Trabalhar juntos para salvaguardar a cibersegurança

Com o rápido desenvolvimento da internet, a cibersegurança tornou-se uma parte importante da segurança nacional. Sem cibersegurança, não haverá segurança nacional; sem cibersegurança, não haverá desenvolvimento estável quer na economia quer na comunidade; sem cibersegurança, será difícil garantir os interesses vitais da população.

Alta ocorrência de ataques cibernéticos em todo o mundo e ameaça para os interesses da segurança

À medida que a internet se torna cada vez mais popular e uma parte inseparável da vida das pessoas, os problemas de cibersegurança tornam-se cada vez mais proeminentes. Vários tipos de actividades ilegais e criminais, tais como invasão e ataque cibernéticos, burla cibernética, subtracção de segredos cibernética, extorsão cibernética, ocorrem com frequência em todo o mundo, pelo que a situação de cibersegurança está a tornar-se cada vez mais complicada. Em Maio deste ano, ocorreram vários ataques cibernéticos de grande envergadura em todo o mundo, fazendo soar novamente o alarme de cibersegurança: o fornecedor de serviços de internet belga Belnet Network foi vítima de um ataque massivo de negação de serviço distribuído (DDoS) em 4 de Maio, que causou uma parálise massiva das redes de mais de 200 entidades governamentais e instituições académicas, incluindo o parlamento, tribunais, agência tributária nacional, entre outros; a maior operadora de oleodutos americana Colonial Pipeline foi atacada em 7 de Maio, por meio de ransomware que obrigou a fechar a sua rede crítica de abastecimento de

combustível da Costa Leste dos EUA; o sistema Health Service Executive, da Irlanda, foi atacado através do ransomware Conti em 14 de Maio, o que provocou um amplo dano a este sistema nacional e a inacessibilidade dos sistemas electrónicos de vários hospitais.

Neste contexto de severa situação, em que vários países têm sucessivamente sofridos ataques cibernéticos, Macau não pode ficar imune. Ao longo deste ano, os sistemas informáticos das infra-estruturas críticas de alguns serviços públicos e privados, em Macau, sofreram ataques de DDoS em grande escala e alguns sistemas até pararam de funcionar. Estes incidentes deram a possibilidade de perceber que a cibersegurança não somente está relacionada com a segurança nacional e local, como também com a nossa vida quotidiana. Nesta era de internet, ninguém pode ficar sem internet, quer seja organização ou indivíduo particular; todos poderão ser verdadeiramente ameaçados pelo crime cibernético. Por conseguinte, a salvaguarda de cibersegurança é tarefa de serviços, empresas e cidadãos e também responsabilidade de toda a comunidade, sendo necessário que toda a população colabore e assuma as suas responsabilidades.

Assumir as próprias responsabilidades e reforçar a protecção para construir juntos uma linha sólida de defesa de cibersegurança

A elaboração rigorosa e a implementação gradual da Lei da Cibersegurança demonstram a determinação, a responsabilidade e a autuação do Governo da RAEM e das autoridades de segurança no âmbito da salvaguarda de cibersegurança. Contudo, a entrada em vigor desta lei e a criação do Centro de Alerta e Resposta a Incidentes de Cibersegurança (CARIC) não implicam que os ataques cibernéticos não

mais aconteçam, que o espaço cibernético se tornará pacífico e que os utentes das redes não precisarão de preocupar-se. Pelo contrário, com a integração mais profunda entre a internet e a sociedade, o desenvolvimento económico e a vida humana, e ainda, a complexidade desse género de crimes, os riscos de cibersegurança não estão a diminuir, mas sim a aumentar gradualmente, e a espalhar-se rapidamente por diversas áreas de segurança da sociedade, país e regiões. Por isso, em termos de salvaguarda de cibersegurança, não se pode baixar a guarda, nem se pode depender apenas do esforço do Governo. Cada empresa e cada indivíduo devem, quando fruem das facilidades trazidas pelo uso da rede, dar importância às suas próprias responsabilidades e assumi-las, conhecendo os riscos de cibersegurança, melhorando o sentido de segurança, reforçando a protecção neste âmbito, construindo juntos uma linha de defesa de cibersegurança.

Em primeiro lugar, todos os intervenientes do sistema de gestão de cibersegurança devem cooperar e desempenhar as suas funções próprias. A Comissão para a Cibersegurança orienta o desenvolvimento geral de cibersegurança de Macau, proporcionando as garantias necessárias às políticas pertinentes, supervisionando o funcionamento ordenado e regular do sistema de cibersegurança. O CARIC, enquanto estrutura de natureza técnica especializada em matéria de prevenção e resposta a incidentes, irá continuar a melhorar o seu trabalho em termos de alertar sobre os riscos, intervir e coordenar quando há incidentes e dar apoio administrativo e técnico, mantendo-se também em estreita cooperação com a Divisão de Investigação de Crimes Informáticos e Divisão de Informática Forense, da Polícia Judiciária, no sentido de

aperfeiçoar a capacidade de prevenção e combate ao crime cibernético. A par disso, as entidades de supervisão das diversas áreas e sectores irão monitorar e promover o cumprimento dos deveres legais dos operadores das infra-estruturas críticas, protegendo o funcionamento seguro e estável de vários sistemas cibernéticos importantes.

Em segundo lugar, os operadores das infra-estruturas críticas, que prestam vários tipos de serviços fundamentais das redes e susceptíveis de enfrentar diversos ataques cibernéticos, desempenham sempre um papel importante e assumem também responsabilidades indispensáveis. Os operadores devem colaborar com as entidades de supervisão, cumprir com firmeza os deveres previstos na lei, incluindo “deveres de carácter orgânico”, “deveres de carácter procedimental, preventivo e reactivo”, “deveres de auto-avaliação e relato” e “dever de colaboração”, satisfazer plenamente os requisitos legais e técnicos, reforçar as medidas de protecção do sistema cibernético, bem como aumentar o nível de gestão e a tecnologia de cibersegurança, a fim de que a segurança das redes de Macau seja eficazmente protegida.

Por fim, considerando que em todos os lugares da internet há “manipuladores do mal nos bastidores” e “vírus”, para a protecção de cibersegurança, a par das partes intervenientes do sistema de gestão de cibersegurança e dos operadores, necessitamos ainda da participação de outras organizações da sociedade e dos numerosos internautas, melhorando o seu sentido de legalidade e de cibersegurança e de aprendizagem de técnicas indispensáveis de identificação e protecção contra os riscos cibernéticos. Quando cada organização e internauta na sociedade tiver em mente a protecção de

cibersegurança e considerar como própria essa responsabilidade, concretizando-a em acções, constituirá uma pedra fundamental ampla e firme em relação à cibersegurança.

Actualmente, a Lei da Cibersegurança está plenamente implementada e o sistema de cibersegurança está a ser estabelecido de forma ordenada, devendo todas as partes intervenientes acumular experiências e aperfeiçoar, de forma gradual, o respectivo trabalho. Com a liderança e supervisão da Comissão, o CARIC irá, com base no princípio de “quem opera, quem se responsabiliza”, continuar a colaborar estreitamente com as entidades de supervisão e todos os sectores da sociedade para fazer um bom trabalho no âmbito do alerta antecipado do incidente e da resposta durante a ocorrência do incidente e da investigação após o incidente, para ajudar, por iniciativa própria, os operadores na resposta aos diversos tipos de riscos de cibersegurança e prestar-lhes apoio técnico, bem como apoiar os operadores no sentido de estes se empenharem no trabalho de protecção de cibersegurança, de modo a podermos elevar o nível geral de gestão de cibersegurança de Macau, construindo assim, juntos, uma linha de defesa sólida para salvaguardar a cibersegurança.