Gestión de riesgos de seguridad cibernética del trabajo remoto en tiempos de epidemias y pandemias

Gestión de riesgos de seguridad cibernética del trabajo remoto en tiempos de epidemias y pandemias. Con los casos del Nuevo Coronavirus (COVID-19) surgiendo en casi todos los estados, muchas empresas están tomando medidas rápidas en un esfuerzo por frenar su propagación.

El teletrabajo, el «trabajo remoto» o simplemente «trabajar desde casa» es una pieza central de esos esfuerzos. Si bien los arreglos de trabajo a distancia pueden ser efectivos para frenar la propagación comunitaria de COVID-19 de persona a persona, presentan desafíos de seguridad cibernética que pueden ser diferentes al trabajo en las instalaciones. A continuación se incluye una lista de consideraciones y consejos para ayudar a guiar a las empresas a superar estos desafíos.

Política

Revise la seguridad de su información actual y otras políticas similares para determinar si existen pautas de seguridad establecidas para el trabajo remoto y el acceso remoto a los sistemas de información de la compañía. Algunas organizaciones pueden tener políticas específicas para el trabajo remoto, mientras que otras pueden prever contingencias en los planes de recuperación ante desastres, las políticas de traer su propio dispositivo y otros planes y políticas similares. Si no existen planes o políticas relevantes, este es un buen momento para establecer al menos algunas pautas básicas para abordar el acceso remoto a los sistemas de información de la compañía

y el uso por parte de los empleados de dispositivos personales para los negocios de la compañía.

Comunicación

Los gerentes deben estar familiarizados con las pautas, planes y políticas de seguridad aplicables, y asegurarse de que la información pertinente fluya a sus equipos y a toda la organización. Es esencial que la organización esté alineada de arriba a abajo. Recuerde, muchos empleados no trabajan en seguridad día a día, y es posible que algunos nunca hayan trabajado remotamente antes. Brindar orientación a todos los empleados es fundamental.

Preparación

Las empresas deben revisar los planes de violación de datos y respuesta a incidentes para garantizar que las organizaciones estén preparadas para responder a una violación de datos o incidente de seguridad. Actualice los planes si es necesario para obtener información de contacto del (ahora) equipo de respuesta a incidentes remoto y asesores externos. El mayor riesgo de seguridad del trabajo remoto refuerza la necesidad de contar con un plan si algo sale mal.

Consejos de seguridad cibernética para trabajo remoto

Recuerde a los empleados los tipos de información que necesitan para salvaguardar. Esto a menudo incluye información como información comercial confidencial, secretos comerciales, propiedad intelectual protegida, producto del trabajo, información del cliente, información del empleado y otra información personal (información que identifica a una persona del hogar).

La información confidencial, como ciertos tipos de información personal (por ejemplo, registros de personal, registros médicos, registros financieros), que se almacena o se envía a o desde dispositivos remotos, debe cifrarse en tránsito y en reposo en el dispositivo y en los medios extraíbles utilizados por el dispositivo.

Capacite a los empleados sobre cómo detectar y manejar ataques de phishing y otras formas de ingeniería social que involucran dispositivos remotos y acceso remoto a los sistemas de información de la compañía. Hay un número cada vez mayor de correos electrónicos de phishing basados en Coronavirus que circulan, aprovechando las preocupaciones de salud del público.

No permita compartir computadoras de trabajo y otros dispositivos. Cuando los empleados traen dispositivos de trabajo a casa, esos dispositivos no deben ser compartidos ni utilizados por nadie más en el hogar. Esto reduce el riesgo de acceso no autorizado o inadvertido a la información protegida de la compañía.

Las redes privadas virtuales (VPN) aseguran que el tráfico de Internet esté encriptado, especialmente si está conectado a

una red Wi-Fi pública. Si su empresa tiene uno, asegúrese de que los empleados utilicen exclusivamente la VPN cuando trabajen y accedan a los sistemas de información de la empresa de forma remota.

La información de la empresa nunca debe descargarse ni guardarse en los dispositivos personales o servicios en la nube de los empleados, incluidas las computadoras de los empleados, las unidades de memoria USB o los servicios en la nube, como sus cuentas personales de Google Drive o Dropbox.

Solicite software de seguridad en los dispositivos de los empleados y asegúrese de que todas las versiones estén actualizadas con todos los parches necesarios.

Considere la posibilidad de prohibir el acceso a los sistemas de información de la empresa mientras esté en una red wifi pública. Con las oficinas cerradas, los empleados pueden verse tentados a trabajar desde sus cafés y cafeterías locales. Sin una VPN de empresa, esto puede conducir a riesgos de seguridad significativos.

Las funciones «Recordar contraseña» siempre deben estar

desactivadas cuando los empleados inician sesión en los sistemas y aplicaciones de información de la empresa desde sus dispositivos personales.

Implemente y aplique la autenticación de dos factores o de múltiples factores (MFA). Si aún no ha activado MFA, ahora es el momento de hacerlo.

Limite el acceso de los empleados a la información protegida al alcance y duración mínimos necesarios para realizar sus tareas.

Considere la administración de dispositivos móviles (MDM) y la administración de aplicaciones móviles (MAM). Estas soluciones pueden ayudar a administrar y asegurar dispositivos móviles y aplicaciones. Estas herramientas también pueden permitir que las organizaciones implementen de forma remota una serie de medidas de seguridad, que incluyen cifrado de datos, análisis de malware y borrado de datos en dispositivos robados.

Mantenga los recursos de TI saludables y con buen personal. Cuando más empleados de lo normal están trabajando de forma remota, o el trabajo remoto es nuevo para una organización, los recursos de TI pueden verse agotados y la asistencia de TI requerida puede aumentar.

En HostDime disponemos de la infraestructura óptima para que las empresas desarrollen no solo su sitio web o aplicación, también su intranet y demás funcionalidades que requiera. Habla con un asesor respecto a tus necesidades puntuales y cómo podemos ayudarte.

Leer también:¿Por qué es importante la seguridad del sitio web?; 10 razones para probar la computación en la nube