COMO MANTER A SEGURANÇA DE DADOS DURANTE O HOME OFFICE?

Tangerino

prolinx
Security First

ÍNDICE

INTRODUÇÃO

1.

Você já se perguntou se sua empresa está protegida no home office? Para muitos, a mudança para esse regime aconteceu em razão da pandemia do novo coronavírus e, sobretudo por essa razão, medidas de segurança de dados não foram devidamente pensadas e implementadas.

De fevereiro para março de 2020, **o número de ataques de ransomwares — o malware sequestrador de dados — aumentou em 148%.** A mudança está relacionada a Covid-19 que impõe a realização do trabalho feito em casa, e não no escritório, a muitos profissionais e empresas.

Os *dados* são da da *VMWare Carbon Black*, empresa de softwares e segurança que aparece entre as que têm acompanhado a movimentação dos *hackers* e seus golpes para roubar dados e até dinheiro de pessoas e organizações.

Diante dessa nova realidade, gestores e funcionários precisam aprender a evitar comportamentos de risco para evitar a perda de informações sensíveis da empresa e os problemas que decorrem dessa situação. Antes mesmo da pandemia, o *home office* já era uma uma *modalidade de trabalho ganhando força no Brasil*. Com isso, pode ser que sua empresa decida manter essa possibilidade mesmo quando as restrições provocadas pelo estado de calamidade pública passar.

Sendo assim, a segurança de dados durante o *home office* pode ser entendida como mais do que uma preocupação temporária. Em todo caso, “prevenir é melhor do que remediar” e você vai descobrir como manter sua empresa protegida com as dicas que Tangerino e Prolinx — cujo foco é a segurança da informação — apresentam neste e-book.

Boa leitura!

Medidas básicas de proteção de dados no home office

2.

Para falar sobre como manter a segurança de dados da empresa enquanto os funcionários trabalham no regime de *home office*, vamos começar por medidas simples que dependem diretamente da colaboração dos trabalhadores.

Por essa razão, antes de qualquer coisa, vamos ressaltar um ponto crucial: o *home office* pode ser desafiador para quem nunca o vivenciou — algo que vale tanto para funcionários e para gestores. Por isso a **comunicação é a chave para que tudo corra bem**, inclusive a segurança.

Existem diferentes *ferramentas para manter a produtividade no home office*, sendo algumas delas especialmente voltadas para facilitar a comunicação — como o *Google Hangouts* e o *Microsoft Teams*.

Isso é importante para dar fluidez ao trabalho no dia a dia e, no que diz respeito à proteção de dados, passar as devidas orientações para que os funcionários adotem, em suas casas, as medidas básicas apresentadas a seguir.

2.1 - Alteração de senhas padrão e fortalecimento de senhas

Os equipamentos em uso para o trabalho em *home office* precisam contar com senhas fortes. Se o funcionário usa no notebook pessoal uma senha fraca ou conhecida por outras pessoas de seu convívio, por segurança, deve ser instruído a escolher uma combinação nova e exclusiva.

Mais do que isso, deve ser orientado também a alterar a senha do *wi-fi* de casa. Certamente, outros moradores podem ser informados sobre a nova combinação, mas a ideia é recorrer a uma senha diferente daquela que já foi passada a tantos visitantes ao longo do tempo — e, claro, apostar em algo forte.

Ainda, é importante conhecer *dicas práticas para manter o wi-fi seguro*, sendo elas:

☑ Escolher de uma (nova) senha de acesso forte e criptografada

O *wi-fi* vem com uma senha padrão que comumente é alterada antes do uso. A questão é que, para garantir a segurança de dados da empresa, o funcionário precisa escolher uma boa senha — daquelas com cerca de oito caracteres, alternando letras e números — e, se tiver essa opção, ativar a *criptografia.*

☑ Evitar compartilhar a combinação com pessoas de fora da própria casa

É comum que o *wi-fi* de casa seja compartilhado com os visitantes e, em um dado momento, perde-se o controle de quantas pessoas têm acesso à rede em questão.

Em qualquer situação, convém alterar a senha de tempos em tempos para eliminar essa fraqueza. No *home office*, fazer isso é imprescindível para proteger os dados da empresa.

☑ Ocultar a rede de wi-fi para que não seja visualizada por vizinhos ou pessoas passando pelas redondezas

Já reparou que, ao ligar o *wi-fi* em um dispositivo, diversas redes aparecem como opção? Em geral, é preciso saber a senha para acessá-las, mas se a ideia é dificultar o trabalho dos *hackers*, ocultar a rede é uma boa ajuda.

☑ Mudar a senha de acesso ao roteador

Alguns equipamentos, como os roteadores, vêm com senhas padrão e isso os torna mais vulneráveis a um ataque *hacker*. Por isso, essa senha padrão deve ser alterada.

Muitos computadores ou *notebooks* usados em casa já vem com antivírus e *firewall* instalados. Entretanto, a empresa pode optar por usar serviços corporativos que são mais potentes do que os softwares de uso pessoal.

Seja como for, é necessário que os funcionários sejam orientados a manter ambos os programas em funcionamento frisando que não vale escolher entre um e outro. *Antivírus* e *firewall* são serviços complementares e desativar um deles pode deixar os dados da empresa mais vulneráveis.

2.2 - Ativação de softwares antivírus e firewall

2.3 - Atualização de softwares e uso de programas originais

Eventualmente, equipamentos eletrônicos compartilham um aviso de que há atualizações disponíveis a serem feitas. Muita gente prefere deixar para depois, para não atrapalhar o trabalho, ou simplesmente ignorar e isso é perigoso.

Atualizações precisam ser feitas porque, mais do que apresentar novidades, trazem mudanças que corrigem falhas e brechas de segurança que, até então, expunham o equipamento ao ataque de *hackers*. Por isso, funcionários devem ser orientados a cumpri-las, ainda que agendem um horário pós expediente para tal.

Medidas técnicas de segurança de dados no home office

3.

Nem tudo o que diz respeito à segurança de dados pode ser entendido como responsabilidade dos funcionários. É importante que a empresa acione seu setor de Tecnologia da Informação (TI) ou uma serviço parceiro para configurar programas e equipamentos — algo que pode ser feito remotamente.

☑ Criação de uma VPN

VPN é sigla para *Virtual Private Network*. A criação de uma *Rede Privada Virtual* — na tradução para o português — tem por objetivo a criação direta entre dois dispositivos e duas redes, criptografando os dados trocados e aumentando a segurança no fluxo de informações.

Assim, a criação dessa rede tende a fazer com que os dados gerados por cada profissional em *home office* estejam mais protegidos, inclusive no momento de seu compartilhamento.

☑ Adoção de um Firewall de Última Geração

Lembra-se de que dissemos que o *firewall* faz parte das ferramentas que podem ser escolhidas pela empresa? Se você decidir seguir por este caminho para aumentar a proteção de dados, a recomendação é buscar um *Firewall de Próxima Geração ou Next Generation Firewall (NGFW)*.

Um *firewall* tem por objetivo filtrar as informações trocadas, funcionando como uma “parede de fogo” a impedir que ameaças entrem uma rede particular, seja ela da empresa ou do funcionário em *home office*.

O NGFW, por sua vez, é uma alternativa capaz de lidar com um volume crescente de dados, sendo a solução mais avançada nesse sentido e, portanto, a mais apropriada para manter dados em segurança.

☑ Uso de ferramentas de segurança a distância

Ainda, buscando manter ou aumentar a segurança de dados no *home office*, a empresa pode adotar ferramentas que funcionam à distância.

Um software como o Umbrella atua na camada DNS (Domain Name System) para realizar uma análise dos endereços acessados com auxílio de inteligência artificial.

Assim, consegue identificar eventuais ameaças em sites acessados pelos funcionários, bloqueando-as antes que atinjam a rede e comprometam a segurança de dados.

☑ Uso de uma ferramenta adequada de acesso a aplicações

Uma solução comumente buscada por empresas que têm funcionários em *home office* — ou em outra modalidade de trabalho a distância — é aquela que permite que um mesmo servidor seja acessado remotamente e por equipamentos diferentes.

A ideia é que os profissionais consigam acessar programas e aplicações presentes no servidor da empresa por meio de seus próprios equipamentos. Isso é interessante porque permite aos funcionários contar com a infraestrutura robusta do servidor da empresa mesmo estando em suas próprias casas.

Para fazer isso, há empresas que recorrem a soluções de terminal server que funcionam bem, mas tendem a ser mais susceptíveis a ataques de hackers. Por isso, a recomendação é fazer a opção por uma ferramenta alternativa, mais segura, como o TS Plus.

Medidas estratégicas para a proteção de dados no home office

4.

Por fim, há medidas que chamamos de estratégicas e que podem ser consideradas a “cereja do bolo” entre as decisões tomadas a favor da segurança de dados de sua empresa durante o *home office*.

Rotinas de *backup* devem fazer parte da realidade de qualquer empresa que deseja cuidar da segurança de dados. O *backup* em si não é uma medida de proteção contra ataques ou roubo de dados, mas garante que a empresa tenha como recuperar informações que eventualmente sejam comprometidas.

Atualmente, o *backup em nuvem* é a melhor solução para empresas independente de seu porte e do volume de dados gerados diariamente. Para o *home office*, é a medida ideal. Imagine a dificuldade se cada funcionário, de sua casa, usasse um HD externo ou pen drives para salvar os arquivos gerados. Como compartilhariam esses dados? E como assegurariam que os equipamentos não seriam danificados ou até roubados, levando consigo as informações da empresa?

Esses questionamentos reforçam a ideia da necessidade da realização de rotinas de backup que podem, inclusive, ser orientadas usando os canais de comunicação que mencionamos anteriormente.

4.1 - Realização de backup em nuvem

4.2 - Uso de tecnologias baseadas na nuvem

Outros serviços baseados na nuvem podem ser importantes, especialmente aqueles atrelados a questões administrativas e burocráticas da empresa.

Como você deve saber, o uso de softwares que otimizam processos e sua gestão vem se tornando mais comum nas empresas à medida que essas se tornam mais abertas para o uso de novas tecnologias. Uma das opções existentes é o aplicativo Tangerino, desenvolvido especialmente para facilitar a marcação e a gestão de ponto dos funcionários de uma empresa. Uma solução que torna possível até mesmo o *controle de ponto de trabalhadores em home office.*

Ainda, o app Tangerino oferece armazenamento em nuvem e isso garante com que todas as informações — seja de marcações de ponto ou de trocas de documentos relacionados (como atestados médicos, por exemplo) — fiquem salvas de forma segura. Assim, a empresa tem garantia de acesso aos dados caso enfrente algum problema de segurança cibernética ou de outra natureza.

Isso é importante porque, vale lembrar, a empresa que perde informações sobre a jornada de trabalho dos colaboradores pode ter dificuldade para fechar a folha de pagamentos corretamente. Um erro que ainda pode levar a um processo trabalhista e perdas financeiras que qualquer um gostaria de evitar.

4.3 - Como adotar essas medidas de segurança

A essa altura, você já conhece diferentes medidas que sua empresa pode adotar para garantir a segurança de dados mesmo durante o período de *home office* — quer este tenha sido imposto pela pandemia da Covid-19 ou aconteça por qualquer outro motivo. Como já indicado, uma empresa pode recorrer a seus profissionais de TI para assegurar a adoção dessas medidas de proteção.

Entretanto, pode não ter mão-de-obra suficiente para implementar o uso de softwares e aplicações tão rápido quanto necessário. Da mesma forma, empresas que não têm um setor de TI podem ter dificuldades.

Para ambos os casos, a solução é apostar na terceirização ou no *outsourcing de TI* e contar com ajuda qualificada para a missão de manter os dados de sua empresa em segurança.

Isso é algo que a Prolinx pode oferecer, não só em relação à implementação das soluções a serem utilizadas, como na orientação para as escolhas mais adequadas à realidade enfrentada pela empresa no dia a dia e no *home office*.

5.

CONCLUSÃO

O uso da tecnologia é como um caminho sem volta para as empresas. No dia a dia de trabalho, seja no escritório ou em *home office*, funcionários recorrem a computadores, notebooks e afins para receber, produzir e enviar informações fundamentais para os processos de seus trabalhos.

Com isso, até mesmo empresas de menor porte tendem a gerar um volume crescente de dados que precisam estar sempre seguros. Em situações normais, ataques *hacker* e outros problemas que podem ocasionar perdas também são possibilidade. Em situações atípicas — como a de uma pandemia — ou de quebra do tradicional para o trabalho feito de casa, a atenção e os cuidados precisam ser redobrados.

Para evitar problemas e seus consequentes prejuízos financeiros e à própria imagem, uma empresa deve adotar medidas de segurança de dados como as que foram apresentadas neste e-book.

Entre em contato para conhecer melhor o *aplicativo Tangerino* e contar com os *serviços da Prolinx* para reforçar a segurança da sua empresa durante o *home office*.

SOBRE A PROLINX

6.

Com 15 anos de mercado, a Prolinx é uma empresa especializada em soluções de Tecnologia da Informação, tendo como principal missão a de garantir a segurança de dados de cada cliente.

Para tanto, a Prolinx acompanha as novidades do mercado de tecnologia e inovação para apresentar as melhores e mais adequadas soluções a cada negócio, aliando isso à excelência nos processos e no atendimento.

Entre em contato e garanta que sua empresa esteja sempre segura — inclusive no home office!

SOBRE O TANGERINO

7.

O aplicativo Tangerino é um sistema de gestão e controle de ponto digital. A solução permite que os colaboradores batam ponto de qualquer lugar, tanto na empresa quanto em home office, usando apenas um celular, computador ou tablet. O aplicativo oferece diversas facilidades que transformam o seu RH em uma área realmente estratégica. Gestão de banco de horas, férias e fechamento de folha de ponto com poucos cliques são alguns de seus benefícios.

Agende uma demonstração