

Como a presença do Brasil na Convenção de Budapeste ajuda a combater os cibercrimes

Após anos, o Brasil finalmente teve sua adesão à Convenção de Budapeste, também conhecida como Convenção sobre o cibercrime, a primeira a debater este tema. O congresso tem a ideia de fortalecer os meios disponíveis para prevenir e enfrentar os crimes cibernéticos.

Por causa dessa entrada, o combate aos cibercrimes agora terá ajuda de órgãos internacionais, como a Interpol, por exemplo, e isso adiantará os processos em seis meses em média, segundo especialistas jurídicos. Para o Brasil, isso é uma vantagem, pois de acordo com um levantamento da Roland Berger, consultoria estratégica alemã, mais de 9 milhões de ataques são os chamados ransomware, que sequestram dados e pedem resgate às vítimas para a liberação.

Em janeiro foi comemorado o Mês Internacional da Proteção de Dados, data não muito conhecida no Brasil, mas com relevância o suficiente para chamar a atenção para esse cenário. A importância do dia atenta para o cuidado que as pessoas devem ter ao compartilhar informações na internet e conscientizar empresas para serem mais responsáveis quanto ao tema, principalmente agora na era digital. Para gerar a proteção, é preciso o investimento em segurança cibernética, que ajude a reconhecer riscos e fazer o escaneamento de sites e programas.

Sendo o 5º maior alvo em cibercrimes e ficando atrás apenas dos EUA, Reino Unido, Alemanha e África do Sul, a adesão do Brasil à Convenção traz um reforço à Lei do Marco Civil da Internet e, também, contribuirá ativamente na Lei Geral de Proteção de Dados (LGPD). No ano passado, as perdas globais chegaram a US\$ 6 trilhões, o que significa três vezes mais que o PIB nacional.

Agora em 2022, a tendência é que esse tipo de cibercrime, juntamente com roubos de identidades, phishings e fraudes nos comércios eletrônicos cresçam ainda mais, já que o e-commerce cresceu cerca de 30% após o início da pandemia e a tecnologia continua evoluindo ativamente.

Para ajudar nesse combate, os empreendedores e até mesmo empresas podem adotar medidas como o Zero Trust, a prevenção contra o vazamento de informações e até mesmo criar um plano de conscientização sobre a

cibersegurança. Os setores alvo, conforme o levantamento da consultoria alemã são varejo, finanças, hotelaria e manufatura.

No início de 2020, o Brasil criou o Decreto Federal nº 10.222102, que aprova a Estratégia Nacional de Cibersegurança. O objetivo deste regulamento é orientar o país em termos de segurança e incluir iniciativas para aumentar a proteção contra ataques. Adicionalmente, o decreto propõe um modelo de governação centralizado, para promover a coordenação entre as diferentes áreas relacionadas e estabelece a criação do Conselho Nacional de Cibersegurança.

O Banco Interamericano de Desenvolvimento (BID) elaborou um relatório sobre o estado de maturidade dos países latino-americanos, onde demonstra que o desenvolvimento moderado em cibersegurança na América Latina é um desafio para todos os atores do ecossistema. Para isso, as instituições públicas, privadas, de ensino e o terceiro setor devem coordenar esforços que contribuam para a criação de tecnologias seguras e acessíveis. O preenchimento dessa lacuna não terá apenas impactos positivos nos profissionais e nas empresas, mas também no desenvolvimento da inclusão social.

Por Gustavo de Camargo, Sales Director da VU Brasil, empresa líder em proteção de identidade e prevenção de fraude na América Latina.