Circular No. SRD TR 01/2015

24 August 2015

The Chief Executive Officers of All Financial Institutions

Dear Sir / Madam

EARLY DETECTION OF CYBER INTRUSIONS

Financial institutions ("FIs") today are being targeted by hackers with increasingly sophisticated techniques. While traditional cyber defences may be apt at thwarting malwares with known signatures, such defence strategies are fast losing their effectiveness against more sophisticated cyber-attacks that leverage on zero-day or customised exploits.

2 Many studies have repeatedly shown that most organisations remain oblivious of a breach in their systems and networks long after it has taken place. Such breaches often reveal the presence of advanced persistent threat actors who have employed zero-day or customised exploits when targeting the organisations. In many cases, the breach is discovered by external parties rather than the organisation itself. Such delays in detecting cyber intrusions have compromised the interests of organisations and their customers.

3 Strong cyber resilience therefore requires that FIs not only secure their perimeters from a potential breach, but also have robust capabilities to promptly detect any cyber intrusions so as to enable swift containment and recovery. Since not all successful attacks can be prevented, the speed at which an FI detects and responds to an intrusion becomes crucial. In this regard, it is important that FIs maintain a keen sense of situational awareness by continuously enhancing their technical and internal control processes to monitor and detect:

a. Network intrusion

At the network level, intrusion detection capabilities should be present for not only the external network, but within the internal network as well. Following a successful infiltration, attackers often try to move across systems in an attempt to infiltrate more machines within the network. FIs should monitor internal network communications closely to detect and/or block unauthorised or atypical network communications amongst servers, systems and endpoint devices. For example, FIs could put in place decoys, sensors and/or other appropriate

capabilities to detect anomalous traffic across systems within the internal networks.

b. Systems, servers, network devices and endpoints intrusion

Abnormal and suspicious activities typically start surfacing at the systems, servers, network devices and endpoint devices after they have been compromised. FIs should put in place mechanisms to detect and/or block behavioural anomalies on such systems, servers and devices. Examples of such anomalies include abnormal user activities, unauthorized system configuration changes, and/or unusual memory access and system processes. As compromised devices often attempt to establish connections back to command and control servers through internet connections, FIs should proactively monitor and block callbacks which are tell-tale signs of intrusions.

4 Upon the discovery of a successful intrusion, FIs should perform a thorough investigation to determine the extent of infiltration and damage sustained as well as the vulnerabilities being exploited by the attacker. While the investigation is ongoing, FIs should also take immediate actions to contain the situation in order to prevent further damage and commence recovery efforts to restore operations based on their cyber breach response plan. The presence of a well-thought-out and tested cyber breach response plan will assist FIs in coordinating effective response and recovery actions across the entire organisation and ensure that there is timely communication of key cyber breach details and findings to relevant stakeholders.

5 FIs should continually evolve and improve their ability to anticipate, withstand, detect, and respond to cyber attacks. FIs should regularly perform gap analysis and risk assessments to determine whether their controls remain holistic and adequate, and that their response and recovery plans stay effective. FIs should also put in place a roadmap to promptly address any gaps that are found.

6 Should you have any questions or comments, please contact your respective MAS Review Officers.

Yours faithfully
(Sent via MASNET)
HO HERN SHIN
EXECUTIVE DIRECTOR & HEAD
SPECIALIST RISK DEPARTMENT