



(Tradução)

**Assunto: Interpelação escrita apresentada pelo Deputado à Assembleia Legislativa, Lam U Tou**

Na sequência da interpelação escrita apresentada pelo Deputado Lam U Tou, no dia 29 de Dezembro de 2022, enviada a coberto do ofício n.º 023/E12/VII/GPAL/2023 da Assembleia Legislativa, de 12 de Janeiro de 2023, e recebida pelo Gabinete do Chefe do Executivo a 13 de Janeiro de 2023, após auscultar os pareceres da Polícia Judiciária (PJ) e da Direcção dos Serviços de Administração e Função Pública (SAFP), cumpre a este Gabinete apresentar a seguinte resposta:

No que concerne ao ponto 1 da interpelação, o Centro de Alerta e Resposta a Incidentes de Cibersegurança (CARIC) depois de lhe ter sido comunicada a ocorrência de uma falha no sistema de node network do Aliyun (Alibaba Cloud) de Hong Kong, que interrompeu o acesso e o uso dos websites de certas infra-estruturas críticas locais, contactou imediatamente, por meio do actual mecanismo de cibersegurança, os operadores das infra-estruturas críticas para responderem e acompanharem o referido incidente, bem como divulgou, junto do público, através dos media as informações sobre o incidente. As entidades envolvidas, por sua iniciativa, aplicaram as devidas medidas de protecção e efectuaram o trabalho de resposta à emergência, entre as quais, as que estão sujeitas às obrigações nos termos da Lei da cibersegurança, e comunicaram a tempo com o CARIC, de acordo com as respectivas normas técnicas estipuladas, apresentando pormenorizadamente a área afectada pelo incidente, o grau de dano e as medidas de acompanhamento para recuperação. As disposições de prevenção adoptadas e a execução do plano de contingência correspondem às exigências das respectivas normas técnicas solicitadas pelas autoridades. No decorrer do incidente, o CARIC não recebeu nenhum pedido de apoio das entidades envolvidas, de operadores de infra-estruturas críticas, nem das suas entidades de supervisão.



澳門特別行政區政府  
Governo da Região Administrativa Especial de Macau  
保安司司長辦公室  
Gabinete do Secretário para a Segurança

(Tradução)

Segundo as informações recolhidas, o incidente foi causado por uma falha no sistema de rede no exterior e não por um ataque cibernético. Foram afectados por este incidente 6 operadores de infra-estruturas críticas e algumas entidades privadas que não estão sujeitas a obrigações nos termos da Lei da cibersegurança. A duração da emergência variou de caso para caso, e envolveu sobretudo os serviços prestados pelos operadores através da rede, mas não afectou as actividades sujeitas à supervisão nos termos da Lei da cibersegurança, nem causou qualquer consequência negativa, como a fuga de dados pessoais. Os SAEP informaram ainda que a “Conta Única de Macau” não foi afectada por este incidente.

O CARIC e os operadores de infra-estruturas críticas, através do actual mecanismo de cibersegurança, responderam de modo eficaz a este incidente. No futuro, o Governo da RAEM irá rever oportunamente a Lei da cibersegurança e as respectivas normas técnicas implementadas, de acordo com o desenvolvimento da economia e das indústrias de Macau e, caso seja necessário, irá efectuar alterações para que haja um melhoramento, no sentido de emitir orientações, promoção e apoio mais eficazes aos operadores de infra-estruturas críticas, para que estes continuem a melhorar o trabalho relativo à cibersegurança.

No que diz respeito ao ponto 2 da interpelação, com a entrada em vigor da Lei da cibersegurança, o CARIC e as entidades de supervisão, de acordo com a lei, devem ter uma visão anual sobre o cumprimento dos deveres dos operadores de infra-estruturas críticas na gestão da cibersegurança e na área técnica, pelo que é elaborado anualmente o Relatório Geral de Cibersegurança, que é submetido à Comissão para a Cibersegurança para apreciação e que serve, assim, de referência para o Governo da RAEM na definição de objectivos e estratégias da fase seguinte de trabalho no âmbito da cibersegurança. De um modo geral, os operadores públicos e privados estabeleceram um regime de gestão da cibersegurança e respectivos procedimentos operacionais internos, e melhoram de forma contínua os planos sobre cibersegurança.



澳門特別行政區政府  
Governo da Região Administrativa Especial de Macau  
保安司司長辦公室  
Gabinete do Secretário para a Segurança

(Tradução)

Relativamente à situação da implementação das medidas técnicas, os requisitos das respectivas normas técnicas, em geral, foram cumpridos.

No que diz respeito ao ponto 3 da interpelação, os SAEP afirmaram que o Governo da RAEM está empenhado em reforçar o nível de protecção da cibersegurança e de resposta dos serviços públicos, e através da infra-estrutura do Centro de Computação em Nuvem, concluída e em funcionamento desde 2019, dispõe de condições de gestão concentrada para fornecer redes, servidores, armazenamento de dados e uma plataforma de gestão, o que proporciona recursos em rede e ambiente operacional básico seguros e estáveis para os diversos serviços usarem de forma exclusiva e independente, bem como para desenvolverem diferentes serviços electrónicos e aplicações inteligentes, nomeadamente o funcionamento da plataforma “Conta Única de Macau”. Quanto ao funcionamento quotidiano dos serviços públicos, o sistema está munido de segurança na respectiva plataforma do Centro de Computação em Nuvem, onde foi implementado um regime de gestão seguro que dispõe de uma equipa especializada para uma vigilância 7x24, de forma a garantir que o sistema electrónico e os dados possam funcionar num ambiente seguro e estável.

Em relação ao sector privado, os operadores privados de infra-estruturas críticas estão sujeitos ao cumprimento dos deveres de cibersegurança estabelecidos na Lei da cibersegurança. Contudo, esses operadores, de acordo com o seu próprio ramo de actividade e decisão comercial, podem optar por escolher no mercado operadores de serviços de rede, tecnologia e equipamentos adequados, de modo a construírem a estrutura do sistema de informações de rede e uma forma de funcionamento próprias, tudo de acordo com a lei e a regulamentação técnica.

A Chefe do Gabinete do Secretário para a Segurança

Cheong Ioc Ieng

1 de Fevereiro de 2023