Ataques cibernéticos direcionados à indústria jurídica são uma ocorrência diária, podendo colocar em risco o sigilo dos clientes.

Nesse sentido, é essencial analisar como os **ataques cibernéticos** estão afetando os escritórios de advocacia, quais medidas tomar e as responsabilidades que escritórios devem ter para ajudar a evitar fraquezas cibernéticas.

Os ataques cibernéticos são tentativas virtuais de destruir, danificar, desabilitar computadores, roubar dados ou usar uma rede de sistemas de computador.

Não é surpresa que o risco representado por esses ataques e que a vulnerabilidade de segurança de dados tenha se tornado uma das principais preocupações para conselhos de administração, gestão corporativa, agências governamentais e públicas.

Além disso, existem mudanças rápidas no cenário regulatório, tornando ainda mais desafiador manter-se atualizado com as novas regras e tendências.

As enormes violações aconteceram no ano passado em grandes corporações de todos os tipos, como empresas da saúde, transporte e etc.

COMO AS VIOLAÇÕES CIBERNÉTICAS AFETAM ESCRITÓRIOS DE ADVOCACIA?

Os escritórios de advocacia não costumam contar com um grande suporte tecnológico, o que facilita o acesso a dispositivos e informações confidenciais.

Nesse sentido, os escritórios estão sendo afetados por violações de segurança cibernética, como apenas alguns exemplos ilustram:

- Em março de 2016, o FBI alertou que os hackers estavam mirando grandes escritórios internacionais de advocacia com o objetivo de roubar informações confidenciais de clientes para fins de insider trading
- Um ataque cibernético prejudicou as operações de um escritório global em junho de 2017 e resultou em um desligamento preventivo de toda a operação de TI da empresa nos EUA por vários dias.

CONSEQUÊNCIAS PREJUDICIAIS

Existem consequências significativas para os escritórios de advocacia como resultado de vazamento de dados, incluindo tempo de inatividade e perda de horas faturadas, destruição ou perda de arquivos.

Além disso, existem gastos referentes às taxas substanciais de consultoria para reparar danos resultantes dos ataques, não apenas os danos tecnológicos, mas também danos à reputação.

O QUE UM ESCRITÓRIO DE ADVOCACIA DEVE FAZER PARA ESTAR PREPARADO E EVITAR UMA VIOLAÇÃO CIBERNÉTICA?

Existem muitas ações que os escritórios devem considerar para aumentar a segurança, uma vez que a atenção deve se voltar para proteção do **direito e tecnologia**, como as que serão apresentadas a seguir.

- Empregar um bom consultor ou fornecedor de segurança de computador para procurar áreas fracas, especialmente se a empresa não tiver equipe interna qualificada em TI
- O treinamento de funcionários e advogados da empresa sobre as políticas e procedimentos na prevenção de ataques cibernéticos é fundamental
- Atualize a política de **práticas de segurança** cibernética da empresa pelo menos uma vez por ano, adotando as melhores táticas da justiça digital
- Considere comprar uma apólice de seguro de responsabilidade cibernética para a empresa
- Certifique-se de que a empresa tenha um plano de comunicação de crise em caso de violação
- Atualize software e altere senhas regularmente
- Os sites de escritórios de advocacia devem seguir as práticas mais atuais e recomendadas para a segurança de dados.

Em resumo, estas são as principais considerações acerca dos **ataques cibernéticos** em escritórios de advocacia. Continue acompanhando nosso blog e siga nosso Instagram para

mais conteúdos.