INFORMATIVO
DE DIREITO DIGITAL

LOPES & CASTELO
SOCIEDADE DE ADVOGADOS

Esse informativo é uma publicação da Lopes & Castelo Sociedade de Advogados

73% DAS VIOLAÇÕES NO MUNDO OCORRERAM POR *RANSOMWARE*

Segundo dados recentes da SEK, obtidos pela pesquisa "Think Ahead Report 2024", verificou-se que no período de 2023, a nível global 73% das violações ocorreram por *Ransomware*, comumente conhecido como um software de extorsão que acessa dispositivos para obter dados digitais usando a criptografia e, após isso, bloqueia o acesso para exigir um resgate para desbloqueá-lo.

Em que pese na América Latina o número de violações seja menor em relação ao Hemisfério Norte, os dados da pesquisa revelam números ainda mais alarmantes no aspecto da América Latina, tendo em vista o crescimento acentuado de 440% de empresas se tornando alvos de criminosos cibernéticos.

Os ataques por *Ransomware* representam uma ameaça tanto para as grandes empresas quanto para as empresas de pequeno porte, entretanto, as PMEs podem ser um alvo ainda mais fácil para os cibercriminosos, haja vista que comumente possuem estrutura de proteção menor. Isso só reforça a necessidade de governança em Tecnologia e Segurança da Informação e de uma assessoria competente em direito digital.

PERFIS FALSOS EM REDES SOCIAIS

Os perfis falsos estão cada vez mais disseminados nas redes sociais e representam um grande perigo aos usuários, sejam eles pessoas físicas ou jurídicas. Esses perfis oferecem riscos graves, tendo em vista que coletam informações pessoais ao interagir com os usuários e roubam pessoais.

Grande parte desses perfis falsos se apresentam como empresas fakes e o usuário ao clicar num link dispostos na página do impostor, é redirecionado para sites externos. Isso é muito comum, especialmente com sites de apostas, investimentos e jogos de azar. De modo que, ao usuário acessar o link direcionado, insere dados pessoais, como login, senha, cartão de crédito e, consequentemente, suas informações são roubadas.

Além disso, ainda que o usuário não insira suas informações, ao clicar no link, caso o site opere com malware, o dispositivo do usuário pode ser infectado e, a partir disso, as informações serem coletadas indevidamente.

Caso isso ocorra, é fundamental que o usuário execute todos os trâmites administrativos para reaver sua conta e, não tendo sucesso, se socorra de uma banca jurídica especializada em direito digital para buscar na justiça o direito às suas contas.

COOPERATIVA SICOOB PODE TER SIDO ALVO DE ATAQUE DE *RANSOMWARE* COM VAZAMENTO DE DADOS

A cooperativa financeira Sicoob teria sofrido ataque de *ransomware*, que supostamente gerou o vazamento de cerca de mais de 1TB de dados. Aparentemente, o ataque foi causado por um grupo de *ransomware*, chamado *RansomHub*, que já fez outras empresas como vítimas, como a consultoria brasileira YKP e a casa de leilões britânica Christie's.

Segundo notícias, supostamente foram vazados dados de acordos de não divulgação, informações de cliente e colaboradores, dados financeiros empresariais, informações de projetos, códigos fontes de produtos e bases de dados da cooperativa.

Em nota, a Sicoob confirmou identificou um incidente cibernético no local e ressaltou que já acionou as autoridades competentes e iniciou uma investigação para entender a extensão do incidente.

Após as devidas investigações, caso confirmada a extensão do incidente, a cooperativa pode sofrer graves prejuízos financeiros e reputacionais, inclusive decorrentes da Lei Geral de Proteção de Dados (LGPD), tendo em vista a vulnerabilidade de segurança e dados supostamente vazados.

SOFTWARE ESPIÃO E MONITORAMENTO SECRETO DE DISPOSITIVOS DE DADOS E COMUNICAÇÃO

Cada vez mais tecnologias conhecidas como "software espião" estão sendo utilizadas por serviços de inteligência e órgãos do Estado para supostamente realizar vigilância remota e de dispositivos móveis.

Em que pese as disposições na Constituição Federal, no Marco Civil da Internet e na Lei Geral de Proteção de Dados, acerca dos direitos de privacidade e proteção de dados pessoais, os dispositivos ainda são omissos em relação as novas tecnologias que infectam dispositivos, sem o conhecimento dos usuários, por meio de malwares ou spywares.

Essas ferramentas são comercializadas para invasão de dispositivos de dados e comunicação, como é o caso do produto Pegasus, da NOS Group. Após infectar o dispositivo, o software possui pleno acesso, atuando como administrador e executando comandos com alcance a todo tipo de informação do dispositivo.

Atualmente, é necessária uma regulamentação específica sobre o tema, delimitando eventuais invasões arbitrárias que violem a privacidade e proteção de dados dos usuários. Para se proteger dessa ameaça invisível, alguns cuidados são essenciais, como evitar links ou anexos suspeitos, uso de senhas fortes e troca de senhas com periodicidade, além de consulta com profissionais de tecnologia da informação e, principalmente, apoio de uma assessoria jurídica especializada.

VAZAMENTO MASSIVO DE DADOS ATINGE CLIENTES DA NOMAD, AVENUE E WISE

Um ataque cibernético contra o banco norte-americano Evolve Bank & Trust comprometeu dados mantidos pela instituição e de empresas parceiras que se relacionam com a instituição, como a Nomad, Avenue e Wise.

A Nomad e a Wise, conhecidas por concederem aos brasileiros serviços financeiros internacionais de forma facilitada, bem como a Avenue, corretora de investimentos, prontamente emitiram uma nota sobre o incidente e vazamento de dados de seus clientes.

Segundo informações recentes, o banco não cedeu à tentativa de extorsão dos criminosos cibernéticos, que acessaram e vazaram dados de clientes e terceiros de outros bancos que realizam open banking.

O Incidente evidencia a necessidade tanto de empresas quanto de seus parceiros comerciais possuírem medidas preventivas, políticas e plano de gestão de incidentes efetivos em suas estruturas para garantir a proteção de dados e protocolos de planos de ação em caso de incidentes.