Construir em conjunto uma sólida linha de defesa para a cibersegurança de Macau

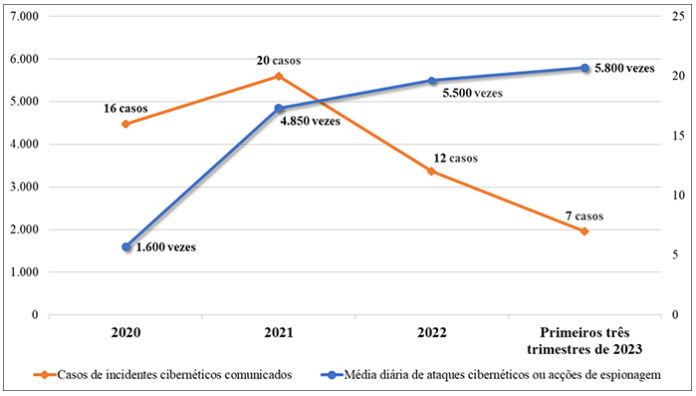
A Lei da cibersegurança entrou em vigor há quase quatro anos, e sob a coordenação e organização da Comissão para a Cibersegurança (CPC), o Centro de Alerta e Resposta a Incidentes de Cibersegurança (CARIC), as entidades de supervisão e os operadores das infra-estruturas críticas dos vários sectores têm trabalhado de forma concertada e, implementando os diversos projectos de cibersegurança de forma ordenada, cada um assume as suas funções, tendo como objectivo comum a construção de uma sólida linha de defesa para a cibersegurança de Macau. Actualmente, o sistema de cibersegurança de Macau tem tido um bom nível de funcionamento, a consciencialização da responsabilidade de todos os participantes em relação a este tema melhorou significativamente, a gestão e a capacidade técnica continuam a melhorar, e consequentemente e de um modo geral, tem demonstrado uma tendência positiva de desenvolvimento gradual. No entanto, o trabalho neste âmbito ainda enfrenta grandes desafios, e os operadores ainda enfrentam habitualmente, a nível técnico, uma série de ameaças de segurança relevantes, e por esta razão, todas as partes devem manter a cooperação no trabalho em equipa, sendo também necessários o apoio e a participação de todos os sectores da sociedade, para melhorar ainda mais o nível geral da cibersegurança de Macau.

I. Melhoria significativa do nível de controlo da gestão de riscos

Conforme os dados do CARIC, o número de ataques cibernéticos e de acções de espionagem às infra-estruturas críticas de Macau tem vindo a aumentar anualmente, e a média diária que em 2020 era de

1.850 vezes (cerca de 1,3 vezes por minuto) aumentou drasticamente para 5.800 vezes nos primeiros três trimestres do corrente ano (cerca de 4 vezes por minuto). Apesar disso, o número de incidentes causados por ataques cibernéticos aos operadores não aumentou da mesma forma, mas sim verificou-se uma tendência visível de abrandamento, com uma diminuição significativa de 40%, passando de 20 casos em 2021 para um total de 12 casos no ano transacto, e diminuiu ainda mais para 7 casos nos primeiros três trimestres deste ano.

Note-se que, com os esforços conjuntos de todos os participantes do sistema de cibersegurança, a gestão e a capacidade técnica dos operadores continuam a melhorar, bem como é continuamente melhorada a resistência a ataques cibernéticos. De um modo geral, o trabalho de desenvolvimento da cibersegurança de Macau mostra uma tendência positiva.



II. É necessário aumentar ainda mais a capacidade de protecção no âmbito da cibersegurança

Embora a implementação da cibersegurança em Macau esteja a crescer a bom ritmo, os incidentes relacionados com ataques cibernéticos continuam a verificar-se ocasionalmente, e na análise do

CARIC verificou-se que os operadores de infra-estruturas críticas ainda enfrentam, de um modo geral, as três seguintes ameaças relevantes:

1) Invasão de sistemas informáticos através das vulnerabilidades existentes: depois de o CARIC ter analisado as provas recolhidas relativamente a todos os incidentes cibernéticos em Macau, constatou-se que cerca de 70% destes se deveram ao facto de os operadores não terem detectado e reparado, em tempo oportuno, a existência de vulnerabilidades de segurança nos sistemas, o que foi aproveitado pelos hackers para os invadir e, por conseguinte, praticarem a extorsão através de ransomware, "mineração" de criptomoedas, alteração do teor do website, entre outras actividades criminosas, tendo mesmo sido atacados outros sistemas através dos computadores infectados;

2) Uso ilícito do sistema para o acesso a contas: deve-se às deficiências existentes na estratégia de gestão da segurança da conta por parte de alguns operadores, e à falta de conhecimento de segurança dos utentes, o que fez com que os hackers pudessem furtar senhas de acesso ao sistema informático do utente, através de ataques de busca exaustiva das senhas brute-force attack, phishing website, entre outros métodos, para depois, através da conta roubada, divulgarem, em maior quantidade, e-mails com vírus, spam e informações falsas, ou recorrerem a outras vulnerabilidades de segurança do respectivo sistema para invadir os sistemas cibernéticos;

3) Ataques distribuídos de negação de serviço (DDoS): por variados motivos, alguns operadores não tinham previsto ataques (DDoS) de forma adequada, para os seus serviços de rede ligados ao exterior, o que fez com que o funcionamento estável desses serviços de rede ficasse

gravemente afectado, chegando mesmo à paralisação ao sofrerem este tipo de ataques.

Relativamente a estas ameaças, este ano o CARIC redobrou os esforços no melhoramento da sua capacidade de recolha e análise das informações nesta área, no sentido de ajudar os operadores, de forma atempada e mais eficiente, a detectarem as vulnerabilidades e o vazamento de contas, entre outros riscos de segurança e, além disso, no final deste ano, vão ser lançadas as “Directrizes técnicas para a gestão de vulnerabilidades”, para facilitar a melhoria das capacidades técnicas dos operadores sobre a gestão de vulnerabilidades. Ao mesmo tempo, os operadores devem continuar a colaborar activamente no trabalho do Governo da Região Administrativa Especial de Macau, cumprindo, nos termos da lei, os deveres de cibersegurança, e devem optimizar e ajustar, de forma contínua, as medidas técnicas e de gestão e ter uma boa gestão e controlo dos riscos de cibersegurança.

III. A salvaguarda da cibersegurança depende da participação de toda a sociedade

Face à situação cada vez mais grave no que diz respeito à cibersegurança, em particular, os riscos severos provenientes de organizações de hackers profissionais ou até mesmo de actividades dos hackers em contexto nacional, todas as partes intervenientes no sistema de cibersegurança, incluindo os operadores, não podem baixar a guarda nem por um momento, e devem estar sempre em alerta e com perseverança e devem, também, aperfeiçoar, de forma contínua, o desenvolvimento global da cibersegurança de Macau conforme a nova conjuntura, os novos desafios e as novas exigências. Sob a coordenação

da CPC, o CARIC, as entidades de supervisão e os operadores devem continuar, como sempre, a cooperar, como devem insistir em aprimorar, em simultâneo, o desenvolvimento e a segurança, e devem optimizar constantemente os mecanismos de funcionamento e os níveis técnicos de cibersegurança, com vista a garantir a segurança e a estabilidade dos diversos tipos de serviços críticos de rede e contribuir para a defesa da segurança nacional e do normal funcionamento da sociedade de Macau.

Em simultâneo, a maioria das empresas privadas e associações não é objecto de regulamentação pela Lei da cibersegurança, também enfrenta riscos de cibersegurança e é alvo de crimes cibernéticos. Assim, todos os sectores da sociedade devem dar maior importância à cibersegurança, melhorar continuamente o sentido de segurança e implementar medidas de protecção adequadas, de forma a dar uma melhor garantia a si próprios e aos destinatários dos seus serviços. A salvaguarda da cibersegurança é responsabilidade comum de toda a sociedade, e são necessárias a colaboração e a participação conjunta do Governo e de todos os sectores da sociedade, para construir, em conjunto, uma sólida linha de defesa para a cibersegurança de Macau.