PHISHX

Como Shadow IT pode ser um risco para sua organização

O que é Shadow IT?

Shadow IT, em português conhecido como TI invisível, são práticas consideradas desconhecidas, não oficiais e não autorizadas pela equipe de tecnologia da informação. São serviços, softwares e dispositivos utilizados sem que o time que administra os recursos de tecnologia esteja ciente.

Alguns exemplos são serviços de nuvem, aplicações de compartilhamento de arquivos e aplicativos de mensagens, que não são explicitamente autorizados pela organização.

Dessa forma, pode ser compreendido como uma prática das pessoas, uma vez que mesmo que algumas ferramentas não tenham autorização expressa para uso, podem ser úteis e tornam o trabalho mais produtivo.

Apesar de ser uma prática comum, existem riscos de falhas na segurança digital, ocasionando vazamentos de dados e prejuízos financeiros. Por isso, é preciso compreender os riscos que a utilização de ferramentas não autorizadas pode trazer.

Quais são os riscos?

O uso de equipamentos e sistemas desconhecidos podem causar a perda de controle das organizações sobre os próprios dados. Além disso, falhas de segurança também podem criar portas de entrada para criminosos, acessando dispositivos vulneráveis conectados a redes corporativas para executar ataques e sequestrar informações.

Como todo tipo de solução adotada oficialmente por uma organização é gerenciada pelo setor de tecnologia da informação, qualquer tentativa de ataque, falha ou vazamento pode ser detectada com mais velocidade, permitindo ações imediatas. Ao utilizar sistemas ou dispositivos não monitorados para manipular dados corporativos, você pode estar abrindo uma brecha na segurança da sua organização.

Outro fator importante é a exposição a vulnerabilidades causadas pela falta de atualização de softwares, que normalmente ficam sob responsabilidade do time responsável pelos recursos tecnológicos. Como os responsáveis por manter os sistemas atualizados não estão cientes da utilização de algumas ferramentas, não é possível descobrir todos os setores desprotegidos.

Governança

Para muitas organizações, a regulação por meio da atuação em conformidade com leis e padrões é crucial. Dessa forma, o Shadow IT pode causar algumas violações em relação às regulamentações.

Uma vez que a equipe de tecnologia da informação não tem o pleno conhecimento da atividade dos usuários, fica mais difícil garantir que todos estão agindo em conformidade com as normas e boas práticas.

Uma das formas para lidar com essas violações é informando as pessoas sobre os riscos que ferramentas e dispositivos podem trazer para as organizações. Em casos mais extremos, a adoção de soluções que limitam o compartilhamento de informações e acesso a dados em nuvem pode ser uma alternativa.

Estratégias para garantir a segurança

É muito importante que os responsáveis pelos setores de TI tenham conhecimento das práticas não autorizadas dentro da organização. Por isso, é essencial a construção de um diálogo entre os setores para adquirir informações sobre quais serviços e ferramentas podem ser adotados e trazer formalidade para as soluções paralelas, ou aprimorar soluções internas.

Vale lembrar que o licenciamento de ferramentas homologado pelas organizações gera economia de recursos, assim, o gerenciamento de soluções traz benefícios legais e financeiros. Além disso, o controle do inventário de dispositivos e de aplicações é importante para fins de auditoria e monitoramento de custos, o que também é uma forma de mitigar os riscos em relação à segurança digital.

Adotar métodos que garantam que as pessoas mantenham seus aplicativos e sistemas operacionais atualizados também é uma estratégia para mitigar riscos. Além da melhora de performance, atualizações podem corrigir vulnerabilidades de segurança de versões anteriores.

Por fim, estabelecer o duplo fator de autenticação para acessar dados e sistemas corporativos é uma proteção contra ameaças cibernéticas, protegendo os usuários de possíveis vazamentos de senhas.