INFORMATIVO SINDIFLORES

ANO 20 – EDIÇÃO 34
AGOSTO/2024

Ataques Cibernéticos

Ataques cibernéticos a pequenos e médios negócios crescem no País,
em paralelo, governo discute Estratégia Nacional de Cibersegurança.

O crescimento de ataques cibernéticos a Pequenas e Médias Empresas (PMEs) no Brasil é, hoje, uma das principais preocupações do setor produtivo e, até mesmo, das instâncias governamentais debruçadas sobre o tema. Elas se valem de uma série de dados — além de relatos — que evidenciam que, de 2023 para cá, esses negócios se tornaram alvo de criminosos que atuam online, invadindo softwares para roubar credenciais (senhas) ou sequestrar informações (dados) e exigir resgate para devolvê-los.

“Até alguns anos atrás, o foco era instituições do governo e grandes empresas”, afirma a advogada Juliana Abrusio, que ocupa, desde o início deste ano, uma cadeira no Comitê Nacional de Cibersegurança. “Agora, porém, aumentou muito a atenção para a vulnerabilidade das PMEs. Eu vejo isso como um elemento central das discussões e das elaborações de políticas”, completa.
Segundo ela, que também é sócia de Direito Digital e Proteção de Dados do escritório Machado Meyer, em São Paulo, o problema é mais profundo, porque a imensa maioria das empresas — muitas destas PMEs — só entende a relevância de se proteger desse tipo de crime quando é efetivamente atacada. É por isso que, para ela, as estratégias precisam focar nas pessoas. “Ainda que projetos sejam feitos para funcionar a partir de estruturas, são elas que executam esses planos. Não há como agir em cibersegurança sem considerar os operadores e, ao mesmo tempo, quem está vulnerável aos ataques”, explicou.

O advogado, especializado em Direito Digital, Vainzof entende, que a partir disso, este é o momento ideal para discutir o assunto no Brasil. Ele observou como, em um período de pouco mais de uma década, as preocupações envolvendo crimes cibernéticos no País cresceram significativamente, na medida em que as empresas se tornaram alvo sem contarem com proteção necessária — tanto dos pontos de vista prático quanto de uma regulação efetiva. “Passamos pelo Marco Civil da Internet; depois, por LGPD e Convenção de Budapeste; agora, debatemos o marco regulatório da Inteligência Artificial (IA) e, em paralelo, a Política Nacional de Segurança Cibernética (PNCiber). Não é à toa, pois essa não é uma pauta técnica, mas de caráter de segurança nacional”, afirmou o consultor.

O advogado, ainda contou, que uma das discussões globais mais presentes atualmente diz respeito às regulações internacionais de cibersegurança como escopos estratégicos dos países. Vainzof foi um dos convidados para a reunião do G20 sobre o tema, em Brasília (DF), há algumas semanas. “As ameaças cibernéticas representam risco contínuo e crescente para empresas, investidores e clientes, bem como para nações inteiras. O custo da inação é alto. É preciso agir urgentemente. Vai muito além da proteção de dados pessoais e dos segredos de negócios corporativos, porque ataques cibernéticos podem travar organizações e países”, completou.

Cibersegurança movimenta trilhões por ano
De fato, uma pesquisa da norte-americana Mastercard com empresas brasileiras realizada em 2022 mostrou que seis em cada dez desses negócios (64%) são alvos potenciais de ataques cibernéticos no País. Esse número fica ainda mais

relevante quando se observa, no mesmo estudo, que apenas metade (48%) dispõe de políticas definidas para segurança digital dos colaboradores, ao passo que só 32% têm departamentos próprios para lidar com o assunto.
Dados compartilhados da IBLISS, mostram que, se fosse uma nação, a cibersegurança seria a terceira maior economia global, movimentando cerca de R$ 43 trilhões por ano. “Além desses números, há os impactos sobre a resiliência das empresas. Quando um ataque acontece, compromete todo o sistema corporativo. A primeira ação é justamente evitar qualquer possibilidade de backup, enfraquecer as estruturas de proteção”.

Um dado específico da pesquisa do INCC — de que 98% dos negócios brasileiros dizem que fazer backups regulares de suas informações —para mostrar como o País está bastante vulnerável. “Isso não resolve nada. Os ataques cibernéticos são feitos justamente para que não haja outra opção que não pagar o resgate. Quando as empresas dizem que essa é a ação mais importante que fazem no campo da cibersegurança, é porque ainda não entenderam nada”. “A resiliência é fundamental porque não se trata de se, mas de quando [um ataque pode acontecer]”.

Mas como regular? O Reino Unido é o principal modelo global existente hoje, cujo escopo pode servir de inspiração para o Brasil. O país europeu tem um orçamento de R$ 1,3 bilhão anual para lidar com o tema, além de medidas significativas como o Centro Nacional de Cibersegurança (NCSC, na sigla em inglês), criado em 2016 para fornecer soluções ao governo britânico.

No caso brasileiro, os recursos despendidos para cibersegurança, no ano passado, foram da ordem de R$ 24 milhões, segundo o INCC. “Não estamos falando apenas de mais dinheiro, mas também da construção de estratégias inteligentes que dependam desse tipo de investimento”, finalizou Luana.

O Sindiflores reúne empresários, especialistas e consultores para fomentar e desenvolver o comércio varejista de flores e plantas ornamentais. Atua junto ao governo para a desburocratização e pela modernização empresarial, com propostas e soluções que possam viabilizar a vida do empreendedor. Representa 4.734 empresas, que empregam mais de 11.000 pessoas diretamente e mais de 5.000 indiretamente.

Se deseja não receber mais mensagens como esta, responda esse e-mail com a palavra CANCELAR

Sindiflores
Sindicato do Comércio Varejista de Flores e Plantas Ornamentais do Estado de São Paulo
Telefone e Whatsapp: (11) 3865-7475 E-mail: secretaria@sindiflores.com.br
https://www.facebook.com/sindifloressp www.sindiflores.com.br https://www.instagram.com/sindiflores_sp