PHISHX

Política de uso de mídias removíveis

Política de uso de mídias removíveis

Apesar de serem muito úteis, mídias removíveis podem trazer muitos riscos. Uma vez que as portas USB podem ser as principais fragilidades de um sistema. Dessa forma, dispositivos como pen drives, cartões de memórias e HDs externos podem ser uma ameaça para as organizações.

Entenda um pouco mais sobre os problemas que esses dispositivos podem proporcionar e como evitá-los.

Quais são os riscos?

Ao conectar um dispositivo infectado em seu computador, você pode estar abrindo todas as portas da sua casa e da sua organização para criminosos. Mas como eles agem, e quais são os riscos a que você pode estar sujeito?

Informações podem ser perdidas: Vale lembrar que todos os arquivos relacionados ao trabalho são propriedade da empresa. Portanto, quando arquivamos dados corporativos sem nenhum tipo de criptografia ou senha, podemos permitir que qualquer pessoa acesse essas informações em caso de perda ou roubo.

Softwares maliciosos: Além de armazenar arquivos, esses dispositivos também podem guardar programas, inclusive softwares maliciosos, como vírus. Assim, ao conectar a mídia removível em um computador, esses programas podem rodar automaticamente, infectando a máquina e até mesmo todos os sistemas.

Como esse tipo de programa conseguiu acesso direto a um computador corporativo, ele pode ultrapassar soluções de segurança sem ser percebido. Dessa maneira, podem ficar coletando e criptografando informações, permitindo que criminosos operem ataques quando for oportuno.

Roubo de senhas: Essas mídias removíveis também podem ser utilizadas para roubar credenciais. Para fazer isso, criminosos instalam programas que armazenam e compartilham esse tipo de dado. Uma vez inserido, esse dispositivo pode monitorar as informações digitadas por alguém, como senhas.

Como se proteger

Como a responsabilidade pelos riscos e impactos que podem ser causados por esse tipo de dispositivo é das pessoas que os utilizam, é preciso ter muito cuidado sempre que optar por usar mídias removíveis, uma vez que elas podem conter vírus ou softwares maliciosos.

Caso a organização autorize a utilização desses dispositivos, é essencial seguir essas dicas para evitar problemas.

Utilize senhas e criptografia: Utilizar senhas e métodos de criptografia é uma das formas para proteger as informações em caso de perda ou roubo de uma mídia removível. Existem algumas ferramentas disponíveis para adicionar essa camada de segurança em seus dispositivos.

Evite dispositivos desconhecidos: Nós já falamos que as portas USB podem ser a melhor forma de entrada para vírus e softwares maliciosos, já que ferramentas de segurança podem não identificar essas ameaças.

Dessa forma, evite conectar qualquer dispositivo desconhecido em um computador que você utiliza, seja ele pessoal ou corporativo. Mas, em último caso, você pode testar o equipamento em um ambiente controlado, antes que ele seja utilizado em outros computadores.

Também é importante evitar conectar mídias removíveis em computadores desconhecidos. Isso porque eles podem conter softwares maliciosos ou vírus que se infiltram nessas mídias e contaminam seus dispositivos pessoais e corporativos.

Desabilite a inicialização automática de programas: A capacidade de rodar um programa assim que um dispositivo for conectado pode facilitar muito a vida de um criminoso. Para se proteger, é muito importante desabilitar a inicialização automática de programas.

Dessa forma, as pessoas podem ser treinadas para ativar os programas presentes em mídias removíveis de forma manual, abrindo a pasta do dispositivo e clicando no ícone do programa.

Ative e atualize ferramentas de segurança: É essencial que as organizações adotem ferramentas como firewalls e antivírus para se protegerem dessas ameaças. Além disso, também é importante manter os sistemas operacionais e dispositivos atualizados, assim como as definições de vírus.

Você também deve escanear as mídias removíveis para verificar se elas estão livres de softwares maliciosos e vírus. Isso pode ser feito toda vez que esse dispositivo for utilizado por outra pessoa, ou você receber de alguém. Para fazer isso, você pode clicar com o botão direito sobre o ícone do dispositivo e verificá-lo com o antivírus.

Monitore o tráfego de informações: Além de todas essas estratégias para reduzir os riscos, as organizações podem optar por monitorar o tráfego de dados entre os equipamentos corporativos e mídias removíveis. Assim, é possível ter controle em casos críticos, como incidentes e ataques cibernéticos, ou de rompimento de alguma política interna.

Treine as pessoas

Como estamos falando de ameaças que ocorrem quando pessoas conectam mídias removíveis inseguras, é muito importante que elas estejam conscientizadas sobre esses riscos.

Elas devem ser treinadas constantemente para compreender os perigos que dispositivos pouco confiáveis podem trazer para a organização.

As pessoas também devem ser informadas sobre a necessidade da utilização de ambientes seguros para testar se os dispositivos estão livres de ameaças. Caso não seja permitido usar esse tipo de recurso, as políticas devem ser claras e bem disseminadas.