CYBER READINESS
INSTITUTE

Prontidão cibernética para o local de trabalho híbrido — **Políticas que as pessoas seguirão**

Empresas de todas as dimensões reconhecem agora que existirá uma "nova realidade" mais permanente para o local de trabalho. Muitas empresas estão a exigir que apenas uma pequena fração da sua força de trabalho regresse ao escritório físico, o que significa que o ambiente de trabalho híbrido - alguns funcionários que trabalham em casa e outros que trabalham no escritório - passará a ser uma realidade.

Essa realidade exige que as empresas desenvolvam e implementem políticas de segurança cibernética resilientes adaptadas ao local de trabalho híbrido. Durante os primeiros meses da pandemia, muitas empresas foram forçadas a concentrar-se na continuidade dos seus negócios e aliviaram as políticas de segurança para ajudar as pessoas a trabalhar com eficiência em locais remotos. É chegada a hora de substituir essas políticas de segurança menos exigentes por políticas híbridas que garantam a segurança uniforme em todos os ambientes de trabalho.

O CRI está focado em ajudar pequenas e médias empresas (PMEs) a estabelecer políticas e procedimentos seguros neste ambiente híbrido.

Para gestores e funcionários, faz sentido pensar na prontidão cibernética para o local de trabalho híbrido em termos de Pessoas, Processos e Tecnologia. Embora, para alguns, essas categorias possam ser usadas em excesso, garantem uma maneira útil de pensar e comunicar sobre a prontidão cibernética - especialmente para pessoas que procuram compreender como lidar com questões de segurança cibernética neste ambiente dinâmico.

Pessoas – quais são as mudanças de comportamento necessárias para ser produtivo e estar preparado para ataques cibernéticos?

Processos – quais são as mudanças nas políticas e procedimentos necessárias para definir expectativas claras para o comportamento dos funcionários e preparar os funcionários para o sucesso?

Tecnologias – que novas tecnologias são necessárias para melhorar a segurança cibernética quando os funcionários estão a trabalhar remotamente ou a alternar rotineiramente o trabalho entre a casa e o escritório?

guide@cyberreadinessinstitute.com

O Cyber Readiness Institute concentra-se no comportamento humano - as pessoas e o processo da estrutura descrita acima - mas também oferecemos orientações sobre tecnologia no ambiente de trabalho híbrido.

Seguem-se sugestões importantes para ajudar gestores a priorizar o que precisam de fazer para garantir um ambiente seguro e híbrido.

Certifique-se de que cada funcionário recebe a devida formação e que aceita as políticas da sua empresa sobre:

- **Palavras-passe:** Uma forte autenticação inclui a utilização de frases secretas de 16 carateres e autenticação multifator, sempre que possível.
- **Phishing:** Disponibilize informações frequentes e atualizadas sobre atividades de phishing, incluindo exemplos de tentativas recentes de phishing em casa ou no trabalho, especialmente relacionadas com a COVID-19.
- **Uso de USB:** Forneça diretrizes disciplinadas sobre como trabalhar com documentos empresariais em vários locais. Esta abordagem pode incluir a criação de um sistema de partilha de ficheiros na nuvem e formação.
- **Atualizações de software:** Descreva as expectativas de que as atualizações devem ser transferidas imediatamente para qualquer dispositivo usado para aceder à rede da empresa.

Todas as empresas devem tentar fornecer um portátil a todos os funcionários que trabalham em casa para evitar a utilização de dispositivos pessoais no trabalho. Se não for financeiramente viável, ajude os seus funcionários a configurar uma conta de utilizador separada nos dispositivos pessoais deles.

Dada a crescente dependência de plataformas de videoconferência, certifique-se de que utiliza plataformas com protocolos de segurança implementados - incluindo a utilização de uma palavra-passe distinta para cada reunião.

Estabeleça comunicações proativas e regulares com a sua equipa, incluindo:

- Ligações de equipa semanais
- Check-ins 1:1 regularmente programados

Acompanhe os nossos guias adicionais da nossa série sobre o local de trabalho híbrido que continuará a desmistificar a segurança cibernética nesta nova realidade e ambiente de trabalho, fornecendo dicas para gestores e funcionários.

Sobre o CRI

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). Os nossos recursos de trabalho remoto estão disponíveis em espanhol e francês. O Programa de prontidão cibernética online está disponível em chinês, inglês, francês, espanhol, português, árabe e japonês. Para saber mais, visite www.BeCyberReady.com.