IT Insight

#58 NOVEMBRO 2025

media NEXT
STAY AHEAD • STAY RELEVANT

REINVENÇÃO EXECUTIVA

DECIDIR, LIDERAR E COMPETIR EM TEMPOS DE IA

POR BRUNO CASTRO,
Fundador & CEO da VisionWare.
Especialista em Cibersegurança e Análise Forense

O QUE TODOS OS LÍDERES DEVEM SABER SOBRE CONTINUIDADE DE NEGÓCIO

O mais recente Microsoft Digital Defense Report (2025) identifica alguns pontos-chave que todos os líderes devem conhecer para proteger os seus ativos, operações e reputação, e que se revelam fundamentais para a resiliência organizacional e continuidade de negócio.

ESTE RELATÓRIO traça um retrato claro: proteger identidades, dados e infraestruturas, é hoje, o fator decisivo para garantir operações resilientes num cenário de ameaças cada vez mais sofisticadas.

A autenticação multifatorial (MFA) continua a ser a medida mais eficaz contra acessos indevidos, ao bloquear mais de 99% das tentativas de intrusão. Mas o relatório é também explícito ao afirmar que já não basta ter MFA, é essencial adotar soluções resistentes a ataques de engenharia social, como o phishing, capazes de evoluir a proteção ao elo mais fraco na cadeia de segurança, o fator humano.

Os cibercriminosos estão também cada vez mais focados em roubo e usurpação de identidades, através do roubo de credenciais que lhes dão acesso direto a dados valiosos que permitem desenvolver ataques mais elaborados e com maior impacto. Setores como o Governo, Administração Pública, Educação, Saúde e Tecnologia, estão entre os mais visados, em

- Bruno Castro -
Fundador & CEO da VisionWare. Especialista em Cibersegurança e Análise Forense

grande parte porque armazenam quantidades massivas de informação de enorme valor para o cibercrime, como dados pessoais ou confidenciais. Quando uma identidade é comprometida, o impacto vai muito além do roubo de dados, já que compromete a confiança, a reputação e, em última instância, a capacidade de continuar a operar, podendo mesmo levar a impacto financeiro irreversível.

Curiosamente, apesar da constante evolução tecnológica, os vetores de ataque continuam a ser os mesmos velhos conhecidos de sempre (phishing, exploração de vulnerabilidades não corrigidas, e ataques de ransomware robotizados); a diferença, é que hoje os cibercriminosos exploram vetores de ataques, assentes em vulnerabilidades conhecidas, mais depressa do que nunca.

O mesmo relatório revela ainda que a maioria dos ciberataques continuam a ser motivados por razões financeiras. Ora, a cibercriminalidade tem vindo a consolidar-se como um modelo de negócio altamente lucrativo, e os dados exfiltrados são frequentemente usados para chantagem ou revenda num mercado "underground" que permite níveis de retorno económico difíceis de acreditar.

Por outro lado, e na perspetiva do pós-ciberataque, cada vez mais os planos de continuidade e recuperação são fundamentais para manter "vivo" o negócio da vítima. Recomendações como incluir cópias de segurança isoladas e imutáveis, mecanismos de deteção precoce a ações suspeitas ou maliciosas, ou procedimentos de resposta e recuperação devidamente testados, são fundamentais para conseguir recuperar a um ciberdesastre. A capacidade de restaurar operações rapidamente, pode fazer toda a diferença entre uma interrupção controlada e uma crise prolongada, que no extremo, pode condicionar a recuperação do negócio e da empresa para o futuro.

A Inteligência Artificial (IA) surge igualmente como um dos grandes temas deste ano. Se, por um lado, potencia a ciberdefesa através do incremento substancial de capacidades de deteção e resposta automatizadas (através de "inteligência"), por outro, também está a ser utilizada pelo cibercrime como multiplicador ao facilitar o desenvolvimento de modelos inovadores de ataques a pessoas através campanhas de phishing altamente convincentes, pela criação de deepfakes e incorporação de contexto personalizado para a vítima.

Por fim, a computação quântica, que embora traga promessas de inovação e progresso, representa também um risco potencial para os sistemas de encriptação que hoje sustentam a segurança digital. A transição para criptografia resistente a quântica, tem de ser planeada agora, como parte da visão de longo prazo para a continuidade e resiliência das organizações. A mensagem é inequívoca: a continuidade de negócio dependerá diretamente da capacidade de se conseguir antecipar, resistir e recuperar perante ciberataques. ■