Divulgação de normas técnicas universais para clarificar os deveres e requisitos de cibersegurança

Com a entrada em vigor da Lei n.º 13/2019 (Lei da cibersegurança), em 22 de Dezembro de 2019, foi estabelecida a base jurídica para a criação do sistema de gestão preventiva da cibersegurança da RAEM. É claramente previsto na lei um conjunto de deveres e responsabilidades dos operadores de infra-estruturas críticas para assegurar a sua própria situação de cibersegurança, tais como: a designação de um responsável pela cibersegurança; o estabelecimento de um regime de gestão e respectivos procedimentos operacionais; e a adopção de medidas de prevenção, revisão, e resposta a incidentes de cibersegurança. Porém, face ao rápido desenvolvimento das tecnologias informáticas, os operadores devem oportunamente actualizar e ajustar, conforme as diferentes situações, os mecanismos de defesa e protecção e as medidas técnicas necessários. Assim, com observância do princípio da proporcionalidade, o Governo da RAEM não regula directamente, nesta lei-quadro fundamental (Lei da cibersegurança), o funcionamento concreto e os requisitos técnicos relativos ao cumprimento dos deveres de cibersegurança por parte dos operadores, emitindo apenas as normas técnicas vinculativas para estes os definirem.

I. De acordo com a realidade concreta de Macau, concentram-se as melhores soluções para a elaboração das normas técnicas

Com o intuito de clarificar a nível técnico, as medidas concretas a serem tomadas pelos operadores de infra-estruturas críticas no cumprimento dos deveres impostos pela lei e nas acções a desenvolver no âmbito da cibersegurança e, ainda, para proporcionar às entidades de supervisão os fundamentos para a definição, das normas técnicas exclusivas dos sectores correspondentes, o Centro de Alerta e Resposta a Incidentes de Cibersegurança (CARIC), composto por PJ, SAFP e CTT, nos termos do artigo 3.º da "Lei da cibersegurança", desde meados de 2018 começou a elaborar a "Regulação de padrões de gestão da cibersegurança" e a "Regulação de alerta, resposta e comunicação de incidentes de cibersegurança", duas normas técnicas universais do âmbito da cibersegurança aplicáveis a operadores de diversos sectores e domínios. Atenta a realidade concreta de Macau, e levando em consideração as diferenças de contexto entre empresas chinesas e estrangeiras, tomando, também, como referência os regimes de protecção de diferentes níveis existentes no interior da China, bem como a certificação internacional de gestão de cibersegurança ISO/IEC27001, ponderando, ainda os regimes do mesmo tipo aplicados nos países/regiões vizinhas, depois de termos ouvido 2 vezes as opiniões das entidades de supervisão e dos operadores, procedemos à revisão e ao aperfeiçoamento desta matéria. Assim, estas duas normas técnicas foram publicadas no Boletim Oficial da RAEM, no dia 13 de Maio deste ano, entrando efectivamente em vigor no dia seguinte (dia 14).

II. Conteúdo principal da "Regulação de padrões de gestão da cibersegurança"

A “Regulação de padrões de gestão da cibersegurança” visa estabelecer os requisitos mínimos no âmbito de regime de gestão, de procedimentos operacionais, medidas de segurança, determinação de nível, e avaliação de riscos, no que diz respeito à gestão da cibersegurança e funcionamento diário dos operadores de infra-estruturas críticas. O conteúdo principal consiste em exigir que os operadores avaliem os níveis de protecção da cibersegurança do sistema e implementem as medidas necessárias consoante os diversos níveis de protecção, de acordo com a importância das redes de informações e do sistema informático para o funcionamento normal da sociedade e a protecção dos legítimos direitos e interesses dos cidadãos. Conforme os níveis de protecção do sistema, os operadores devem implementar especificações de protecção de segurança a diferentes níveis nos seis domínios abrangidos, nomeadamente: gestão da criação da segurança; gestão da segurança de operação e manutenção; segurança física e ambiental; segurança da rede e da comunicação; segurança do servidor; e segurança da aplicação e das informações dos dados informáticos. Por exemplo, o sistema classificado como “nível moderado” tem que satisfazer um total de 46 requisitos para as medidas de protecção, enquanto o sistema classificado como “nível alto” tem que satisfazer 130 requisitos no total. Deste modo, orientam-se os operadores na distribuição dos vários tipos de recursos de forma razoável para onde é necessário, atingindo assim os objectivos tanto de implementar diversos níveis de protecção conforme as necessidades como de haver uma boa gestão e controlo de risco.

III. Conteúdo principal da “Regulação de alerta,

resposta e comunicação de incidentes de cibersegurança”

A “Regulação de alerta, resposta e comunicação de incidentes de cibersegurança” visa estabelecer um mecanismo de coordenação e comunicação bidireccional acerca dos alertas e notificações de incidentes emitidos e recebidos, entre o CARIC, as entidades de supervisão e os operadores, bem como fornecer as orientações gerais para a prevenção e resposta a esses incidentes. O CARIC é responsável pela recolha, através de canais diferentes e análise das informações relativas aos riscos e ameaças de cibersegurança, bem como pela emissão de alertas e sugestões de tratamento aos operadores e pela colaboração com eles na prevenção da ocorrência de incidentes. Se houver um acontecimento neste sentido, os operadores devem classificar o nível do incidente de cibersegurança, sobretudo conforme a sua natureza e o impacto causado para a comunidade e a população em geral, comunicando ao CARIC e às entidades de supervisão os detalhes do incidente no prazo a ser fixado consoante o grau de gravidade, e ainda relatando regularmente o andamento dos trabalhos de resposta ao mesmo incidente. Assim, o Governo da RAEM poderá conhecer de forma atempada as informações mais actualizadas, a fim de coordenar o tratamento do incidente e prestar o apoio e a assistência adequada, em caso de necessidade, no sentido de minimizar o mais possível eventuais danos provocados para a sociedade e os cidadãos. A par disso, os operadores, após concluído o trabalho de resposta ao incidente, devem apresentar à respectiva entidade de supervisão o relatório final sobre aquele incidente e o plano de melhoramento, de modo a evitar a repetição de

acontecimentos semelhantes.

IV. Melhoramento contínuo da capacidade de defesa da cibersegurança de Macau

As duas normas técnicas acima referidas, que traduzem os fundamentos básicos da tomada de medidas concretas e da realização de diversas actividades relativas à cibersegurança no cumprimento dos deveres da Lei da cibersegurança, fornecem aos operadores as instruções adequadas à criação de um regime de gestão da cibersegurança, envolvendo o planeamento antecipado, a execução durante a ocorrência do incidente e a revisão e melhoramento após o incidente, com vista a aumentar gradualmente o nível de gestão da cibersegurança. Com a implementação conjugada da Lei da cibersegurança e das duas normas técnicas referidas, poderemos melhorar constantemente a capacidade global de defesa da cibersegurança em Macau, e prevenir eficazmente eventuais riscos nesse âmbito, bem como garantir o funcionamento normal e seguro das redes e sistemas informáticos das infra-estruturas críticas e a prestação contínua dos serviços.