

Cómo asegurar una fuerza de trabajo remota



GFI™

Aurea SMB Solutions

Содержание

	Introducción	3
---	--------------	---

Temas de Seguridad que los Administradores de Tecnología de la Información necesitan considerar Cuando se Trata de Trabajo Remoto

	Comunicación en línea incrementada substancialmente	4
---	---	---

	Escaneo y parcheado de dispositivos remotos	5
---	---	---

	Seguridad de la Red de Trabajo en Casa	6
---	--	---

	Respalde toda la información con copias de seguridad encriptada	10
---	---	----

	¿Qué tan difícil es asegurar una fuerza de trabajo remota?	11
---	--	----

	Proteja su negocio con Unlimited Network Security	12
---	---	----

Introducción

Su pequeño negocio ha cambiado en formas que usted jamás esperó. Aún si usted no está operando en ubicaciones con orden de quedarse en casa, usted desea mantener a sus empleados en un ambiente seguro. Como consecuencia, su negocio puede haber cambiado parcial o totalmente a estar en línea.

Esto complica la necesidad de mantener todos los archivos y comunicaciones seguras. Las máquinas que manejan su negocio podrían no estar solamente localizadas en sus oficinas.

¿A dónde va desde aquí? Su presupuesto está estirado muy delgadamente. No cuenta con expertos en Tecnología de la Información remota en su equipo. Su plan de negocios posiblemente no está preparado para mantener las cosas seguras en caso de un evento catastrófico en el cual todos los empleados deban quedarse en casa.

Muchos negocios comenzaron a hacer el cambio a empleados remotos antes de la pandemia del COVID-19. Para otros, esto significa que existen buenas prácticas establecidas y software rentable para hacer la vida más sencilla y mantener su compañía segura.

Temas de Seguridad que los Administradores de Tecnología de la Información Deberán Considerar Cuando se Trata de Trabajo Remoto

Comunicación en línea incrementada sustancialmente

Ahora que tantas interacciones y comunicaciones han cambiado a estar en línea, usted necesita asegurarse de contar con un robusto correo electrónico y seguridad en sus comunicaciones.

Mientras está seguro, generalmente con el video chat viene la elección de un software para sus necesidades más privado y amigable, y las elecciones de correo electrónico son más matizadas. El correo electrónico debe mantenerse seguro ante numerosas amenazas, incluyendo accesos no autorizados o pérdidas.

Las intrusiones en el correo electrónico pueden ser ataques de phishing, spam o malwares, con sujetos, anexos, contenidos o enlaces engañosos que atraen usuarios. Usted necesita un servicio anti-spam integral acoplado con la educación del empleado acerca de la naturaleza y apariencia de estos ataques.

Los ataques de phishing dirigidos a quienes trabajan en casa posiblemente se incrementarán mientras actores maliciosos saben que habrá más personas en esta nueva y menos protegida posición.

Existen numerosos ataques al trabajo-desde-el-hogar y otros que pueden costar dinero a las personas, poner en riesgo información vital y abrir su compañía a otros ataques. Los intentos de piratería potenciales pueden ser reconocidos si las personas saben qué buscar. Ofrezca un curso de actualización a los empleados para que sean conscientes acerca de los ataques de estafas o phishing.



Los actores maliciosos podrían aún usar correo electrónico no asegurado como punto de acceso a su red de trabajo. Para prevenir esto, asegúrese de contar con una contraseña fuerte y la Autenticación Multi Factorial (MFA, por sus siglas en inglés) habilitada.

Como mejor práctica, su compañía debe considerar también la solución de correo electrónico encriptado que analiza el tráfico de correo electrónico saliente para reconocer material sensible y encriptar dichos correos.



Si usted está usando un gran correo electrónico basado en el buscador tal como Gmail, usted ya está encriptando cada correo electrónico con Seguridad de Capas de Transporte (TLS, por sus siglas en inglés). Este tipo de encriptación no es tan segura como la encriptación de extremo a extremo, así que deberá aún usar un servicio diferente para la información sensible. Mientras todos en su compañía sigan los consejos mencionados anteriormente para mantener sus cuentas seguras, y reconocer los escenarios de phishing, sus comunicaciones deberán estar seguras para el trabajo remoto.

Herramienta(s) que Usted Necesita para este Tema de Seguridad

-  Anti-virus con escaneo de correo electrónico
-  Herramientas de Protección para Seguridad de Internet (típicamente integradas en su buscador).

Mejores Prácticas

- Eduque a sus empleados en todos los ataques comunes de phishing y spam.
- Este muy atento de todos los enlaces y anexos enviados a través del correo electrónico, particularmente de remitentes desconocidos.
- Refuerce las regulaciones apropiadas de las contraseñas.
- Refuerce la autenticación de dos factores.
- Use métodos de encriptación más seguros de extremo a extremo para enviar información sensible.



Escaneo y parcheado de dispositivos remotos

En circunstancias normales, su equipo de Tecnología de la Información sigue una programación y una práctica, emitiendo parches vitales inmediatamente y siguiendo parches no vitales durante la noche o durante horas fuera del trabajo para reducir su interferencia con el personal. Ahora, su red de trabajo incluye máquinas que solo estén en la oficina.

Para mantener a todos asegurados mientras trabajan desde casa, usted necesita software que escanee y parche todos los dispositivos remotos.

Una de cada tres violaciones es causada por vulnerabilidades no parcheadas. Estas violaciones de la seguridad pueden ser prevenidas simplemente asegurándose de que sus máquinas estén completamente parcheadas.

Esto es más difícil cuando usted cambia a personal remoto pero no es imposible. Existen opciones de software elaboradas para éste exacto propósito. Su equipo de Tecnología de la Información puede seguir su plan de seguridad en el lugar sin mayores modificaciones. Los dispositivos de su personal podrán mantenerse actualizados y seguros, aún si se encuentran en remoto.

Herramienta(s) que Usted Necesita para éste Tema de Seguridad

-  Monitor de Red de Trabajo
-  Software para gestión remota

Mejores Prácticas

- Haga una valoración de su red de trabajo y elabore un inventario completo. Escanee regularmente su red de trabajo en busca de parches faltantes.
- Asegúrese que todos los sistemas operativos en su red de trabajo estén cubiertos (algo de lo que puede no tener de qué preocuparse cuando no trabaje remotamente, si cada computador de la oficina opera solo con Windows, por ejemplo).
- Programe tiempo para empujar los parches mientras está atento de actualizaciones vitales que deben ser instaladas inmediatamente.
- Haga una prueba después del despliegue y esté listo para retroceder los parches que causen problemas hasta que una solución sea encontrada o se emita un nuevo parche.
- Identifique las vulnerabilidades con escaneos remotos, aún aquellas que no tengan parches faltantes.

Seguridad de la Red de Trabajo en Casa

Otro paso importante hacia la seguridad de los trabajadores remotos es asegurarse que el sistema de seguridad de la red de trabajo en casa este lista y sea robusta.

Encriptando la información en tránsito

Cuando trabaje desde casa, es importante que sus empleados encripten su información. Para mantener los materiales privados, todos en su compañía deberán usar una Red de Trabajo Privada Virtual (VPN, por sus siglas en inglés) cuando traten con información sensible.

Una Red de Trabajo Privada Virtual (VPN) proporciona un túnel encriptado que protege el tráfico de su red y lo desliga de su dirección IP específica. Esto le da a su compañía y empleados una mayor privacidad.

Dependiendo de su Red de Trabajo Privada Virtual, los empleados podrán añadir más riesgo a su red de trabajo a través de las conexiones para dispositivos potencialmente inseguros. Asegúrese que los empleados sean conscientes de éste riesgo y que solamente usen la VPN cuando accedan a información relacionada con el trabajo.



WiFi Encriptado

Mientras que es muy extraño que una WiFi personal sea comprometido, y si ocurre el atacante podrá interceptar todo lo que usted envíe o introduzca en línea: información bancaria, cuentas de correo electrónico, credenciales de acceso corporativo, y más.

Asegúrese que su red de trabajo esté debidamente configurada y encripte su conexión. WPA2 o ahora la WPA3 es considerada típicamente la mejor opción para la encriptación del WiFi, y su contraseña de WiFi deber ser fuerte.

Cambios en el enrutador

Usted deberá cambiar su login o apertura de sesión, al igual que su contraseña. Esto puede considerarse estándar (tal como “administrador”) y ambas pueden ser débiles o fáciles de adivinar. Los actores maliciosos toman ventaja de esto para capturar el enrutador, convirtiéndolo en un bot (robot) o permitiendo que los piratas lo espíen mientras su información en línea es enviada a través del enrutador. Asegúrese que las actualizaciones del firmware sean instaladas automáticamente para gestionar las vulnerabilidades de seguridad.

Dependiendo del nivel de seguridad que su negocio requiera, usted también podrá tomar medidas adicionales al tener a sus empleados con restricciones de tráfico saliente y entrante, seleccionando el más alto nivel de encriptación ofrecido en los ajustes del enrutador, y apagando el Ajuste de Protección del WiFi (WPS, por sus siglas en inglés). Estos pasos no son amigables, así que desplieguelos solo si es absolutamente necesario.

Ajustes del Firewall

Verifique dos veces los ajustes de sus cortafuegos (firewall)) para reforzar la seguridad de su red de trabajo en el hogar. Los cortafuegos crean una barrera para prevenir amenazas que intenten acceder a su sistema. Esto ayuda de dos formas: deteniendo los programas maliciosos para que no entren en su red, y previniendo fugas de información desde los dispositivos de su hogar.

Típicamente, los cortafuegos ya están contruidos para sus dispositivos; asegúrese que estén activados en sus ajustes. Los pequeños negocios podrían necesitar un plan de seguridad más integral a través de un tercer proveedor para fortalecer el cortafuegos.

Active soluciones de anti-virus para los dispositivos personales.

Mientras que las máquinas que usted tiene en la oficina pueden tener protección anti-virus ya instalada, muchos empleados están usando ahora dispositivos personales que podrían no tenerla. Aún si ellos siguen el otro consejo dado, los dispositivos pobremente asegurados sin un riesgo significativo para la seguridad.

Asegúrese de que los computadores que están siendo por sus empleados en sus hogares tengan instalado poderosas soluciones anti-virus. Debido a las circunstancias, esto podría incluir el adquirir una confiable solución anti-virus para los dispositivos de sus empleados, al menos mientras tengan en ellos información privada de la compañía.

Es crítico que usted proteja toda la información relacionada con su negocio, y eso incluye asegurar los dispositivos personales y asegurar las actualizaciones de estas soluciones.

Herramienta(s) que usted Necesita para este Tema de Seguridad

- ✓ Red de Trabajo Privada Virtual o VPN
- ✓ Gestión de banda ancha
- ✓ Herramientas de firewall mejorado
- ✓ Soluciones Anti-virus



Mejores Prácticas

- Siempre use una Red de Trabajo Privada Virtual en redes no confiables.
- Sea consciente de las capacidades de banda ancha de la Red de Trabajo Privada Virtual de una compañía.
- Solo descargue su VPN en dispositivos que usted use en su trabajo.
- Asegúrese que el método de autenticación de la VPN y la encriptación sean lo más fuertes posible.
- Monitoree constantemente las comunicaciones entrantes y salientes de la red de trabajo en busca de actividades sospechosas.
- Tenga una contraseña fuerte para su red inalámbrica.
- Use un enrutador de su propiedad y no alguno ofrecido por su Proveedor de Servicios de Internet (ISP, por sus siglas en inglés) y cambie el nombre y contraseña establecidos de fábrica.
- Utilice las capacidades de cortafuegos más Fuertes que le permitan acceder a su internet cuando lo desee.
- Implemente WPA2 o WPA3 en su red inalámbrica.
- Mantenga su enrutador actualizado.
- Mantenga sus soluciones anti-virus actualizados.



Respalde toda la información con copias de seguridad encriptada

La información no está debidamente asegurada sin copias de seguridad regulares y encriptadas. Esto es cierto sin importar si sus empleados están trabajando desde sus casas, pero es aún más importante con trabajadores remotos.



Usted tiene menos control sobre los dispositivos de trabajadores remotos, y por lo tanto, jamás podrá estar seguro de que todo esté totalmente funcional y seguro. Aún algo tan simple como derramar café sobre un dispositivo podría significar la pérdida de trabajo o información si no cuenta con copias de seguridad apropiadas.

Un Sistema bien asegurado garantiza que toda la información de la compañía pueda ser encriptada, cargada y respaldada en una Fuente centralizada (frecuentemente en la nube, pero no tiene que ser así), así que no tendrá que preocuparse acerca de perder información importante debido a errores humanos o acciones maliciosas.

Herramienta(s) que Usted Necesita para este Tema de Seguridad

 Software de almacenamiento con encriptación activada

Mejores Prácticas

- Realice copias de seguridad frecuente y regularmente.
- Encripte la información durante su almacenamiento.
- Decida cuanto tiempo es necesario para mantener las copias de respaldo para depender de su negocio y el cumplimiento de las reglas.
- Considere almacenar la información más importante en más de un lugar (asegurándose que este toda encriptada y protegida debidamente).

¿Qué tan difícil es asegurar una fuerza de trabajo remota?

Muchas de estas acciones sugeridas requieren pequeñas alteraciones de prácticas que usted ya tiene establecidas o que ha estado realizando, tales como un servicio de gestión de parcheado automatizado o copias de respaldo de su información.

Algunos cambios pueden requerir un ajuste inicial, pero hay muchos productos para apoyar a compañías en proceso de cambio de empleados parcialmente remotos a totalmente remotos. Siguiendo algunas simples mejores prácticas y adicionando algunas herramientas necesarias, su negocio y empleados podrán trabajar remotamente y de forma segura, manteniéndose a salvo.



Proteja su negocio con el juego de solución de seguridad GFI

Unlimited | Network Security

Seguridad multi-capas para prevenir, detectar y gestionar amenazas a su red

Asegure la Red de Trabajo con Firewall & Prevención de Intrusiones

Asegure el Tráfico con Anti-virus para Redes & Correo Electrónico

Asegure los Nodos Terminales con Monitoreo de Vulnerabilidad y Parcheado

Conozca Más

GFITM

Aurea SMB Solutions

Todos los nombres de los productos y compañías mencionadas podrían ser marcas registradas de sus respectivos propietarios. Toda la información contenida en éste documento era válida hasta donde sabemos en el momento de su publicación. La información contenida en éste documento podría cambiar sin previo aviso.