CYBER READINESS INSTITUTE

Como preparar a sua força de trabalho remota para as ameaças cibernéticas

Embora a tecnologia permita às pessoas trabalhar de forma remota, também abre a porta a novos riscos de cibersegurança e proteção de dados.

Agora, mais do que nunca, todas as organizações têm de designar um Líder cibernético: alguém que irá orientar a sua força de trabalho. Veja o nosso site (www.cyberreadinessinstitute.org) para saber mais sobre o nosso Programa de preparação cibernética gratuito e a função de um Líder cibernético.

Apresentamos a seguir as três áreas-chave que os gestores devem ter em consideração para estabelecer uma força de trabalho pronta para a cibernética:

- Que dispositivos é que as pessoas utilizam para se ligar e aceder a informações?
- Como se ligam para aceder às informações?
- De que forma acedem, gerem e protegem as informações?

Dispositivos

Caso os colaboradores utilizem um dispositivo da empresa em casa:

- Relembre os colaboradores para aderir às políticas de palavra-passe/frase de acesso e atualização de software

Se os colaboradores usam dispositivos pessoais:

- Usar palavras-passe/frases de acesso diferentes para uso profissional e pessoal
- Instalar e executar software de análise de vírus
- Atualizar todo o software antes de se ligar à rede da sua organização
- Ativar as atualizações automáticas para todo o software
- Ativar a autenticação multifator sempre que esta estiver disponível

Se os colaboradores usam dispositivos pessoais partilhados (com cônjuge, filhos, etc.):

- Sair e encerrar todas as aplicações no final do trabalho
- Terminar sessão, sair e encerrar todas as bases de dados ou navegadores
- Evitar anotar palavras-passe/frases de acesso e deixá-las no computador ou perto do mesmo
- Não guardar palavras-passe/frases de acesso no dispositivo nem usar o início de sessão automático

Se os colaboradores usarem computadores públicos (como um parque, bibliotecas, cafés ou outros, se estiverem abertos):

- Esta utilização deve ser desaconselhada ao máximo e apenas feita se for essencial
- Fechar e reabrir as aplicações que estavam abertas
- Utilizar a navegação privada no navegador, se possível
- Sair e encerrar todas as aplicações, incluindo navegadores, no final do trabalho
- Nunca guardar documentos no computador público
- Se usar uma pen USB, o que é vivamente desaconselhado, nunca a coloque num computador público

guide@cyberreadinessinstitute.org

Ligações

Caso os colaboradores utilizem uma ligação Wi-Fi pessoal em casa:

- Mudar a palavra-passe/frase de acesso existente na rede Wi-Fi antes de começar o teletrabalho

Caso os colaboradores utilizem um hotspot pessoal ou de empresa

- Usar sempre o hotspot em vez da rede Wi-Fi pública

Se os colaboradores usam uma Wi-Fi pública:

- Regra geral, os colaboradores devem evitar utilizar uma Wi-Fi pública, a menos que a sua organização possua uma Rede privada virtual (VPN) que os colaboradores sabem como usar

Gestão de dados e acessos

Enumere os sistemas e dados a que cada colaborador pode aceder em operações normais.

Terá de haver mudanças no que se pode aceder em teletrabalho?

Em termos de uso de pens USB, o melhor é proibi-los e facultar uma partilha de ficheiros na cloud para transferir, partilhar e armazenar dados:

- Se a sua organização proíbe o uso de pens USB, relembre as pessoas disso mesmo e enfatize a importância de seguir a política durante o teletrabalho
- Se a sua organização permite o uso de USB (não recomendado), dê a cada colaborador um que tenha sido alvo de análise de malware. Informe os colaboradores de que só a podem usar no computador do teletrabalho. ALÉM DISSO, certifique-se de que possuem software de análise de vírus no computador ANTES de inserirem a pen USB

Partilhar e guardar trabalhos para quem está em teletrabalho pode apresentar novos desafios.

- Se a sua organização tem uma partilha de ficheiros centralizada (OneDrive, Google Drive, i-Cloud, Box, Drop Box, etc.), os colaboradores já estão habituados a gerir a forma como colaboram em documentos no trabalho
- Se não for o caso, tem de estabelecer orientações sobre como os colaboradores gerem e partilham os documentos:
  - De preferência, deve configurar um site de partilha de ficheiros.
  - Entretanto, peça aos colaboradores que enviem os documentos como anexos de e-mail encriptados. Muitas aplicações de e-mail (Outlook, Gmail, Apple Mail, etc.) permitem a encriptação de anexos. Existem programas auxiliares que permitem a encriptação de e-mails e anexos (Virtu, Tutanota, VMware Boxer, Symantec Desktop, etc.)
  - As suas orientações devem abranger a nomenclatura de documentos e elementos básicos do controlo de versões. Se os colaboradores guardam documentos de trabalho em dispositivos pessoais, tem de criar uma forma de impedir que um documento tenha mais do que uma versão

Estamos empenhados em ser um recurso de relevo na ajuda às PME a equilibrar teletrabalho e cibersegurança. Entre em contacto connosco para perguntas, comentários ou histórias de sucesso (support@cyberreadinessinstitute org).

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). O Programa de preparação cibernética online está disponível em chinês, inglês, francês, espanhol, português, árabe e japonês.

Para saber mais, visite www.becyberready.com.