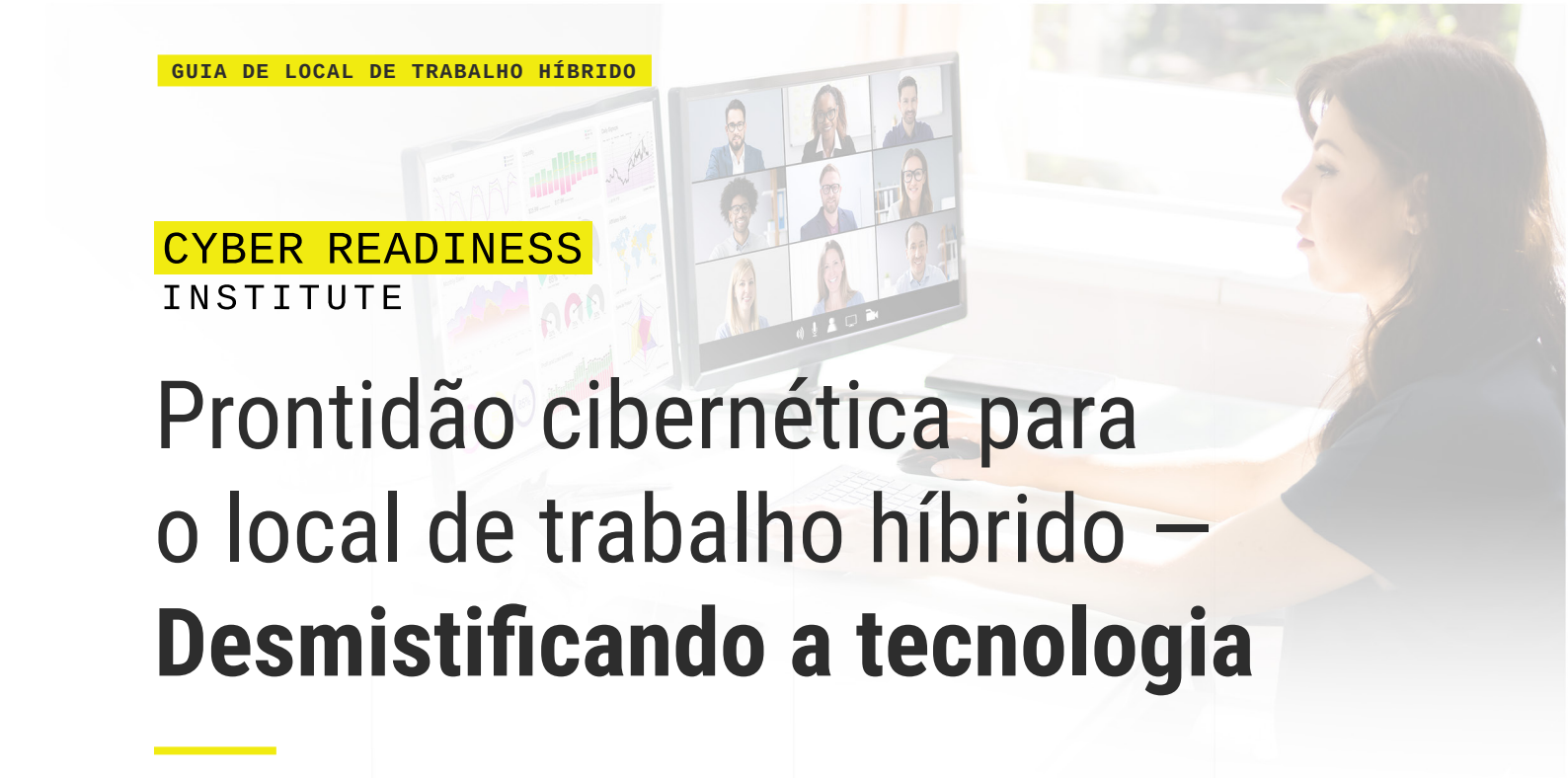

CYBER READINESS
INSTITUTE

Prontidão cibernética para o local de trabalho híbrido — **Desmistificando a tecnologia**

Esta é a situação que as pequenas e médias empresas (PMEs) enfrentam agora: funcionários que trabalham em casa, no escritório e em outros locais (mesmo ao ar livre, se o tempo o permitir). Funcionários que usam dispositivos da empresa e dispositivos pessoais. Funcionários que acedem ou transferem documentos de um local para outro e de um dispositivo para outro. Funcionários que partilham documentos com outros funcionários e terceiros. Hackers sondam redes sistematicamente, procurando tirar proveito de novas vulnerabilidades.

O local de trabalho híbrido apresenta novos desafios de segurança cibernética enormes para empresas de todas as dimensões. As pessoas precisam de desenvolver novos hábitos e as empresas precisam de implementar novas políticas adaptadas ao local de trabalho híbrido.

Dispositivos:

1. **Que dispositivos os funcionários estão a usar?**
2. **Estão a usar os mesmos dispositivos, independentemente de onde estejam?**

Ligação:

1. **De que forma os funcionários estão a ligar-se à sua rede quando estão num local remoto?**
2. **De que forma os funcionários estão a ligar-se à sua rede no local da empresa?**

O comportamento humano é a base da segurança em todas as empresas.

No entanto, as empresas também precisam de considerar a implementação de novas tecnologias para o local de trabalho híbrido. Conforme os funcionários se movem de um local para outro, podem usar dispositivos diferentes. Definitivamente, estão a usar ligações diferentes para aceder à sua rede e dados a partir de locais diferentes. O acesso no local de trabalho híbrido cria vulnerabilidades e o potencial para confusão e caos.

Para as PMEs, recomendamos que pense sobre o local de trabalho híbrido em termos de dispositivos, ligações e dados. Aqui estão as perguntas básicas que precisa de responder:

Dados

1. **De que forma os funcionários estão a aceder aos dados de cada dispositivo e local?**
2. **A que dados estão a aceder?**
3. **De que forma os funcionários estão a transferir dados de um dispositivo para outro, de um local para outro e para outros funcionários ou terceiros?**
4. **Como e onde as pessoas estão a armazenar dados?**

guide@cyberreadinessinstitute.com

Há uma enorme quantidade de tecnologia disponível para tentar reduzir o risco de segurança cibernética, incluindo um número impressionante de opções de hardware e software. O desafio para as PMEs é entender qual o investimento em tecnologia reduzirá significativamente o risco de segurança cibernética - e qual tecnologia permitirá o comportamento seguro dos funcionários em vez de encorajar soluções alternativas.

Pensar em tecnologia através das lentes de dispositivos, ligações e dados é uma forma eficaz de avaliar as suas opções e tomar decisões. Ao pensar em tecnologia, o número de funcionários e o seu orçamento terão, obviamente, um grande impacto sobre o que é possível. Aqui estão algumas considerações para que possa começar.

Dispositivos:

1. **Computadores e/ou tablets fornecidos pela empresa:** Isso reduzirá o risco e proporcionará mais controlo sobre que softwares estão instalados, atualizações de software, limpezas de vírus e malware, etc. Uma alternativa é considerar a infraestrutura de desktop virtual (ver abaixo).
2. **Smartphones fornecidos pela empresa:** Dependendo da sua empresa e de como as pessoas trabalham, considere também estes dispositivos fornecidos pela empresa. Os indivíduos conduzem grande parte das suas vidas pessoais através de um smartphone e as vulnerabilidades criadas por aplicações sociais e de entretenimento podem fornecer acesso à rede da sua empresa se não estiverem devidamente protegidos por firewall. Os smartphones fornecidos pela empresa podem ser controversos porque as pessoas não gostam de carregar dois smartphones. Como gestor, precisa de tomar a decisão de gestão de risco que fizer sentido.

Ligações:

1. **Rede privada virtual (VPN):** Uma VPN é uma proteção básica importante quando as pessoas estão a trabalhar remotamente. Cria um “pipeline” privado e seguro entre a casa do funcionário e a sua rede.
2. **Segregar a rede doméstica do funcionário:** Para funcionários que acedem a informações valiosas e confidenciais, ajude-os a configurar a sua própria rede Wi-Fi em casa com uma palavra-passe separada.
3. **Pontos de acesso fornecidos pela empresa:** Alguns dos pontos de acesso móveis de hoje têm uma VPN integrada. Estes pontos de acesso podem ser uma boa alternativa para que as pessoas usem o Wi-Fi partilhado ou o seu telemóvel pessoal como ponto de acesso. Além disso, um ponto de acesso fornecido pela empresa é uma boa opção para funcionários que trabalham em vários locais remotos.

Dados:

1. **Partilha de ficheiros na nuvem:** Um ótimo lugar para começar. Esta partilha de ficheiros elimina muitos dos problemas de segurança com acesso, transferência e armazenamento de dados quando as pessoas estão a trabalhar em vários locais, porque os documentos são armazenados centralmente. No entanto, exige que as pessoas mudem o seu comportamento e desenvolvam novos hábitos, como: A) Uma abordagem organizada para documentar localizações; e B) Um processo para controlo de versão. As empresas também devem garantir que os funcionários têm ligações fortes e seguras (ver acima) quando estiverem a trabalhar remotamente para garantir a segurança do sistema de partilha de ficheiros.
2. **Infraestrutura de desktop virtual (VDI):** VDI significa que o “desktop” dos funcionários não está nos seus dispositivos. Está num servidor ao qual podem aceder a partir de qualquer dispositivo e podem eliminar a necessidade de fornecer dispositivos fornecidos pela empresa. Aplicações e dados existem apenas no servidor para que possam ser geridos centralmente. Esta oferta geralmente é fornecida com serviços na nuvem, software e software de segurança cibernética.

Não importa a abordagem de tecnologia que escolha, lembre-se de que o comportamento humano é o elemento mais crítico no desenvolvimento de uma cultura cibernética na sua empresa. Ao selecionar e implantar uma nova tecnologia, certifique-se de que é prática para as pessoas usarem de acordo com os seus empregos, de que atualiza as suas políticas conforme necessário e de que fornece formação e suporte contínuos.

Fique atento enquanto continuamos a nossa série de locais de trabalho híbridos para desmistificar a segurança cibernética, fornecendo dicas para gestores e funcionários. Dê uma vista de olhos nos nossos outros guias sobre como ajudar as pessoas a desenvolver bons hábitos de preparação cibernética e implementar políticas práticas que as pessoas seguirão.

CYBER READINESS
INSTITUTE

Sobre o Cyber Readiness Institute

O Cyber Readiness Institute é uma iniciativa sem fins lucrativos que reúne líderes empresariais de vários setores e regiões geográficas para a partilha de recursos e conhecimento que informam o desenvolvimento de ferramentas gratuitas de segurança cibernética para pequenas e médias empresas (PMEs). Explore os blocos de construção de uma boa segurança cibernética com o nosso Kit de Iniciação ou crie uma cultura de prontidão cibernética na sua empresa com o programa de prontidão cibernética online. Os nossos recursos de trabalho remoto e guias de local de trabalho híbrido oferecem dicas oportunas para lidar com os desafios cibernéticos em evolução nos dias de hoje. Para saber mais, visite www.BeCyberReady.com.

CYBER READINESS
INSTITUTE

Prontidão cibernética para o local de trabalho híbrido — **Desmistificando a tecnologia**

Esta é a situação que as pequenas e médias empresas (PMEs) enfrentam agora: funcionários que trabalham em casa, no escritório e em outros locais (mesmo ao ar livre, se o tempo o permitir). Funcionários que usam dispositivos da empresa e dispositivos pessoais. Funcionários que acedem ou transferem documentos de um local para outro e de um dispositivo para outro. Funcionários que partilham documentos com outros funcionários e terceiros. Hackers sondam redes sistematicamente, procurando tirar proveito de novas vulnerabilidades.

O local de trabalho híbrido apresenta enormes desafios de segurança cibernética para empresas de todas as dimensões. As pessoas precisam de desenvolver novos hábitos e as empresas precisam de implementar políticas adaptadas ao local de trabalho híbrido. O comportamento humano é a base da segurança em todas as empresas.

No entanto, as empresas também precisam de considerar a implementação de novas tecnologias para o local de trabalho híbrido. Conforme os funcionários se movem de um local para outro, eles podem usar dispositivos diferentes. Provavelmente estão a usar ligações diferentes para aceder à sua rede e dados de locais diferentes. O acesso variável em todo o local de trabalho híbrido cria vulnerabilidades e o potencial para confusão e caos.

Para as PMEs, recomendamos que pense sobre o local de trabalho híbrido em termos de dispositivos, ligações e dados. Aqui estão as perguntas básicas que precisa de responder:

Dispositivos:

1. **Que dispositivos os funcionários estão a usar?**
2. **Estão a usar os mesmos dispositivos, independentemente de onde estejam?**

Ligação:

1. **De que forma os funcionários estão a ligar-se à sua rede quando estão em locais remotos?**
2. **De que forma os funcionários estão a ligar-se à sua rede no local da empresa?**

Dados

3. **De que forma os funcionários estão a aceder aos dados de cada dispositivo e local?**
4. **A que dados estão a aceder?**
5. **De que forma os funcionários estão a transferir dados de um dispositivo para outro, de um local para outro e para outros funcionários ou terceiros?**
6. **Como e onde as pessoas estão a armazenar dados?**

Há uma enorme quantidade de tecnologia disponível para tentar reduzir o risco de segurança cibernética, incluindo um número impressionante de opções de hardware e software. O desafio para as PMEs é entender qual investimento em tecnologia reduzirá significativamente o risco de segurança cibernética - e qual tecnologia permitirá o comportamento seguro dos funcionários em vez de encorajar soluções alternativas.

Pensar em tecnologia através das lentes de dispositivos, ligações e dados é uma forma eficaz de avaliar as suas opções e tomar decisões. Ao pensar em tecnologia, o número de funcionários e o seu orçamento terão, obviamente, um grande impacto sobre o que é possível. Aqui estão algumas considerações para que possa começar.

guide@cyberreadinessinstitute.com

Dispositivos:

1. **Computadores e/ou tablets fornecidos pela empresa:** Isso reduzirá o risco e proporcionará mais controlo sobre que softwares estão instalados, atualizações de software, limpezas de vírus e malware, etc. Uma alternativa é considerar a infraestrutura de desktop virtual (ver abaixo).
2. **Smartphones fornecidos pela empresa:** Dependendo da sua empresa e de como as pessoas trabalham, considere também estes dispositivos fornecidos pela empresa. Os indivíduos conduzem grande parte das suas vidas pessoais através de um smartphone e as vulnerabilidades criadas por aplicações sociais e de entretenimento podem fornecer acesso à rede da sua empresa se não estiverem devidamente protegidos por firewall. Os smartphones fornecidos pela empresa podem ser controversos porque as pessoas não gostam de carregar dois smartphones. Como gestor, precisa de tomar a decisão de gestão de risco que fizer sentido.

Ligações:

1. **Rede privada virtual (VPN):** Uma VPN é uma proteção básica importante quando as pessoas estão a trabalhar remotamente. Cria um “pipeline” privado e seguro entre a casa do funcionário e a sua rede.
2. **Segregar a rede doméstica do funcionário:** Para funcionários que acedem a informações valiosas e confidenciais, ajude-os a configurar a sua própria rede Wi-Fi em casa com uma palavra-passe separada.
3. **Pontos de acesso fornecidos pela empresa:** Alguns dos pontos de acesso móveis de hoje têm uma VPN integrada. Estes pontos de acesso podem ser uma boa alternativa para que as pessoas usem o Wi-Fi partilhado ou o seu telemóvel pessoal como ponto de acesso. Além disso, um ponto de acesso fornecido pela empresa é uma boa opção para funcionários que trabalham em vários locais remotos.

Dados:

1. **Partilha de ficheiros na nuvem:** Esta partilha de ficheiros elimina muitos dos problemas de segurança com acesso, transferência e armazenamento de dados quando as pessoas estão a trabalhar em vários locais, porque os documentos são armazenados centralmente. No entanto, exige que as pessoas mudem o seu comportamento e desenvolvam novos hábitos, como: A) Uma abordagem organizada para documentar localizações; e B) Um processo para controlo de versão. As empresas também devem garantir que os funcionários tenham ligações fortes e seguras (ver acima) quando estiverem a trabalhar remotamente para garantir a segurança do sistema de partilha de ficheiros.
2. **Infraestrutura de desktop virtual (VDI):** VDI significa que o "desktop" dos funcionários não está nos seus dispositivos. Está num servidor ao qual podem aceder a partir de qualquer dispositivo e podem eliminar a necessidade de fornecer dispositivos fornecidos pela empresa. Aplicações e dados existem apenas no servidor para que possam ser geridos centralmente. Esta oferta geralmente é fornecida com serviços na nuvem, software e software de segurança cibernética.

Não importa a abordagem de tecnologia que escolhe, lembre-se de que o comportamento humano é fundamental para o desenvolvimento de uma cultura cibernética na sua empresa. Ao selecionar e implementar uma nova tecnologia, certifique-se de que é prática para as pessoas usarem de acordo com os seus empregos, de que atualiza as suas políticas conforme necessário e de que fornece formação e suporte contínuos.

Fique atento enquanto continuamos a nossa série de locais de trabalho híbridos para desmistificar a segurança cibernética, fornecendo dicas para gestores e funcionários. Dê uma vista de olhos nos nossos outros guias sobre como ajudar as pessoas a desenvolver bons hábitos de preparação cibernética e implementar políticas práticas que as pessoas seguirão.

Sobre o Cyber Readiness Institute

O Cyber Readiness Institute é uma iniciativa sem fins lucrativos que reúne líderes empresariais de vários setores e regiões geográficas para a partilha de recursos e conhecimento que informam o desenvolvimento de ferramentas gratuitas de segurança cibernética para pequenas e médias empresas (PMEs). Explore os blocos de construção de uma boa segurança cibernética com o nosso Kit de Iniciação ou crie uma cultura de prontidão cibernética na sua empresa com o programa de prontidão cibernética online. Os nossos recursos de trabalho remoto e guias de local de trabalho híbrido oferecem dicas oportunas para lidar com os desafios cibernéticos em evolução nos dias de hoje. Para saber mais, visite www.BeCyberReady.com.