Cómo proteger a su organización de las amenazas de seguridad en medio del aumento de los teletrabajadores

Cómo proteger a su organización de las amenazas de seguridad en medio del aumento de los teletrabajadores. La seguridad se convierte en un desafío mayor a medida que más personas trabajan desde casa debido al coronavirus. Aprenda a proteger mejor a su organización y empleados.

La propagación continua del coronavirus está provocando que más empleados trabajen desde casa, ya sea por su propia voluntad o según lo requieran sus empleadores. El manejo de la seguridad interna para una organización es lo suficientemente difícil, pero cuando también debe lidiar con una fuerza laboral remota remota, las demandas de seguridad pueden ser aún más difíciles.

¿Cuáles son algunos de los desafíos de seguridad relacionados con los trabajadores remotos y cómo puede garantizar que su organización se mantenga sólida y protegida contra las amenazas cibernéticas durante este tiempo?

¿Cuáles son algunas de las amenazas que las organizaciones deben vigilar dado el aumento de trabajadores remotos?

Pishing

Estamos viendo un aumento en los ataques de phishing como resultado de la rápida transición al trabajo remoto para una gran cantidad de personas. Esto es especialmente problemático para las pequeñas y medianas empresas que no tienen la ventaja de contar con personal de seguridad y TI a tiempo completo para monitorear y hacer cumplir la protección adecuada.
Las grandes empresas generalmente han establecido prácticas de trabajo desde el hogar y la infraestructura y los sistemas para respaldar esto. Lo mismo no es cierto para las organizaciones más pequeñas que han tenido que hacer una transición abrupta sin la capacitación, las tecnologías o los procedimientos necesarios. Esto abre a las pequeñas y medianas empresas al posible compromiso de los piratas informáticos que buscan aprovechar la incertidumbre y la inestabilidad inherentes a esta transición.

Personas que acceden a aplicaciones que hasta ahora no eran accesibles de forma remota

El riesgo aquí es que las aplicaciones a las que se accede no están habilitadas para una autenticación fuerte y una comunicación cifrada.

Además, las personas que acceden a las aplicaciones utilizando sus propios dispositivos personales o no administrados. En el caso del trabajo remoto, hasta ahora la mejor práctica era tener dispositivos administrados con controles apropiados, tales como protección contra pérdida de datos, controles antimalware actualizados y una capacidad de monitoreo central. Con este repentino aumento enorme en el número de trabajadores remotos, la menor seguridad de los dispositivos de punto final que usan puede ser un riesgo significativo.

Las organizaciones, especialmente aquellas que operan predominantemente con fuerzas de trabajo en el sitio, pueden no permitir el acceso remoto a los sistemas corporativos. Esto se debe a que los perímetros tradicionales, como los firewalls, que están diseñados para bloquear a los malos actores, también pueden impedir que la fuerza de trabajo remota de una empresa acceda a los recursos para realizar su trabajo.

Para acomodar el trabajo remoto, los equipos de TI pueden necesitar abrir brechas en sus políticas corporativas de red y seguridad para permitir que toda la fuerza laboral acceda a ciertas aplicaciones y servicios de forma remota. Esto podría

dejar huecos para que los malos actores exploten y comprometan los datos críticos del negocio en aplicaciones locales que antes eran inaccesibles desde Internet público.

¿Cuáles son algunos de los riesgos para los trabajadores remotos y para la organización más grande?

Cuando las personas que no están acostumbradas a trabajar a distancia comienzan a trabajar de forma remota, pueden ser un poco descuidados al garantizar que siguen cuidadosamente las precauciones de seguridad. Esto se debe a que generalmente trabajan dentro del «perímetro», y eso les da un mayor grado de protección. Por lo tanto, las buenas prácticas de seguridad deben reforzarse mediante programas de sensibilización que les permitan trabajar de forma remota de forma segura.

El descuido puede generar responsabilidad para algunos trabajadores remotos, dependiendo de las condiciones de su empleo. Para una organización más grande, una fuerza de trabajo remota significativamente ampliada aumenta la superficie de ataque y, por lo tanto, el riesgo de una violación.

Los trabajadores remotos llevan las computadoras portátiles a su entorno hogareño y de repente toneladas de dispositivos fuera del control de los equipos de TI están en la misma red. Esto aumenta significativamente la superficie de ataque y la posibilidad de ser dañado por ransomware u otro malware. Cuando los equipos de TI brindan acceso a los empleados a través de una VPN, a esos dispositivos adicionales también se les puede dar acceso inadvertidamente al centro de datos de la organización. Los equipos de TI y los CISO deben prepararse para una afluencia de ataques internos, que no provienen de fuentes externas, sino internas.

Las organizaciones estarán expuestas a un mayor nivel de riesgo como resultado de los ciberdelincuentes que intentan capitalizar las debilidades en las defensas a medida que las empresas se adaptan a la «nueva normalidad» del trabajo remoto. Las organizaciones de TI se distraerán durante las próximas semanas y meses a medida que aborden problemas urgentes desde el punto de vista operativo, ya sea para garantizar una comunicación y conectividad adecuadas para los empleados, implementar herramientas de colaboración o garantizar que los sistemas y procesos existentes puedan escalar. Si bien la ciberseguridad estará en su lista de prioridades, competirá por la atención con muchas otras bolas que se han lanzado inesperadamente en el aire.

Un error que las empresas podrían cometer es implementar soluciones y políticas de seguridad que restrinjan las formas en que las personas quieren trabajar. Si bien bloquear el acceso a los datos o establecer reglas para limitar la actividad de los empleados podría ayudar a evitar que los datos caigan en las manos equivocadas, tales medidas pueden impedir la productividad si son demasiado restrictivas. Las empresas necesitan empoderar a los empleados para que trabajen de manera segura, sin que la seguridad se interponga en su trabajo.

Las VPN, los escritorios virtuales y otras metodologías que las empresas usan tradicionalmente no son fáciles de escalar para las grandes empresas, ya que están impulsadas por la potencia informática, y no proporcionan la misma escalabilidad y flexibilidad que los servicios en la nube. Las empresas aprenderán rápidamente que no será posible tratar de encontrar formas seguras de proporcionar acceso con este tipo de estrategias remotas tradicionales, y los equipos de TI crearán inadvertidamente varias brechas de seguridad para que los actores de amenazas las exploten.

Algunos errores que las organizaciones pueden cometer al tratar con trabajadores remotos incluyen no aplicar políticas de seguridad y control de acceso basado en roles en todo el dominio corporativo. Además, si no existen soluciones integrales de registro y monitoreo, o la protección de punto final y MDM (administración de dispositivos móviles) no se implementan en toda la organización.

Las medidas de seguridad también pueden debilitarse si se permiten dispositivos no conformes dentro del perímetro. Otra posible debilidad para las organizaciones es no imponer el uso de la autenticación de dos factores para validar los privilegios de acceso.

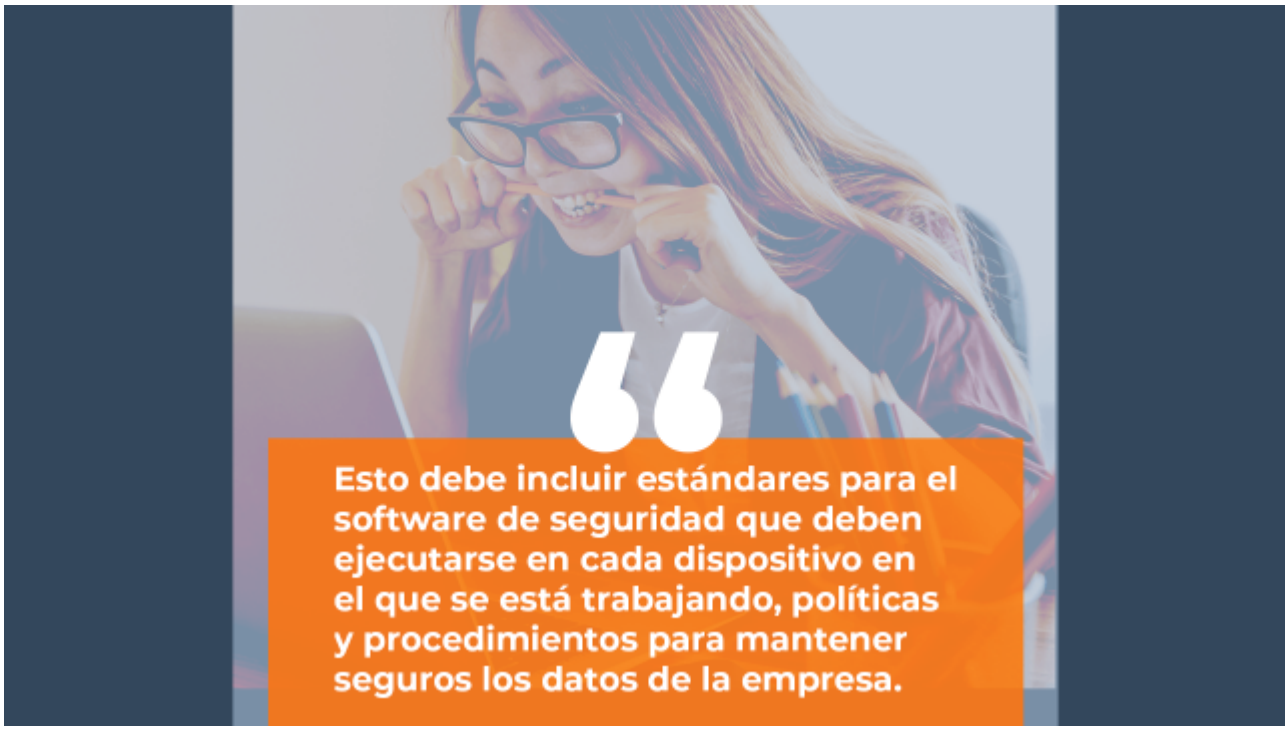
¿Cómo pueden protegerse las organizaciones con el aumento del trabajo remoto?

Siempre que sea posible, el trabajo desde casa debe realizarse desde computadoras portátiles seguras y provistas de trabajo, a través de mecanismos seguros que las organizaciones suelen usar (encriptados y autenticados usando credenciales corporativas y autenticación multifactor).

Si no es posible, y el trabajo desde máquinas personales es

imprescindible, el acceso debe limitarse a la información absolutamente necesaria. Para los casos necesarios, considere incluso comprar una computadora portátil ad hoc de bajo costo que se utilizará únicamente para fines laborales en lugar de utilizar máquinas personales en el hogar que ya estén infectadas y no se puedan limpiar más adelante.

La solución es cambiar a un estilo de trabajo sin perímetro a largo plazo. Las decisiones de autenticación deben tener en cuenta la sensibilidad de los datos a los que se accede, el contexto de la solicitud y el nivel de seguridad de que una acción se origina en un dispositivo autorizado. Estas capacidades se pueden cumplir con una plataforma de identidad bien diseñada que no solo puede tomar estas decisiones rápidamente y decidir si se necesita otra capa de validación de identidad a través de la autenticación de múltiples factores, sino que puede escalar con grandes empresas y reducir la fricción a largo plazo .



Desarrolle un plan y comuníquelo clara y repetidamente a su organización. Esto debe incluir estándares para el software de seguridad que deben ejecutarse en cada dispositivo en el que se está trabajando, políticas y procedimientos para mantener seguros

los datos de la empresa, procesos de escalación cuando surgen problemas y una actualización general de la conciencia y la capacitación en seguridad cibernética.

Asegúrese de que los dispositivos de sus empleados estén ejecutando software de seguridad de punto final y que esto se actualice continuamente. Esto debe incluir capacidades anti-phishing. Idealmente, este software debería administrarse centralmente a través de un portal en la nube. Esto permitirá que el personal de TI (o los gerentes que tienen la responsabilidad de TI) supervisen y controlen la postura cibernética de la organización, incluso cuando los empleados son remotos.

Todos los empleados deben conectarse a Internet a través de una VPN. Esto es especialmente importante si los empleados se conectan a través de conexiones públicas de Internet, aunque generalmente es una buena higiene cibernética mantener la VPN activa en todo momento al acceder a los datos o servicios del trabajo.

Si no eres cliente HostDime, ponte en contacto ya mismo con nuestros asesores para que busquemos como trasladar tu información a nuestra infraestructura y podamos ayudarte a asegurar la data de tu empresa.

Leer también: Post anterior teletrabajo; ¿Qué es la seguridad web? Definición, significado, concepto.