Melhores práticas em segurança

Estas questões e preocupações comuns são inerentes ao atual mundo de dispositivos conectados. Saber sobre elas é o primeiro passo. O próximo é aplicar o bom senso aliado às melhores práticas em todos os seus dispositivos conectados. Use esta lista de verificação como um guia para seu planejamento.

1. Comece cedo

Faça seus planos pensando em novas tecnologias e em como você as manterá protegidas.

2. Proteja os dados

Use conexões criptografadas e autenticadas sempre que possível.

3. Controle os serviços

Pense em desativar os serviços de tecnologia que você não pretende usar.

4. Mude as senhas

Usar senhas padrão facilita o acesso de hackers aos seus dispositivos. **Ative senhas de interface de usuário.**

5. Gerenciamento remoto

Adote um sistema de gerenciamento remoto que permita a atualização de suas configurações rapidamente. Quanto mais tempo os dispositivos, soluções e sistemas usarem configurações ultrapassadas, mais fácil será invadi-los.

6. Habilite o registro de atividades

Use os registros de atividades e auditorias quando disponíveis para detectar comportamentos nocivos.

7. Só quem precisa saber

Informe os agendamentos e planos de atualização somente para quem realmente precisa deles. Quando muitos funcionários ficam sabendo dos planos de atualização, as chances de uma brecha de segurança aumentam.

8. Monitore dispositivos fora de alcance

Desenvolva um método de monitoramento constante dos dispositivos fora de alcance do seu sistema. Quando suspeitar que um dispositivo foi removido, revogue suas credenciais até confirmar sua localização.

9. Capacidade de atualização

Escolha dispositivos que possam ser atualizados durante toda sua vida útil para mantê-los em dia com novos padrões. Assegure que seus sistemas de atualização possam prevenir a adulteração de arquivos.

10. Desativação do dispositivo

Planeje a desativação do dispositivo removendo as configurações dos sistemas corporativos, excluindo contas e credenciais de usuários e verificando que os sistemas atuais não tenham sido rigidamente codificados para buscar unidades inativas.

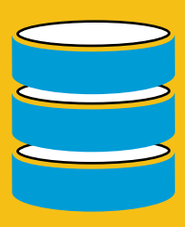
11. Modelo “CID”

Pense na confidencialidade, integridade e disponibilidade (CID) em todas as etapas do ciclo de vida do seu dispositivo.

12. Planejamento contínuo

Fazer atualizações de segurança deve ser uma prioridade constante. O planejamento de segurança não deve ser um evento isolado.

Você sabia?



US$ 360.000

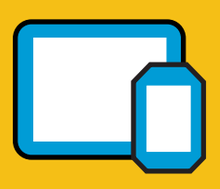
Em média, a criptografia reduz os custos de um vazamento de dados em **US$ 360.000**, sendo a medida mais eficaz contra invasões.[1]

81%

O uso de senhas fracas ou roubadas representou **81%** dos vazamentos de dados causados por hackers.[2]

US$ 1,2 milhão

Empresas que contam com equipes de resposta a brechas de segurança e testam planos de resposta reduzem os custos de um vazamento de dados em mais de **US$ 1,2 milhão.**[3]



38%

38% das empresas relataram incidentes de segurança envolvendo dispositivos corporativos.[4]

40%

40% dizem que ataques cibernéticos são um fator que intensifica a importância de adotar medidas de segurança para dispositivos móveis.

197 dias

Em média, uma organização só percebe que houve um vazamento de dados depois de 197 dias.[5]

[1] IBM Security, *Cost of a Data Breach Report*, 2019 • [2] IBM Security, *Verizon Data Breach Investigations Report*, 2017 • [3] *Cost of a Data Breach Report*, 2019 • [4] Carbon Black, *Incident Response Threat Report*, Novembro de 2018 • [5] Ponemon Institute, *Cost of a Data Breach Report*, 2018 e 2019