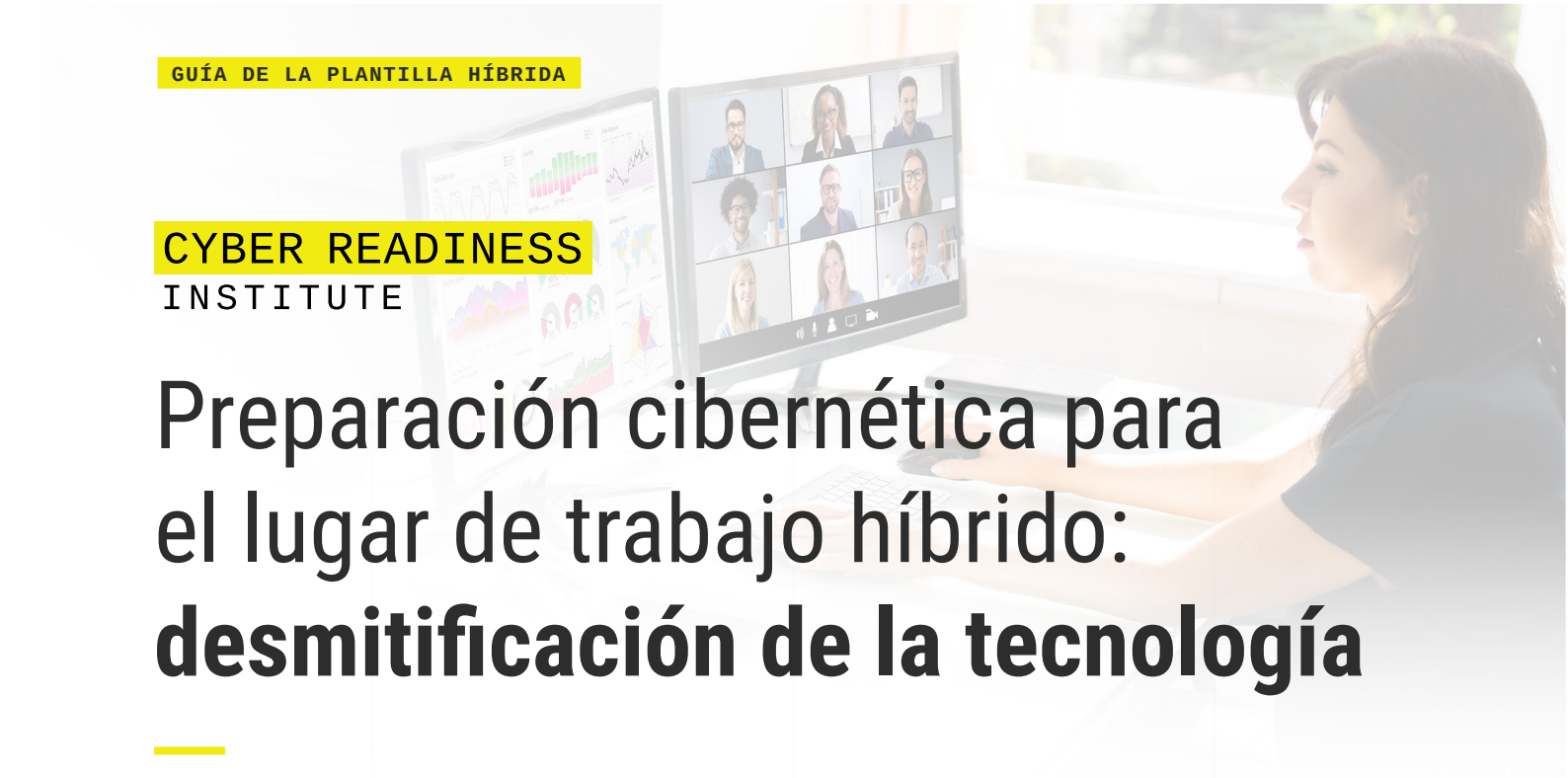

CYBER READINESS
INSTITUTE

Preparación cibernética para el lugar de trabajo híbrido: **desmitificación de la tecnología**

Esta es la situación a la que se enfrentan ahora las pequeñas y medianas empresas (pymes): empleados que trabajan desde casa, la oficina y otros lugares (incluso al aire libre, si el tiempo lo permite). Empleados que utilizan dispositivos de la empresa y dispositivos personales. Empleados que acceden o transfieren documentos de una ubicación a otra y de un dispositivo a otro. Empleados que comparten documentos con otros empleados y terceros. Los piratas informáticos sondean sistemáticamente las redes, buscando aprovechar las nuevas vulnerabilidades.

El lugar de trabajo híbrido plantea nuevos y enormes retos de ciberseguridad para organizaciones de todos los tamaños. Las personas deben desarrollar nuevos hábitos y las organizaciones deben implementar nuevas políticas adaptadas al lugar de trabajo híbrido. El comportamiento humano es la base de la seguridad en todas las organizaciones.

Sin embargo, las organizaciones también deben considerar la posibilidad de implantar nueva tecnología para el lugar de trabajo híbrido. A medida que los empleados se trasladan de una ubicación a otra, es posible que utilicen diferentes dispositivos. Indudablemente utilizan diferentes conexiones para acceder a su red y datos desde distintas ubicaciones. El acceso en el lugar de trabajo híbrido crea vulnerabilidades y el potencial de confusión y caos.

Para las pymes, recomendamos pensar en el lugar de trabajo híbrido en términos de dispositivos, conexiones y datos. Estas son las preguntas básicas que debe responder:

Dispositivos:

1. **¿Qué dispositivos utilizan los empleados?**
2. **¿Utilizan los mismos dispositivos independientemente de dónde se encuentren?**

Conexión:

1. **¿Cómo se conectan los empleados a su red cuando trabajan de forma remota?**
2. **¿Cómo se conectan los empleados a su red en la ubicación de la empresa?**

Datos

1. **¿Cómo acceden los empleados a los datos desde cada dispositivo y ubicación?**
2. **¿A qué datos acceden?**
3. **¿Cómo transfieren los empleados los datos de un dispositivo a otro, de una ubicación a otra y a otros empleados o terceros?**
4. **¿Cómo y dónde almacena la gente los datos?**

guide@cyberreadinessinstitute.com

Hay una enorme cantidad de tecnología disponible para tratar de reducir el riesgo de ciberseguridad, incluido un número abrumador de opciones de hardware y software. El reto para las pymes es comprender qué inversión en tecnología reducirá considerablemente el riesgo de ciberseguridad y qué tecnología permitirá un comportamiento seguro de los empleados en lugar de fomentar soluciones alternativas.

Pensar en la tecnología desde el punto de vista de los dispositivos, las conexiones y los datos es una forma eficaz de evaluar sus opciones y tomar decisiones. Al pensar en la tecnología, el número de empleados y su presupuesto tendrán, por supuesto, un gran impacto en lo que es posible. Aquí se indican algunas consideraciones para empezar.

Dispositivos:

1. **Ordenadores o tabletas de la empresa:** estos reducirán su riesgo y le permitirán tener más control sobre el software que se instala, las actualizaciones de software, los análisis de virus y malware, etc., si se lo puede permitir. Una alternativa es considerar la posibilidad de una infraestructura de escritorios virtuales (véase más abajo).
2. **Smartphones de la empresa:** dependiendo de su negocio y de cómo trabajan las personas, considere también estos dispositivos que proporciona la empresa. Las personas llevan a cabo gran parte de su vida personal en un smartphone y las vulnerabilidades creadas por las aplicaciones sociales y de entretenimiento podrían otorgar acceso a la red de su empresa si no cuentan con un firewall adecuado. Los smartphones de empresa pueden ser controvertidos porque a las personas no les gusta llevar dos smartphones. Como director, debe tomar la decisión de gestión de riesgos que tenga sentido.

Conexiones:

1. **Red privada virtual (VPN):** una VPN es una protección básica importante cuando las personas trabajan de forma remota. Crea un “canal” privado y seguro entre el hogar del empleado y su red.
2. **Segregación de la red doméstica del empleado:** en el caso de los empleados que acceden a información valiosa y confidencial, ayúdelos a configurar su propia red wifi doméstica con una contraseña independiente.
3. **Hotspot de la empresa:** algunos de los hotspots móviles de hoy en día tienen una VPN integrada. Estos hotspots pueden ser una buena alternativa a que la gente utilice una red Wi-Fi compartida o su teléfono personal como hotspot. Además, un hotspot proporcionado por la empresa es una buena opción para los empleados que trabajan desde varias ubicaciones remotas.

Datos:

1. **Intercambio de archivos basado en la nube:** Un buen lugar para empezar. Este intercambio de archivos elimina muchos de los problemas de seguridad con el acceso, la transferencia y el almacenamiento de datos cuando las personas trabajan desde varias ubicaciones porque todos los documentos se almacenan de forma centralizada. Sin embargo, requiere que las personas cambien su comportamiento y desarrollen nuevos hábitos, como: A) Un enfoque organizado para documentar ubicaciones; y B) un proceso para el control de versiones. Las empresas también deben asegurarse de que los empleados tengan conexiones fuertes y seguras (véase más arriba) cuando trabajen de forma remota para garantizar la seguridad del sistema de intercambio de archivos.
2. **Infraestructura de escritorios virtuales (VDI):** VDI significa que el “escritorio” de los empleados no se encuentra en su dispositivo. Está en un servidor al que pueden acceder desde cualquier dispositivo y así se elimina la necesidad de que la empresa proporcione dispositivos. Las aplicaciones y los datos solo existen en el servidor, de modo que se pueden gestionar de forma centralizada. Esta oferta suele incluirse con servicios en la nube, software y software de ciberseguridad.

Independientemente del enfoque tecnológico que elija, recuerde que el comportamiento humano es el elemento más importante para desarrollar una cultura de preparación cibernética en su organización. A la hora de seleccionar e implementar una nueva tecnología, asegúrese de que sea práctica para que las personas la utilicen en sus trabajos, que actualiza sus políticas según sea necesario y que brinda formación y asistencia continua.

Permanezca atento mientras continuamos nuestra serie sobre el lugar de trabajo híbrido para desmitificar la ciberseguridad ofreciendo consejos para directores y empleados.
Eche un vistazo a nuestras otras guías sobre cómo ayudar a las personas a desarrollar buenos hábitos de preparación cibernética y a implementar políticas prácticas que las personas seguirán.

CYBER READINESS
INSTITUTE

Acerca del Cyber Readiness Institute

El Cyber Readiness Institute es una iniciativa sin fines de lucro que reúne a líderes empresariales de todos los sectores y zonas geográficas para compartir recursos y conocimientos que impulsan el desarrollo de herramientas de ciberseguridad gratuitas para las pequeñas y medianas empresas (pymes). Explore los elementos básicos de una buena ciberseguridad con nuestro Kit básico o cree una cultura de preparación cibernética en su organización con el Programa de Preparación Cibernética autodirigido y disponible en línea. Nuestras guías sobre Recursos de trabajo remoto y Lugar de trabajo híbrido ofrecen consejos oportunos para abordar los cambiantes retos cibernéticos de hoy en día. Para obtener más información, visite www.BeCyberReady.com.

CYBER READINESS
INSTITUTE

Preparación cibernética para el lugar de trabajo híbrido: **desmitificación de la tecnología**

Esta es la situación a la que se enfrentan ahora las pequeñas y medianas empresas (pymes): empleados que trabajan desde casa, la oficina y otros lugares (incluso al aire libre, si el tiempo lo permite). Empleados que utilizan dispositivos de la empresa y dispositivos personales. Empleados que acceden o transfieren documentos de una ubicación a otra y de un dispositivo a otro. Empleados que comparten documentos con otros empleados y terceros. Los piratas informáticos sondean sistemáticamente las redes, buscando aprovechar las nuevas vulnerabilidades.

El lugar de trabajo híbrido plantea enormes retos de ciberseguridad para organizaciones de todos los tamaños. Las personas deben desarrollar nuevos hábitos y las organizaciones deben implementar políticas adaptadas al lugar de trabajo híbrido. El comportamiento humano es la base de la seguridad en todas las organizaciones.

Sin embargo, las organizaciones también deben considerar la posibilidad de implantar nueva tecnología para el lugar de trabajo híbrido. A medida que los empleados se trasladan de una ubicación a otra, es posible que utilicen diferentes dispositivos. Es probable que utilicen diferentes conexiones para acceder a su red y datos desde distintas ubicaciones. El acceso variable en el lugar de trabajo híbrido crea vulnerabilidades y el potencial de confusión y caos.

Para las pymes, recomendamos pensar en el lugar de trabajo híbrido en términos de dispositivos, conexiones y datos. Estas son las preguntas básicas que debe responder:

Dispositivos:

1. **¿Qué dispositivos utilizan los empleados?**
2. **¿Utilizan los mismos dispositivos independientemente de dónde se encuentren?**

Conexión:

1. **¿Cómo se conectan los empleados a su red cuando trabajan de forma remota?**
2. **¿Cómo se conectan los empleados a su red en la ubicación de la empresa?**

Datos

3. **¿Cómo acceden los empleados a los datos desde cada dispositivo y ubicación?**
4. **¿A qué datos acceden?**
5. **¿Cómo transfieren los empleados los datos de un dispositivo a otro, de una ubicación a otra y a otros empleados o terceros?**
6. **¿Cómo y dónde almacena la gente los datos?**

Hay una enorme cantidad de tecnología disponible para tratar de reducir el riesgo de ciberseguridad, incluido un número abrumador de opciones de hardware y software. El reto para las pymes es comprender qué inversión en tecnología reducirá considerablemente el riesgo de ciberseguridad y qué tecnología permitirá un comportamiento seguro de los empleados en lugar de fomentar soluciones alternativas.

Pensar en la tecnología desde el punto de vista de los dispositivos, las conexiones y los datos es una forma eficaz de evaluar sus opciones y tomar decisiones. Al pensar en la tecnología, el número de empleados y su presupuesto tendrán, por supuesto, un gran impacto en lo que es posible. Aquí se indican algunas consideraciones para empezar.

guide@cyberreadinessinstitute.com

Dispositivos:

1. **Ordenadores o tabletas de la empresa:** estos reducirán su riesgo y le permitirán tener más control sobre el software que se instala, las actualizaciones de software, los análisis de virus y malware, etc., si se lo puede permitir. Una alternativa es considerar la posibilidad de una infraestructura de escritorios virtuales (véase más abajo).

2. **Smartphones de la empresa:** dependiendo de su negocio y de cómo trabajan las personas, considere también estos dispositivos que proporciona la empresa. Las personas llevan a cabo gran parte de su vida personal en un smartphone y las vulnerabilidades creadas por las aplicaciones sociales y de entretenimiento podrían otorgar acceso a la red de su empresa si no cuentan con un firewall adecuado. Los smartphones de empresa pueden ser controvertidos porque a las personas no les gusta llevar dos smartphones. Como director, debe tomar la decisión de gestión de riesgos que tenga sentido.

Conexiones:

1. **Red privada virtual (VPN):** una VPN es una protección básica importante cuando las personas trabajan de forma remota. Crea un "canal" privado y seguro entre el hogar del empleado y su red.

2. **Segregación de la red doméstica del empleado:** en el caso de los empleados que acceden a información valiosa y confidencial, ayúdelos a configurar su propia red wifi doméstica con una contraseña independiente.

3. **Hotspot de la empresa:** algunos de los hotspots móviles de hoy en día tienen una VPN integrada. Estos hotspots pueden ser una buena alternativa a que la gente utilice una red Wi-Fi compartida o su teléfono personal como hotspot. Además, un hotspot proporcionado por la empresa es una buena opción para los empleados que trabajan desde varias ubicaciones remotas.

Datos:

1. **Intercambio de archivos basado en la nube:** Este intercambio de archivos elimina muchos de los problemas de seguridad con el acceso, la transferencia y el almacenamiento de datos cuando las personas trabajan desde varias ubicaciones porque todos los documentos se almacenan de forma centralizada. Sin embargo, requiere que las personas cambien su comportamiento y desarrollen nuevos hábitos, como: A) un enfoque organizado para documentar ubicaciones; y B) un proceso para el control de versiones. Las empresas también deben asegurarse de que los empleados tengan conexiones fuertes y seguras (véase más arriba) cuando trabajen de forma remota para garantizar la seguridad del sistema de intercambio de archivos.

2. **Infraestructura de escritorios virtuales (VDI):** VDI significa que el "escritorio" de los empleados no se encuentra en su dispositivo. Está en un servidor al que pueden acceder desde cualquier dispositivo y así se elimina la necesidad de que la empresa proporcione dispositivos. Las aplicaciones y los datos solo existen en el servidor, de modo que se pueden gestionar de forma centralizada. Esta oferta suele incluirse con servicios en la nube, software y software de ciberseguridad.

Independientemente del enfoque tecnológico que elija, recuerde que el comportamiento humano es esencial para desarrollar una cultura de preparación cibernética en su organización. A la hora de seleccionar e implementar una nueva tecnología, asegúrese de que sea práctica para que las personas la utilicen en sus trabajos, que actualiza sus políticas según sea necesario y que brinda formación y asistencia continua.

Permanezca atento mientras continuamos nuestra serie sobre el lugar de trabajo híbrido para desmitificar la ciberseguridad ofreciendo consejos para directores y empleados. Eche un vistazo a nuestras otras guías sobre cómo ayudar a las personas a desarrollar buenos hábitos de preparación cibernética y a implementar políticas prácticas que las personas seguirán.

Acerca del Cyber Readiness Institute

El Cyber Readiness Institute es una iniciativa sin fines de lucro que reúne a líderes empresariales de todos los sectores y zonas geográficas para compartir recursos y conocimientos que impulsan el desarrollo de herramientas de ciberseguridad gratuitas para las pequeñas y medianas empresas (pymes). Explore los elementos básicos de una buena ciberseguridad con nuestro Kit básico o cree una cultura de preparación cibernética en su organización con el Programa de Preparación Cibernética autodirigido y disponible en línea. Nuestras guías sobre Recursos de trabajo remoto y Lugar de trabajo híbrido ofrecen consejos oportunos para abordar los cambiantes retos cibernéticos de hoy en día. Para obtener más información, visite www.BeCyberReady.com.