António Costa, diretores do SIS e da GNR e deputados com dados expostos

Em agosto, após o ciberataque, a TAP garantia que não tinha havido acesso indevido a dados de clientes

Informações sobre números de telemóveis, moradas e *e-mails* de políticos como António Costa ou André Ventura e dos líderes de forças e serviços de segurança, como Neiva da Cruz (SIS) e Rui Clero (GNR), constam na lista publicada na *dark web* pelos *hackers* que atacaram a TAP. P7


FOTO JOSÉ CARIA

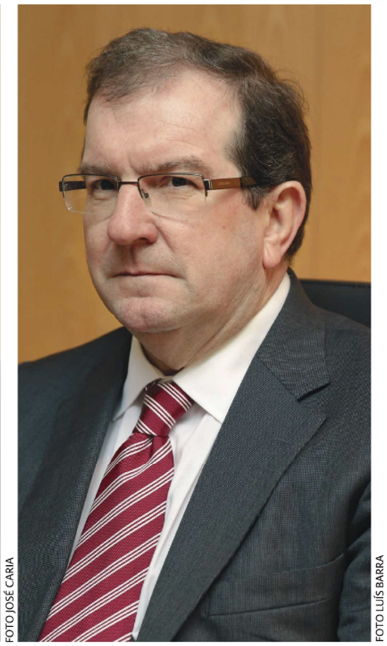
FOTO LUÍS BARRA

António Costa e Neiva da Cruz estão na lista publicada na *dark web* dos *hackers* que atacaram a TAP

Ciberataque Deputados, membros do Governo e altos responsáveis das forças e serviços de segurança foram também alvo dos piratas informáticos. Especialistas apontam o dedo à TAP

Costa e chefe do SIS com dados expostos

HUGO FRANCO

Os dados pessoais do primeiro-ministro, António Costa, do diretor do Serviço de Informações de Segurança (SIS), Adélio Neiva da Cruz, do comandante-geral da GNR, Rui Clero, e do líder do Chega, André Ventura, foram expostos na *dark web* pelo grupo de *hackers* Ragnar Locker, que atacou os servidores da TAP. No caso de Costa, ficou pública uma morada antiga, mas não o número de telemóvel, apenas o *e-mail* de uma colaboradora do seu gabinete, ao contrário de Ventura, que viu o seu número pessoal e *e-mail* expostos, mas não o endereço de casa. Quanto a Neiva da Cruz e Rui Clero, ficaram à vista a morada, o número de telemóvel e o *e-mail*.

Da lista — que não chegará aos 1,5 milhões de clientes da companhia aérea já anunciados, uma vez que há muitos nomes repetidos — constam também os dados de deputados e ex-deputados, como Edite Estrela, Jamila Madeira, Joana Mortágua, José Cesário, José Silvano, Paulo Portas, Alexandre Quintanilha ou Susana Amador. O Expresso sabe que há ainda uma lista com 294 *e-mails* expostos com o domínio gov.pt.

Os especialistas que falaram ao Expresso são unânimes em isentar os altos responsáveis do Estado de qualquer culpa, apontando exclusivamente o dedo à transportadora portuguesa pela falha de segurança. "Estas pessoas falharam? Não. Confiaram na TAP e a culpa não é delas que o seu nome, morada, *e-mail* e telefone tenham sido tornados públicos pelos *hackers*. A culpa é da empresa, que não soube proteger os dados. A única culpa deles é terem confiado na TAP quando se inscreveram como clientes. Esta é uma quebra irreparável de confiança por parte da TAP", defende Hugo Costeira, presidente do Observatório de Segurança Interna. "Não deve haver um regime especial de segurança para estes altos funcionários do Estado, pois é algo que pode ser interpretado pelos cidadãos comuns como sendo um privilégio a que todos deveriam ter direito. Na verdade, estes altos responsáveis podem agora alterar o seu número de telemóvel exposto pelos *hackers*. E, se houver necessidade, os serviços de informações podem fazer facilmente uma análise de risco às suas pessoas."

Também Bruno Castro, especialista em cibersegurança e CEO da VisionWare, salienta que "qualquer pessoa, mesmo um alto quadro político ou das forças de segurança, é obrigada a preencher os seus dados pessoais como cliente da TAP ou de qualquer outra companhia aérea". E, na sua ótica, a TAP é que, pela responsabilidade que tem no circuito, deveria ter implementado medidas adicionais de segurança para proteger os dados pessoais dos clientes. "Já para não falar da sua própria infraestrutura interna, que assumimos que foi igualmente comprometida. Por exemplo, permitir que os dados de reserva tivessem caído nas mãos dos cibercriminosos, como é o caso, é uma questão muito sensível e pode implicar a segurança dos próprios passageiros."

"NÃO FOI APURADO QUALQUER FACTO QUE PERMITA CONCLUIR TER HAVIDO ACESSO INDEVIDO A DADOS DE CLIENTES", DISSE A TAP EM AGOSTO

Um responsável em cibersegurança, que está a analisar os dados publicados pelo Ragnar Locker e que falou no anonimato, criticou a falta de rapidez da TAP na admissão de que dados de clientes tinham sido comprometidos. "Os *hackers* podem não ter causado qualquer dano às operações, apesar do sistema de reservas da empresa continuar a funcionar com bastantes problemas, mas causaram um dano irreparável às pessoas que foram expostas devido a este ataque."

Alertas para *phishing*

Esta semana, num novo comunicado, a TAP revelou que as categorias de dados pessoais expostos podem ser o nome, nacionalidade, sexo, data de nascimento, morada, *e-mail*, contacto telefónico, data de registo de cliente e número de passageiro frequente. E pediu aos clientes que alterassem as senhas do serviço Miles&Go, alertando mesmo para possíveis burlas. "A divulgação de dados pessoais através de fontes abertas pode aumentar o risco da sua utilização ilegítima, nomeadamente com o objetivo de obter outros dados que possam comprometer os sistemas digitais para perpetrar fraudes (*phishing*)." E garantiu: "Todos os sistemas afetados foram isolados e procedeu-se à limpeza desses sistemas. A boa notícia é que as operações da TAP nunca foram afetadas — todas as operações da TAP estão a decorrer em segurança."

Recorde-se que no primeiro comunicado, no final de agosto, logo após o anúncio do ciberataque, a transportadora aérea garantia: "Não foi apurado qualquer facto que permita concluir ter havido acesso indevido a dados de clientes."

O Ministério Público abriu um inquérito ao ciberataque, que está a ser acompanhado desde o primeiro momento pela PJ e Centro Nacional de Cibersegurança.

hfranco@expresso.impresa.pt