AVSECCEA

JULHO, 2025

BOLETIM INFORMATIVO

Qantas sofre cyber ataque e tem dados de 5,7 milhões de clientes vazados

A companhia aérea australiana Qantas confirmou que 5,7 milhões de registros de clientes foram comprometidos em um ataque cibernético recente. A violação ocorreu por meio de engenharia social aplicada a um call center terceirizado da empresa, sem envolvimento direto com os sistemas internos da Qantas.

- **Os criminosos usaram técnicas de vishing (fraude por telefone) para enganar funcionários e obter acesso a informações como:**
  - Nomes completos
  - Números de passageiro frequente (frequent flyer)
  - Endereços de e-mail e histórico de voos

A empresa afirma que dados financeiros e passaportes não foram comprometidos, mas o incidente reforça como falhas humanas em parceiros e fornecedores ainda representam ponto crítico de risco cibernético na aviação.

O FBI e grandes empresas de cibersegurança (Google, Palo Alto Networks) emitiram um alerta conjunto sobre o aumento de ataques a companhias aéreas por parte do grupo hacker conhecido como Scattered Spider (também chamado Muddled Libra).
Esse grupo tem como alvo:

- Companhias como Hawaiian Airlines e WestJet
- Sistemas de suporte e help desks
- Parceiros terceirizados e redes com autenticação fraca

A tática mais comum envolve acesso inicial por engenharia social, seguido por elevação de privilégios e comprometimento de sistemas críticos.

A ameaça agora não se limita ao que é visível ou físico. A segurança cibernética se tornou uma nova fronteira da AVSEC, onde a falha de um simples atendimento terceirizado pode abrir as portas para o colapso de todo o sistema.
No Brasil, a crescente dependência digital nos aeroportos – check-in eletrônico, despacho automatizado, redes de CFTV conectadas à nuvem, sistemas de vigilância remota, aplicativos internos de coordenação – expõe o setor a riscos muito além do que a cerca e o raio-x podem conter.

Da teoria à prática: onde estão os riscos no Brasil?

- Infraestrutura terceirizada: muitos aeroportos dependem de empresas externas para TI, CFTV, controle de acesso e bilhetagem.
- Sistemas legados: aeroportos regionais operam com softwares desatualizados, sem criptografia nem atualizações de segurança.
- Conectividade frágil: redes Wi-Fi abertas, senhas genéricas e usuários com privilégios amplos em estações compartilhadas.
- Ausência de treinamentos específicos: enquanto o efetivo AVSEC treina contra explosivos e invasões, poucos são capacitados para reconhecer sinais de comprometimento cibernético (como lentidão anormal de sistemas, acessos fora de horário, e-mails de phishing).

A segurança do voo começa muito antes da decolagem – e, hoje, também passa pelos servidores.

É hora de integrar a segurança física com a lógica, de capacitar o efetivo AVSEC para reconhecer ameaças cibernéticas e de implementar planos de resposta eficazes para situações em que o “agente ilícito” não tem rosto, mas sim IP.

Sua organização está preparada para um incidente cibernético?

- Seus sistemas críticos têm autenticação multifatorial e segmentação de acesso?
- Como são treinados os funcionários terceirizados que operam sistemas com acesso remoto ou suporte técnico?
- Existe um protocolo AVSEC em caso de pane sistêmica de origem suspeita?
- Em um eventual vazamento de dados ou informações operacionais, qual seria o plano de resposta e comunicação da sua unidade?
- A segurança física (acesso, vigilância, contingência) está integrada com a segurança da informação?
- Existe monitoramento ativo e contínuo dos acessos aos sistemas sensíveis do aeroporto?

O elo mais fraco não é a cerca – é o colaborador mal orientado. E fortalecer esse elo é a nova missão da Segurança AVSEC.

FONTE: https://www.reuters.com/world/asia-pacific/qantas-confirms-over-million-customers-personal-information-leaked-2025-07-09/