

Daniel Markuson: Os escritórios e as ameaças cibernéticas

22/02/2021

Com a transição para o trabalho remoto, as questões de segurança *online* ganharam nova importância no universo laboral. Mas nem todo mundo foi afetado da mesma forma. Advogados e demais profissionais que lidam com informações confidenciais sofreram o maior impacto e se tornaram os alvos preferenciais de *hackers* e agentes mal-intencionados na rede.

Por isso, escritórios de advocacia mais do que nunca devem se informar e melhorar suas políticas de segurança para conseguir dar maior confiabilidade à sua prática. Erros comuns, como o uso de redes wi-fi públicas, podem ser fatais ao bom andamento dos negócios. Ninguém quer contratar um escritório que, como o Grubman Shire Meiselas & Sacks, [termina no noticiário por motivos menos que honrosos](#).

É claro, todavia, que esse aprimoramento pode não ser sempre tão fácil. Seja por falta de recursos ou de conhecimento técnico, a indústria jurídica pode enfrentar alguns desafios no caminho. Diante deles, elas podem decidir por buscar um auxílio profissional em empresas especializadas em segurança cibernética caso tenham meios para isso ou adotar pequenas medidas que, embora econômicas, podem ter grandes efeitos na proteção dos seus serviços.

Armazenar em nuvem

Uma dessas estratégias mais simples é a adoção do armazenamento em nuvem. Essa tática permite ao usuário armazenar seus dados com maior praticidade e segurança já que os serviços de nuvem, além de fáceis de se usar, também estão submetidos a rígidas políticas de processamento e criptografia de dados.

Para quem é novo no assunto, o termo "nuvem" se refere a um moderno modelo de servidores remotos que possuem alta capacidade de armazenamento de dados e estão protegidos por mecanismos de segurança de ponta, como a criptografia minuciosa de toda informação ali localizada.

Fazer backups regulares

Uma segunda medida a ser tomada é a realização de *backups* regulares dos arquivos importantes do escritório, como contratos digitais e documentos. Manter uma cópia segura de tais dados é imperativo para o bom funcionamento dos negócios, pois previne a perda de informações.

Em combinação com o armazenamento em nuvem, essa prática garante um melhor gerenciamento dos documentos do escritório, evitando transtornos futuros e facilitando o acesso seguro e rápido a eles.

Investir em tecnologia da informação

Manter uma equipe de tecnologia da informação em seu escritório é uma ótima tática de segurança cibernética. Apesar de talvez ser mais dispendioso que outras possibilidades, esse recurso é fundamental para aumentar a confiabilidade dos negócios e garantir um trabalho livre de maiores dores de cabeça.

Com uma equipe de TI, afinal, pode-se antever riscos e problemas com a rede e, assim, não apenas evitar prejuízos decorrentes de ataques e invasões maliciosas, como também projetar processos de recuperação caso o pior ocorra.

Usar um software jurídico

Um *software* jurídico é outra grande possibilidade de adição aos recursos do escritório. Com ele, o gerenciamento de documentos e processos da companhia pode ser feito de forma mais eficiente e segura, evitando vazamentos e outros problemas menores, como perdas de prazos.

É importante, contudo, que o software escolhido possua atualizações e otimizações regulares pelo seu provedor. Isso porque a cada dia novas ameaças surgem no horizonte e programas desatualizados podem ser tão arriscados quanto o não uso de nenhum deles.

Ter um antivírus instalado

Embora possa parecer bastante básico, muitos escritórios de advocacia são negligentes quanto a essa ferramenta. Um antivírus de qualidade é um dos principais elementos da segurança cibernética, sem ele, todo o resto pode ruir facilmente.



As empresas devem, portanto, buscar uma versão que atenda às suas necessidades e possua constantes atualizações, pois, assim como no caso do software jurídico, **um antivírus desatualizado não é de grande ajuda.**

Assinar uma rede virtual privada

As redes virtuais privadas (também conhecidas pela sigla VPN) são responsáveis por criptografar o tráfego de navegação dos computadores e fazer com que os dados transmitidos por eles estejam sempre seguros onde quer que o usuário esteja.

No atual cenário em que muitos estão trabalhando em casa ou usando redes wi-fi inseguras, o uso de uma VPN se tornou imprescindível. Os escritórios que desejem manter seus negócios protegidos devem buscar um provedor de confiança o quanto antes. Uma boa dica é procurar serviços de **VPN com teste grátis** para poder experimentar suas funcionalidades antes de se comprometer com uma assinatura.

Fonte: <https://conjur.jumps.com.br/2021-fev-22/daniel-markuson-escritorios-ameacas-ciberneticas/>