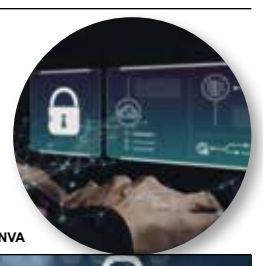

anyaberkut_CANVA

SEGURANÇA DIGITAL

CIBERSEGURANÇA SAI DA SALA DE TI E VIRA O RISCO NÚMERO UM NA AGENDA DOS CEOS

Pela primeira vez, a segurança digital ocupa o topo da lista de preocupações dos principais executivos do país.

Gabriel Pedroso (*)

Na edição mais recente do CEO Outlook, estudo da EY-Parthenon com 50 CEOs de grandes empresas brasileiras de setores como indústria, energia, saúde, consumo e serviços financeiros, as ameaças cibernéticas e a privacidade de dados aparecem como o principal risco de negócio para os próximos 12 meses, apontadas por 26% dos entrevistados, à frente de tensões geopolíticas (16%), incerteza regulatória (14%), rupturas na cadeia de suprimentos (12%) e volatilidade macroeconômica (10%).

O dado marca uma virada: o tema que por décadas foi tratado como assunto técnico, discutido entre a TI e o fornecedor de antivírus, passou a disputar espaço com inflação e câmbio na cabeça de quem decide o rumo das empresas.

A mudança aconteceu porque o custo de ignorá-la ficou visível. Ataques de ransomware que paralisam operações inteiras, vazamentos que destroem reputação construída em décadas e fraudes que atravessam cadeias de fornecedores transformaram a segurança digital em variável de continuidade do negócio.

Quando um incidente é capaz de interromper o faturamento, derrubar o valor de mercado e acionar responsabilidades legais da diretoria, a decisão sobre o quanto investir e o que proteger deixa de caber ao gerente de infraestrutura e sobe, inevitavelmente, para o conselho.

O setor que dita o padrão de maturidade

Se há um setor que mostra como fica uma agenda de segurança tratada como risco de negócio, é o financeiro. A Pesquisa Febraban de Tecnologia Bancária 2026, realizada pela Deloitte com 25 bancos que respondem por cerca de 85% dos ativos da indústria bancária nacional, projeta R$ 50,4 bilhões de investimento em tecnologia neste ano, alta de 8% sobre 2025 e crescimento de 58% no orçamento em cinco anos.

Dentro dessa cifra, a cibersegurança alcançou um patamar que nenhuma outra tecnologia atingiu: 100% das instituições a classificam como prioridade alta ou média, à frente de cloud e inteligência artificial generativa, ambas com 84%.

Divulgação

Gabriel Pedroso

> Quando um incidente é capaz de interromper o faturamento, derrubar o valor de mercado e acionar responsabilidades legais da diretoria, a decisão sobre o quanto investir e o que proteger deixa de caber ao gerente de infraestrutura e sobe, inevitavelmente, para o conselho.

Os bancos brasileiros processaram 240,8 bilhões de transações em 2025, com 78% delas realizadas pelo celular, segundo a mesma pesquisa, e sustentam um sistema de pagamentos instantâneos que funciona sem pausa. Nesse ambiente, segurança não concorre com o negócio, ela é condição para que o negócio exista, e o orçamento reflete essa compreensão sem a resistência que ainda trava a pauta em outros segmentos.

O detalhe menos comentado do levantamento talvez seja o mais instrutivo: mais de 220 mil profissionais do setor foram treinados em tecnologia e cibersegurança no último ano, o que representa praticamente metade do quadro de bancários.

O setor mais maduro do país em defesa digital não aposta apenas em ferramenta, aposta em gente, porque sabe que a porta de entrada da maior parte dos incidentes continua sendo o clique de um colaborador desatento, e não a falha sofisticada de um sistema.

Governança antes da tecnologia

A experiência do setor financeiro sugere que a transição da sala de TI para a agenda do conselho passa menos por comprar mais soluções e mais por estruturar como se decide. Tratada como risco de negócio, a cibersegurança ganha o que qualquer risco relevante tem: dono definido, apetite declarado, métricas acompanhadas pela alta liderança e orçamento defendido em comitê, não disputado nas sobras do budget de infraestrutura.

Esse enquadramento também muda a relação com a resposta a incidentes. Empresas maduras partem do princípio de que o ataque bem-sucedido é questão de tempo, e por isso ensaiam a crise antes de vivê-la, com planos de resposta testados, papéis claros entre tecnologia, jurídico e comunicação e critérios definidos para decisões difíceis, como isolar sistemas ou acionar autoridades.

A diferença entre um incidente absorvido e uma crise devastadora raramente está na ferramenta de detecção, está na velocidade e na ordem das decisões das primeiras horas.

Há ainda a camada dos terceiros, que o setor financeiro aprendeu a levar a sério à força. Episódios recentes envolvendo prestadores de serviço do ecossistema mostraram que a defesa de uma organização vale o elo mais fraco da sua cadeia, e a resposta madura foi estender exigências de segurança a fornecedores, conectar monitoramento e compartilhar inteligência de ameaças.

Prostock-Studio_CANVA

O que podemos aprender com o setor Financeiro

A boa notícia para quem está fora do setor financeiro é que o caminho não precisa ser descoberto, precisa ser adaptado. Elevar o tema ao conselho com um responsável claro, mapear os processos cuja parada fere o negócio, medir a capacidade real de detecção e resposta, treinar as pessoas de forma contínua e estender a régua de segurança aos fornecedores críticos formam uma agenda que independe do porte da empresa e que custa uma fração do que custa o incidente que ela evita.

A pesquisa da EY-Parthenon ainda traz um dado que torna essa agenda ainda mais urgente: 72% dos CEOs brasileiros pretendem ampliar investimentos em inteligência artificial nos próximos meses, e a própria consultoria observa que a aceleração da IA amplia a exposição a riscos de dados, governança e segurança. As empresas estão, ao mesmo tempo, digitalizando o que têm de mais valioso e ampliando a superfície que precisa ser defendida, e são esses motivos que explicam por que o risco cibernético chegou ao topo da lista e não deve sair dela tão cedo.

(*) Head da Selbetti Cybersecurity Solutions.