DICAS PRECIOSAS, COM CUSTO ZERO, PARA MAIOR PROTEÇÃO DOS DADOS DA SUA CONCESSIONÁRIA

Alexandre Ayres | Neocom

20/08/2021

As concessionárias de automóveis e montadoras de veículos têm investido tempo e dinheiro para se adequar à LGPD - Lei Geral de Proteção de Dados. Esse assunto tem estado no centro das atenções dos empresários, mas não se pode esquecer que a proteção de dados só é efetiva quando também são tomadas medidas de segurança da informação.

A relação entre segurança da informação e LGPD é próxima, mas o texto da lei não se aprofunda suficientemente nos aspectos e cuidados necessários para reduzir vulnerabilidades e assegurar, na prática, a proteção de dados.

Dessa forma, é fundamental compreender que as vulnerabilidades e ameaças a que estão sujeitas as estruturas tecnológicas das empresas podem permitir graves violações de dados pessoais, trazendo problemas e prejuízos para os negócios.

Uma das mais perigosas e comentadas ameaças tecnológicas da atualidade são os Ramsomware. Ransomware é um malware que pode bloquear dados de computadores e servidores por meio do uso de criptografia. Esse malware é inserido em sua rede de computadores por meio de uma invasão e usado para exigir resgates e extorquir dinheiro de seu proprietário. Em troca, os hackers prometem – claro, sem qualquer garantia – restaurar o acesso às máquinas afetadas ou aos dados.

Segundo levantamento da SonicWall, o Brasil foi o nono país que mais sofreu ataques de Ransomware em 2020. Neste ano, houve êxito em mais de 3,8 milhões de invasões que tiveram como foco, principalmente, as pequenas e médias empresas brasileiras.

Seguem três dicas simples, que podem ser implantadas com CUSTO ZERO para reduzir riscos de invasões em sua empresa, apenas com a mudança de comportamentos perigosos:

DICA NÚMERO 1: SENHA

Uma parte considerável das invasões ocorrem por utilização de senhas consideradas fracas, como as que usam datas de aniversário, nomes dos filhos e sequências básicas de números. Mais que isso: há quem use uma mesma senha fraca - o que é um grande risco – para realizar o acesso a diversos ambientes e sistemas. Uma senha forte, de forma resumida, deve ter letras (maiúsculas e minúsculas), números e caracteres especiais.

DICA NÚMERO 2: PHISHING

Por meio do phishing, cibercriminosos se passam por autoridades ou empresas confiáveis (bancos, corporações renomadas, correios e governo), ou até mesmo, pelo departamento de TI da sua própria empresa, para obter suas informações pessoais, invadir sua rede e roubar dados.

Um e-mail de phishing muitas vezes parece legítimo. Para identificar um e-mail malicioso, fique atento aos seguintes indícios:

- **Verifique o endereço de e-mail**: observe se o endereço de e-mail que lhe enviou a mensagem tem uma grafia duvidosa ou apresenta uma grande extensão com muitos números e abreviações.
- **Preste atenção em erros ortográficos**: Se você recebe uma mensagem com erros de português grotescos, desconfie. Um e-mail legítimo de grandes empresas raramente contém erros ortográficos e de gramática.
- **Não clique em links**: Ao passar o mouse em cima do link disponível, você verá a URL com o endereço da página a ser aberta. Se for um endereço estranho, não clique.

- **Não abra anexos**: Esses arquivos podem conter um malware anexado. Eles podem danificar o computador, roubar suas senhas, além de espiar suas ações, câmera e microfone.
- **Não forneça informações pessoais**: Bancos, correios, empresas e administradoras de cartão de crédito não pedem dados dos clientes por e-mail. Em caso de dúvida, entre em contato pelo telefone ou pelo site oficial da empresa.
- **Não confie nas imagens**: Para maior chance de sucesso, os cibercriminosos usam logotipos, cores e slogan das marcas para dar mais veracidade ao e-mail. Por mais que pareça ser uma mensagem verdadeira, desconfie.

DICA NÚMERO 3: VULNERABILIDADES NA SUA CONEXÃO WI-FI

A rede Wi-Fi da sua empresa pode ser a porta de entrada para invasões que podem expor computadores, servidores, celulares e outros dispositivos que estejam nela conectados. Uma vez que é explorada, a falha permite que o hacker veja tudo o que está sendo transmitido pela rede e injete códigos maliciosos para corromper diversas atividades da organização.

Deixe sua conexão Wi-Fi mais segura com medidas simples:

- **Nunca utilizar um SSID padrão ou senha padrão**: O nome do Wi-Fi é conhecido como identificador de conjunto de serviços (SSID) e, muitas vezes, as empresas se esquecem de mudar o padrão vindo de fábrica. Essa é uma das principais portas de entrada para hackers.
- **Não proteger os APs e hardware de rede**: Nunca deixe pontos de acesso sem fio e outros componentes da rede sem proteção física. Quando isso acontece, uma pessoa mal intencionada passa a ter fácil acesso a ela e, assim, nenhum protocolo de segurança resolveria a situação. Certifique-se de que os principais componentes e equipamentos, como modem, roteadores e switches sejam mantidos em salas ou armários trancados e fora do alcance dos funcionários. Assim, apenas pessoas autorizadas podem ter acesso.
- **Compartilhar a senha Wi-Fi com todos os colaboradores**: Atualmente, a maioria dos funcionários utilizam diversos dispositivos para realizar seu trabalho no escritório, inclusive aparelhos pessoais. No entanto, isso não é motivo para a TI sair espalhando senhas do Wi-Fi corporativo por aí. Se um colaborador deixa a empresa ou se seu dispositivo configurado com a senha Wi-Fi é roubado, pessoas mal intencionadas poderiam facilmente acessar a rede.

Essas dicas não são novidade, e provavelmente você já as conhece, mas a pergunta que realmente importa é: você, de fato, incorporou essas sugestões na rotina da sua empresa?

Alexandre Ayres é Professor na Fundação Getúlio Vargas e Diretor da Neocom Informação Aplicada, empresa especializada em geração de inteligência para o mercado automotivo.
Conheça mais sobre a Neocom no site www.neocom.info.