O maior prejuízo de um ataque digital não está na multa



Na prevenção a ataques digitais, o roteiro se repete: campanhas internas, treinamentos e alertas contra e-mails suspeitos. São medidas necessárias. O problema é que elas tratam o ataque como um erro individual, que se evita com atenção. No ransomware, o ataque em que criminosos bloqueiam os sistemas e os dados de uma empresa e exigem pagamento para liberá-los, o prejuízo aparece em outro lugar: na linha de produção que não roda, no pedido que não é faturado, na entrega que não sai.

Em outubro, o Brasil registrou 32 ataques de ransomware, o maior número do ano e o quinto mês seguido de alta, segundo a plataforma Ransomware.live. Parece pouco, mas foi o suficiente para colocar o país em quarto lugar no ranking mundial. Em setembro, ele havia chegado ao terceiro, num mês em que o total global caiu 27%. A conta considera apenas as empresas que os criminosos expõem em sites de vazamento. Quem negocia o resgate em silêncio fica de fora, e o número real é desconhecido.

Em outros países, esses casos deixam rastro. Em julho de 2025, a Clorox processou a Cognizant, sua prestadora de suporte técnico, em US$ 380 milhões pelo ataque que parou suas operações em agosto de 2023. No mesmo ano, a Qantas cortou em 15% o bônus de seus executivos depois de uma violação de dados. No Brasil, os incidentes acontecem, mas quase nunca chegam a um tribunal ou a uma ata de conselho. Sem esse registro, cada empresa calcula o risco pelo que ouve dizer: algumas contam com a sorte, outras acreditam que estar adequadas à LGPD basta.

A ANPD foi confirmada como agência reguladora pelo Congresso neste ano, e é compreensível que a multa tenha virado a principal preocupação. Só que a multa da LGPD tem teto: 2% do faturamento no Brasil, limitado a R$ 50 milhões por infração. A parada não tem. Investigação forense, resposta ao incidente, receita perdida e reconstrução de sistemas entram todos na conta.

O dano também passa de uma empresa para outra. O ataque à Jaguar Land Rover, em setembro de 2025, parou fornecedores da cadeia automotiva no Reino Unido. Aqui, os incidentes com participantes indiretos do Pix mostraram o que acontece quando o controle sobre terceiros falha. As mais vulneráveis são as indústrias e as pequenas e médias empresas, que têm menos orçamento e menos familiaridade com as exigências regulatórias.

Poucas empresas chegam a esse momento protegidas. No primeiro semestre de 2026, o seguro cibernético movimentou R$ 179,1 milhões no país, alta de 63% sobre o mesmo período de 2025, segundo a CNseg. O mercado cresce rápido, mas parte de uma base pequena. O seguro atua em duas frentes. Antes do ataque, a contratação estabelece requisitos técnicos e critérios mínimos de segurança, o que leva a empresa a corrigir falhas que desconhecia. Depois, a apólice absorve perdas financeiras e amplia a capacidade de resposta, justamente nos dias em que a operação está parada. A Estratégia Nacional de Cibersegurança, atualizada pelo governo federal em agosto de 2025, prevê o estímulo a seguros contra ciberincidentes para serviços essenciais e infraestruturas críticas, mas a adesão ainda é baixa.

Essas campanhas continuam valendo. Falta acrescentar a elas uma conta que muitas empresas ainda não fizeram: quais processos dependem de sistemas digitais e por quantos dias o negócio se mantém sem eles. Quem tem essa resposta consegue decidir quanto investir em prevenção, o que exigir dos fornecedores e quanto do risco transferir a uma seguradora.

Marta Schuh é Diretora de Seguros Cibernéticos e Tecnológicos da Howden Brasil.

Fonte: Ryto, em 10.11.2026