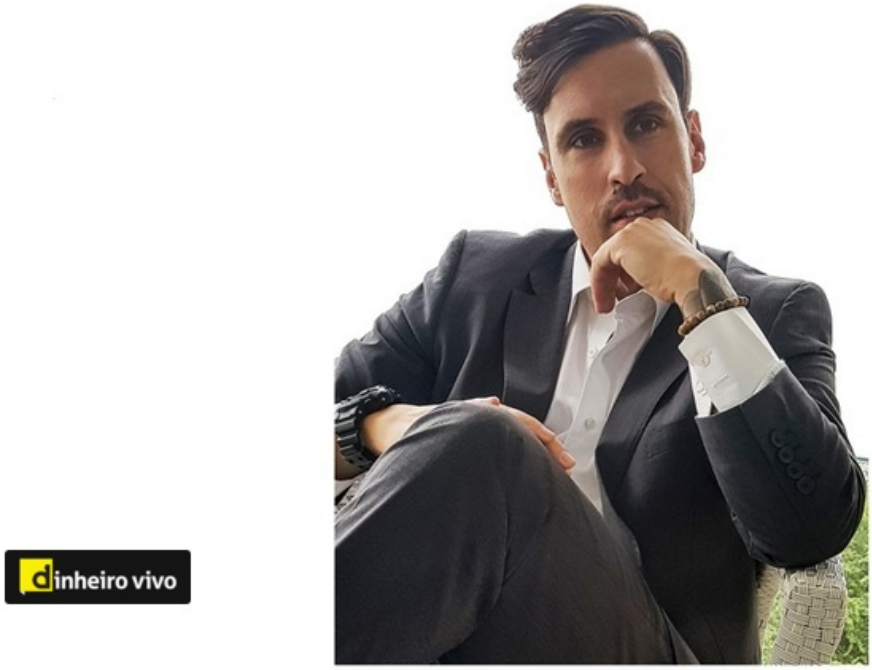
Aviação, infraestruturas críticas e cibersegurança: uma nação vulnerável?

dinheirovivo.pt/opiniao/aviacao-infraestruturas-criticas-e-ciberseguranca-uma-nacao-vulneravel-12806585.html

13 de junho de 2019



A aviação é um setor profundamente ameaçado, tanto em termos físicos quanto lógicos, como aliás demonstrado por trágicos eventos ocorridos nos últimos anos.

Talvez por esse motivo se tenha tornado ainda mais num exemplo de enorme maturidade no que respeita à disciplina de segurança, nomeadamente, quando comparado com setores normalmente considerados como infraestruturas críticas.

Ainda assim, e por razões óbvias, este setor continua a ser alvo de inúmeras ameaças e ataques que se destinam não só à interrupção do seu serviço – o que se traduz em incidentes com enorme visibilidade, capazes de provocar imensa agitação social – mas também no que concerne à segurança física de todas as infraestruturas e serviços que, direta e indiretamente, o rodeiam.

Só neste ano, nos EUA, na UE e no Canadá, no setor da aviação já foram identificados sete ataques cibernéticos a estruturas, o que se torna particularmente preocupante visto que um simples ataque com sucesso, ou até com sucesso residual, pode desencadear um conjunto de consequências dramáticas, pondo em causa a segurança de todas as suas envolvências – humanas, físicas ou tecnológicas. O impacto, obviamente, estende-se à reputação de qualquer organização que esteja envolvida.

Estamos a falar de um setor que depende, em grande medida, de plataformas digitais. Este é, aliás, um aspeto cada vez mais comum e relevante entre prestadores de serviços essenciais ao funcionamento normal de um Estado.

E se um dos setores mais maduros, como é o do transporte aéreo, apresenta vulnerabilidades, que dizer das restantes infraestruturas críticas?

O transporte, a energia, a saúde e a própria administração pública são estruturas que não se podem dar ao luxo de ficar indisponíveis nem de ver de alguma maneira posta em causa a segurança da sua atividade – quer se trate dos seus colaboradores, de clientes ou até da população em geral, sob pena de desencadear uma crise capaz de abalar uma nação inteira.

A facilidade, a economia e a eficácia com que o cibercrime pode ser praticado faz com que a criticidade de um incidente desse tipo aumente exponencialmente. Afinal, atacar uma infraestrutura crítica tem sempre impacto, mas preparar um ataque físico implica, em relação aos ataques lógicos, riscos bastante superiores. Já através de um ataque cibernético, pode criar-se o caos, estando a milhares de quilómetros da estrutura atacada.

Veja-se o que aconteceu no passado dia 7 de maio, na cidade de Baltimore (EUA): pela segunda vez neste ano, um vírus – da categoria de *ransomware* – espalhou-se por grande parte dos sistemas tecnológicos da cidade, o que obrigou a que a maioria dos servidores tivesse de ser desligada apenas por precaução. A linha de apoio ao cliente e o departamento de transportes foram afetados. Os residentes de Baltimore, mas também os não residentes que tinham negócios com a cidade, foram afetados. As pessoas não conseguiram pagar as contas, incorrendo em risco de incumprimento. Os funcionários foram mandados mais cedo para casa pois não podiam trabalhar. Um mês depois, a cidade ainda não recuperou do ataque.

Este exemplo é apenas uma pequena amostra do potencial catastrófico que um ataque aos serviços essenciais pode representar. Aviões podem ser desviados ou remotamente controlados, assim como qualquer outro meio de transporte; o acesso a bens de primeira necessidade pode ser cortado e o mesmo se diga em relação às linhas telefónicas da polícia, dos bombeiros e de emergência médica; na verdade, qualquer dispositivo conectado pode ser manipulado para não funcionar devidamente e contribuir para criar o caos.

O Regime Jurídico da Segurança do Ciberespaço, publicado no início do ano, estabelece que a **Administração Pública**, os **Operadores de Infraestruturas Críticas** ou de **Serviços Essenciais**, **Prestador de Serviços Digitais** ou **qualquer outra entidade que utilize Redes e Sistemas de Informação** devem adaptar os seus comportamentos organizacionais, tornando-os mais seguros, sob pena de, por negligência, infração grave ou muito grave, serem muitíssimo penalizados. Em causa está o estrito cumprimento de um conjunto de requisitos de segurança e normalização, assente nas boas práticas do setor, assim como a necessidade de notificação - obrigatória e voluntária - de eventuais incidentes à Autoridade de Controlo competente (CNSC). Estes requisitos correspondem a um conjunto de medidas técnicas e organizativas adequadas e proporcionais aos riscos de segurança das redes e dos sistemas de informação utilizados, capazes de estabelecer um nível de segurança adequado ao risco em causa e minimizar o seu impacto.

É a pensar neste tipo de ameaças tão complexas quanto difíceis de identificar que a VisionWare tem colaborado, cada vez mais, com as referidas infraestruturas críticas. Sem monitorização constante, treino e implementação de boas práticas, não se estará apto para responder aos desafios da era digital. Afinal, e como em tudo o resto, a exposição e as ameaças cibernéticas às organizações identificadas como infraestruturas críticas, começa a partir do momento em que se passa a estar conectado ao mundo cibernauta.

Bruno Castro é CEO da VisionWare