisiones precipitadas y, sobre todo, tener en cuenta que la ciberseguridad sigue siendo prioritaria a la hora de diseñar las telecomunicaciones si no queremos que el remedio sea peor que la enfermedad.

Publicar escritorios remotos no es lo recomendable y tiene una fácil solución: El uso de conexiones seguras mediante VPN

La mayoría de los firewalls del mercado ofrecen la posibilidad de configurar estos accesos, de forma que nuestros usuarios puedan conectar de forma segura desde sus equipos en movilidad hacia los recursos de la compañía. Estas conexiones de acceso remoto, ya sean mediante el protocolo SSL o Ipsec, permiten que la comunicación realizada por los usuarios se realice a través de un canal seguro de forma que no pongan en riesgo los recursos de la organización. Además, es posible aumentar la seguridad de estos accesos configurando un sistema de validación de doble factor, esto significaría que, aunque el usuario perdiera su contraseña, aun sería necesario un segundo paso (normalmente la generación de un código de acceso temporal) para completar la validación.

Crear una conexión segura con XG Firewall

El uso de una Red Privada Virtual (VPN) garantiza que todos los datos transferidos entre el usuario y la red de la oficina estén cifrados y protegidos.

SOPHOS

Sophos, con la solución XG Firewall, no solo ofrece esta posibilidad, sino que lo hace sin ningún tipo de coste adicional ni limitación más allá del número de conexiones soportadas por el equipo. Con Sophos XG contamos tanto con un cliente VPN SSL como con un cliente VPN IPSEC (Sophos Connect) incluidos en el propio firewall de forma totalmente gratuita los cuales ofrecen diferentes formas de despliegue incluyendo la autenticación de doble factor u OTP (One Time Password).

8 buenas prácticas para teletrabajar seguros

Pero no solo se trata de securizar las comunicaciones, se trata también de convertir el entorno de teletrabajo en un entorno lo más privado y seguro posible. Para ello, debemos tener en cuenta que tanto si se va a utilizar un ordenador o smartphone cedido por la empresa como si van a utilizar su propio dispositivo personal, en todos los casos los usuarios deben seguir la siguiente lista de buenas prácticas en entornos de teletrabajo:

- **Cambiar la contraseña de la clave WIFI y del router**. Además de desactivar la opción de WPS. Esto ya era recomendable, pero ahora lo es más. Ya no estamos en casa si no que nos hemos llevado la oficina a casa. La conexión que utilizamos para manejar información confidencial debe ser lo más segura posible.
- **Utilizar equipos y aplicativos actualizados**. Un equipo o una aplicación con parches de seguridad no aplicados es un posible punto de entrada para un ciberdelincuente. Debemos mantener al día todo el software que utilicemos con el fin de maximizar la seguridad.
- **Utilizar contraseñas seguras y proteger nuestros dispositivos**. De todo y de todos, ahora los dispositivos que utilizamos forman parte de la empresa, debemos activar el bloqueo automático de los dispositivos, no compartir la contraseña con el resto de los miembros de la familia y bloquear el dispositivo siempre que no se use.
- **Cifrar los dispositivos**. Siguiendo el consejo anterior, nuestro dispositivo ahora contiene información sensible. No queremos que si nos lo roban o lo extraviamos se pierda información o que esta se convierta en algo al alcance de cualquiera. Windows, MAC, Android o IOS incluyen esta opción de forma nativa.
- **Cuidado con los USB**. Muchos de estos dispositivos contienen malware que puede ponernos en un apuro. Es importante utilizar solamente los dispositivos que sepamos que son confiables.
- **Realiza copias de seguridad**. Ante desastres o infecciones de ransomware es importante tener un plan B. En muchas ocasiones tener la información importante guardada en un disco duro puede salvar todo el trabajo de mucho tiempo.
- **No utilizar equipos sin protección antimalware**. Pide a tu empresa que te recomiende una solución antimalware de nueva generación para tu dispositivo personal si lo vas a utilizar para el teletrabajo.
- **Vigilar el correo electrónico y huir del phishing**. También en tu correo personal.

Sophos facilita la vida a los teletrabajadores

Desde el punto de vista de los administradores, también hay muchas cosas que se pueden hacer no solo para mejorar la seguridad de los empleados sino para hacerles la vida más fácil (y sobre todo no depositar en ellos toda la responsabilidad) con las soluciones de Sophos, incluyendo opciones gratuitas.

- **Proteger los dispositivos**. La solución InterceptX cuenta con la mayor calificación en los principales test de terceros en cuanto a la protección Anti-Hacking, Antiransomware y Anti-Exploit que ofrece a los puestos finales. Además, Sophos, en su versión Home, ofrece también a los usuarios domésticos la misma protección, incluyendo una opción gratuita hasta 3 equipos.
- **Gestionar el cifrado**. Si los dispositivos tienen que estar cifrados es posible que los usuarios olviden su clave de acceso. Para facilitar la recuperación de estas claves, Sophos integra en el mismo agente de protección del puesto, la gestión de dichas claves, así como la facilidad de inventariar los dispositivos cifrados o crear documentos confidenciales.
- **Conectividad segura**. Publicar Escritorios Remotos (RDP) no es una buena opción. Con Sophos XG contaremos con toda la flexibilidad para crear accesos VPN de forma sencilla, y haciendo que también lo sea para el usuario.
- **Proteger el correo**. Desde el punto de vista de la empresa y desde el punto del usuario. Tanto con Sophos Email como con la herramienta de concienciación Phish Threat, no solo limpiaremos el correo recibido, sino que enseñaremos a nuestros usuarios a identificar amenazas incluso en su correo personal.
- **Proteger la navegación**. Los usuarios ya no están detrás del firewall de la empresa, pero no por ello vamos a descuidar la protección mientras navegan. El agente de protección de puesto de Sophos permite crear reglas de filtrado web, de forma que los usuarios puedan seguir navegando de forma segura incluso en sus casas.
- **Proteger los dispositivos móviles**. Cualquier dispositivo móvil puede suponer una herramienta de trabajo y un riesgo a su vez. Intercept X para Android e IOS cuenta tanto con su versión gratuita como con la versión gestionada Sophos Mobile con la que podremos proteger, geolocalizar, borrar, inventariar o instalar aplicaciones de forma remota entre otras muchas opciones.

La Seguridad Sincronizada de Sophos, la mejor solución

Sophos permite que sus soluciones hablen entre sí y esto es una herramienta muy útil para un administrador. Con la seguridad sincronizada también podemos evaluar el estado de salud de los equipos que conectan por VPN antes de que alcancen nuestros servicios internos o incluso garantizar que ningún equipo que no cuente con Sophos Endpoint instalado pueda acceder a la organización, es decir, aunque un usuario instale el cliente VPN en su PC personal no podrá acceder a los recursos corporativos detrás del firewall si así lo queremos.

Sophos obtiene la certificación LINCE

Sophos ha obtenido la certificación LINCE del Centro Criptológico Nacional (CCN) para la inclusión de Central Intercept X Advanced con EDR en el Catálogo de Productos STIC acreditando su uso por parte de las Administraciones Públicas que deben cumplir con el Esquema Nacional de Seguridad.

La inclusión en este catálogo permite a las Administraciones Públicas hacer uso de la solución de Sophos para cumplir con el Esquema Nacional de Seguridad. Más información aquí.

Sophos XG recibe las certificaciones Common Criterial EAL4+ certification e ICSA Labs

Consolidando dos de las certificaciones más importantes del séctor, Sophos garantiza a sus clientes, especialmente a aquellos del sector publico, que los requisitos y estandares de seguridad se implementan adecuadamente.

Más información aquí.

Durante la duración de la pandemia Sophos ofrece a Administraciones Públicas su solución de protección NextGen Endpoint: Intercept X y su solución XG Firewall (virtual) gratis por 3 meses.

Si quiere más información sobre cómo Sophos puede ayudarle, llámenos al teléfono 913 756 756 o envíe su petición por correo a Inigo.Stuyck@sophos.com

CYBERSECURITY EVOLVED.