IT Insight SECURITY

#24 JUNHO 2025

CIBERGUERRA:
O NOVO CAMPO DE BATALHA

visionware

por Bruno Castro, Fundador & CEO da VisionWare.
Especialista em Cibersegurança e Investigação Forense

CYBERWARFARE: UMA AMEAÇA AO QUOTIDIANO EMPRESARIAL

A CIBERGUERRA DEIXOU DE SER UMA REALIDADE CONFINADA AOS ESTADOS E INSTITUIÇÕES MILITARES PARA SE TORNAR UMA PREOCUPAÇÃO CONCRETA E URGENTE TAMBÉM PARA ORGANIZAÇÕES, DADA A CRESCENTE DIGITALIZAÇÃO DOS PROCESSOS ECONÓMICOS E OPERACIONAIS. O CIBERESPAÇO CONSOLIDOU-SE COMO UM NOVO DOMÍNIO DE CONFRONTO ESTRATÉGICO, NO QUAL EMPRESAS PRIVADAS ASSUMEM, MUITAS VEZES SEM O DESEJAREM, UM PAPEL CENTRAL, NÃO APENAS COMO ALVOS, MAS TAMBÉM COMO ELEMENTOS ATIVOS DE DEFESA.

Ao contrário do cibercrime tradicional, a ciberguerra caracteriza-se por campanhas persistentes, altamente sofisticadas e frequentemente atribuídas a atores estatais ou a grupos com capacidades equivalentes. Estas ameaças, muitas vezes APTs (Ameaças Persistentes Avançadas), têm como objetivo comprometer infraestruturas críticas, causar disrupções económicas de larga escala e manipular ou desestabilizar processos de decisão política. Setores como a energia, telecomunicações, finanças e saúde estão entre os principais alvos, tendo em conta as suas funções estruturais e o impacto sistémico que qualquer interrupção pode provocar no normal funcionamento.

Neste contexto, emerge uma componente particularmente preocupante e difícil de combater: o ciberterrorismo. Trata-se da utilização de meios digitais para fins ideológicos ou políticos, através da ameaça, intimidação ou efetiva destruição de ativos digitais e físicos. O ciberterrorismo pode manifestar-se através da sabotagem de sistemas de transporte, hospitais ou redes elétricas, mas

também através da disseminação de desinformação massiva com o intuito de causar pânico, polarização social ou colapsos de confiança nas instituições democráticas.

Esta prática tem vindo a ganhar terreno como instrumento de ciberguerra híbrida, na qual se combinam métodos militares, tecnológicos, económicos e informacionais para atingir objetivos estratégicos sem recorrer a confrontos armados convencionais. Nestes cenários, grupos terroristas, milícias digitais e mesmo agentes estatais recorrem ao ciberespaço para recrutamento e/ou promover campanhas de desestabilização ao explorar vulnerabilidades tecnológicas e sociais. O ciberterrorismo representa, por isso, uma ameaça híbrida e assimétrica: de baixo custo, difícil de atribuir e com elevado potencial de impacto.

As organizações privadas, em particular, as de maior dimensão ou inseridas em setores estratégicos, deixaram de ser meros utilizadores de tecnologia para se tornarem atores centrais na ciberesiliência nacional. Em muitos casos, são as primeiras a detetar sinais de campanhas hostis e a agir sobre


BRUNO CASTRO, VISIONWARE

incidentes com elevado grau de complexidade técnica e impacto operacional.

Torna-se, por isso, imperativo, que os conselhos de administração, os diretores de sistemas de informação e os responsáveis pela cibersegurança compreendam o novo contexto em que operam. A segurança digital deve ser encarada como uma função estratégica, transversal à organização e suportada por políticas robustas, tecnologias adequadas e equipas especializadas.

Adicionalmente, é essencial que as organizações desenvolvam a capacidade de identificar e interpretar indicadores de campanhas de desinformação e manipulação psicológica, frequentemente utilizadas no contexto de ciberterrorismo. A articulação entre equipas de cibersegurança, departamentos de comunicação, recursos humanos e gestão de crise é cada vez mais importante para garantir uma resposta integrada e eficaz.

A realidade é clara: a ciberguerra, com todas as suas vertentes - técnicas, psicológicas, económicas e ideológicas - é um fenómeno em expansão, com impacto direto no tecido económico e social. Preparar as organizações para este novo cenário não é uma opção, é uma exigência estratégica. Investir em ciberesiliência significa proteger ativos, garantir a continuidade do negócio, salvaguardar a reputação institucional e contribuir para a estabilidade digital do país.

Numa Era em que a fronteira entre a guerra digital e o quotidiano empresarial é cada vez mais ténue, a cibersegurança torna-se uma responsabilidade partilhada por todos. ◀