HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/29C

25 November 2022

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Guidance on anti-DDoS protection

I am writing to provide authorized institutions (AIs) with additional guidance on protection against distributed denial-of-service (DDoS) attacks.

As stated in module "TM-E-1 Risk Management of E-banking" of the HKMA's Supervisory Policy Manual (SPM), AIs should implement adequate controls to promptly detect and respond to the threats posed by DDoS attacks that could impact the delivery of e-banking services. Module "TM-G-1 General Principles for Technology Risk Management" also states that AIs should put in place proper controls to safeguard their networks and systems against disruption. In view of the growing incidence and sophistication of DDoS attacks, the HKMA considers that there are merits to provide AIs with more detailed guidance on this specific area of cyber security.

The below guidance is developed with reference to the findings of a round of thematic reviews completed recently by the HKMA to assess the effectiveness of the anti-DDoS protective measures maintained by AIs. It is grouped under four key principles:-

Undertaking regular risk assessment and vulnerability management – As part of their cyber threat surveillance, AIs should monitor the latest trends, tactics and techniques of DDoS attacks. They should have in place a robust mechanism to regularly identify, assess and mitigate vulnerabilities in their networks and systems which may be at risk to new forms of DDoS attacks, and critically assess whether their anti-DDoS defence mechanism remains adequate, including in terms of mitigation capacity and activation and mitigation time. The assessment should cover not only the institution's own protective measures but also those provided by third parties. While the regular assessment should normally be undertaken by the first line of defence, the second line of defence should be involved to provide an additional opinion.

Designing the architecture of anti-DDoS controls properly – The architecture of the institution's anti-DDoS controls should be properly configured and regularly reviewed to provide comprehensive protection against DDoS attacks. Both customer-facing channels (e.g. online banking) and key components that support the institution's operations (e.g. remote access servers, email gateways and Domain Name System (DNS) servers) should be covered by the protective measures. AIs should deploy multi-layered defence (e.g. a combination of cloud-based DDoS protection services, clean pipe services from internet service providers and on-premises solutions) to achieve optimal protection.

Maintaining effective governance over service providers and putting in place robust contingency arrangements – AIs should identify the key third parties which are critical to the availability of their internet-facing services and are potential targets of DDoS attacks (e.g. DNS and internet service providers). An effective mechanism should be in place to regularly evaluate their cyber defence capability. AIs should also develop appropriate contingency arrangements for potential disruption to the services of these third parties, and avoid placing excessive reliance on a single service provider to minimise the risk of a single point of failure. With regard to anti-DDoS controls supported by third parties, a rigorous due diligence process should be in place to assess their capabilities of DDoS defence. The key performance indicators to be observed by the service providers should be clearly set out in written agreements.

Establishing proper incident response procedures and conducting regular rehearsal exercises – AIs should establish end-to-end incident response and escalation procedures, covering, among others, actions required of anti-DDoS service providers (e.g. timely identification of DDoS attempts, adjustment in relevant thresholds and rules for responding to DDoS attacks). Lessons learned from significant DDoS incidents, occurred both locally and internationally, should be incorporated into AIs' incident response and escalation procedures. Apart from table-top DDoS drill exercises, AIs are expected to perform technical drills (with appropriate involvement of anti-DDoS service providers) to validate the effectiveness of the anti-DDoS protective measures.

The above guidance seeks to complement the HKMA's supervisory expectations in relation to the management of DDoS attacks as stated in the relevant SPM modules. AIs are expected to take into account the above guidance in their regular assessments of the effectiveness of their anti-DDoS protection.

Should your institution have any questions about this circular, please feel free to contact Ms Connie Tse on 2597 0617 or Mr Daniel Tang on 2597 0690.

Yours faithfully,

Raymond Chan
Executive Director (Banking Supervision)