PHISHX

O que é BYOD?

Seu dispositivo

BYOD é uma sigla em inglês para Bring Your Own Device, em português “traga seu próprio dispositivo”. Em linhas gerais, consiste na utilização de aparelhos pessoais para realizar atividades corporativas.

Esse conceito ganhou força pois grande parte das pessoas possuem equipamentos mais modernos do que os oferecidos pelas organizações. Dessa forma, a liberdade para utilizar tecnologias mais conhecidas, pode trazer mais conforto e produtividade. Além disso, a adoção do trabalho remoto também popularizou ainda mais esse conceito recentemente.

Vantagens

Entre as vantagens, está a possibilidade de utilizar dispositivos que as pessoas estão mais familiarizadas, permitindo que usufruam de toda a capacidade do equipamento. Isso pode gerar um aumento da produtividade e da motivação das equipes. Outro fator importante é que novos colaboradores se adaptam mais facilmente, sabendo que utilizarão dispositivos próprios.

Principais desafios

Sabemos que ameaças cibernéticas são oportunistas, criminosos aproveitam brechas para se infiltrar em sistemas para roubar, sequestrar e vazar informações sensíveis de organizações. Dessa maneira, existem alguns desafios para mitigar os riscos do modelo BYOD.

Ao misturar a vida profissional com a pessoal em seus dispositivos, as pessoas estão ainda mais vulneráveis ao vazamento de dados sensíveis. Essa é uma das preocupações iniciais com esse modelo.

Além de existir a possibilidade de um dispositivo ser roubado ou perdido, também pode ser invadido. Por isso, é preciso favorecer redes confiáveis enquanto utilizadas para fins corporativos, dando preferência para redes virtuais privadas, as chamadas VPNs.

Também é importante separar o que é pessoal das informações que são importantes para a organização. Separar o perfil pessoal do corporativo pode contribuir para a segurança dos dados.

Políticas

O BYOD pode ser um ótimo modelo para muitas organizações, mas é necessário que sejam estabelecidas algumas práticas para encarar os desafios.

É essencial definir políticas claras, com diretrizes de uso, definição de propriedade do equipamento, limites e obrigações de utilização de requisitos de segurança.

Além disso, conscientizar todos os usuários sobre os riscos cibernéticos, com treinamentos constantes e permanentes, torna as pessoas parte ativa das estratégias de segurança. Fazendo com que elas se preocupem com as vulnerabilidades dos dispositivos.

Todas essas estratégias de segurança podem ser aplicadas tanto em computadores quanto em celulares, ou qualquer dispositivo. Assim, a definição das boas práticas deve estar alinhada com as necessidades das organizações e das pessoas que as compõem, para garantir um ambiente seguro.

Dicas

Outro passo fundamental é tornar as senhas obrigatórias em todos os dispositivos, adotando combinações complexas e únicas. Também é possível adotar diferentes formas de autenticação, que incluem múltiplos fatores, como biometria.

Criar uma lista de aplicativos e sistemas que não devem ser instalados e acessados também é necessário para garantir mais segurança. E a obrigatoriedade da utilização de softwares de proteção, como antivírus, além da criptografia dos arquivos também são passos que garantem a segurança digital das organizações.

A definição de boas práticas e políticas podem mitigar muitos riscos, mas se ainda assim houver um incidente, é preciso encontrar maneiras para restaurar as informações. Para isso, pode ser interessante definir estratégias para garantir que qualquer dado armazenado em um dispositivo BYOD possa ser recuperado.