NOTICE TO FINANCIAL INSTITUTIONS

NOTICE NO. FTU/N-1/2017/1

EARLY DETECTION OF CYBER INTRUSION AND INCIDENT REPORTING

---

1. INTRODUCTION

1.1 This Notice is issued pursuant to section 54 of the Autoriti Monetari Brunei Darussalam Order, 2010 (AMBD Order) which applies to all Financial Institutions as defined in this Notice.

1.2 In light of the recent rise in number of cybersecurity incidents happening around the world, it is becoming more likely that Financial Institutions ("FIs") are being targeted by hackers. Their techniques are also becoming more sophisticated such as by exploiting vulnerabilities and using ransomware such as WannaCry and NotPetya. While traditional cybersecurity tools are appropriate in preventing malwares with known signatures, such strategies are gradually losing their effectiveness against more sophisticated cyber-attacks that leverage on zero-day and exploits. Many studies have repeatedly shown that most organisations were unaware of a breach in their systems and networks long after it has taken place. In many cases, external parties rather than the organisation itself discovered the breach. Such delays in detecting cyber intrusions have compromised the interests of the organisations and their customers. The Autoriti Monetari Brunei Darussalam (AMBD) therefore, places great emphasis on the requirements for the FIs to continuously enhance their detection of cyber intrusion and to report major IT incidents to AMBD.

1.3 This Notice shall take effect from 1st January 2018.

2. DEFINITIONS

2.1 For the purpose of this Notice, and unless otherwise expressly stated, all words and terms in this Notice shall have the same meaning as used in the AMBD Order.

2.2 "Cyber intrusion" is the act of accessing network, IT systems, servers, end-points, and IT devices without authorisation or consent.

2.3 "Financial Institution" means :-

(a) any person licensed, registered or regulated under any of the following legislations:

(i) Banking Order, 2006;

(ii) Islamic Banking Order, 2008;

(iii) Insurance Order, 2006;

(iv) Takaful Order, 2008;

(v) Finance Companies Act, Cap. 89;

(vi) Moneylenders Act, Cap. 62;

(vii) Pawnbrokers Order, 2002;

(viii) Money-Changing and Remittance Businesses Act, Cap. 174;

(ix) Securities Markets Order, 2013 (excluding recognized and designated market operators); and

(b) Perbadanan Tabung Amanah Islam Brunei established under the Tabung Amanah Islam Brunei Act (Cap. 163).

2.4 "Network" refers to the computer networks on FIs work premise that are used in conducting FIs work activities.

2.5 "System" refers to the FIs' IT system to run their operation.

2.6 "Server" refers to servers that are managed by the FIs that host their system.

2.7 "End-point" refers to computer or laptop used for the FIs' work purposes and to store information related to the FIs, stakeholders and customers.

2.8 "Major IT incident" means system malfunction or cybersecurity incident, which has a severe and widespread impact on the FI's operations or materially impacts the FI's service to its customers. For example, a downed server that affects the core financial system, ransomware attacks and other incidents of a similar nature.

2.9 "Near-miss cybersecurity Incident" is cybersecurity incident that has no negative impacts, but if given shift of time, will cause severe and widespread impact on the FI's operations or materially impacts the FI's service to its customer.

3. EARLY DETECTION OF CYBER THREATS

3.1 FIs must have robust capabilities to proactively detect cyber intrusions, which will enable quick response and recovery by the FIs. Since not all successful attacks can be prevented, the speed at which an FI detects and responds to a cyber 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 in monitoring and detecting:

3.1.1 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 network communications amongst servers, systems and endpoint devices. For example, FIs could put in place devices, software tools, sensors and/or other appropriate capabilities to detect anomalous traffic across systems within the internal networks.

3.1.2 Abnormal and suspicious activities typically start developing at the systems, servers, network 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 activities include unusual user access pattern, unauthorised system configuration changes, and/or abnormal memory access and system processes. As affected devices often attempt to establish connections to the command and control servers through internet connections, FIs should proactively monitor and block these indicators.

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

4. INCIDENT REPORTING

4.1 FIs are to notify AMBD as soon as possible but no later than **one (1) hour** upon the discovery of a successful cyber intrusion or any major IT incident (collectively "Incident") and there upon to provide timely updates. In any event, FIs are not allowed to make any public announcement in regards to the incident prior to such notification.

4.2 FIs must submit root-cause and impact analysis report(s) ("IT Incident Report") to AMBD within 7 days or such longer period as AMBD may allow, from the discovery of the Incident. FIs should submit the IT Incident Report in the format as may be determined by AMBD.

4.3 Non-successful cyber intrusions or near-miss cybersecurity incidents must be recorded and compiled. FIs are to submit details of these non-successful cyber intrusions and near-miss cybersecurity incidents to AMBD within 1 week after end of each month (if any) in the format as determined by AMBD.

5. GAP ANALYSIS

5.1 FIs must regularly perform gap analysis and risk assessments to determine whether their controls remain appropriate 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.

MANAGING DIRECTOR

AUTORITI MONETARI BRUNEI DARUSSALAM

Issue Date: 26 October 2017