المدير التنفيذي للرقابة المصرفية
Executive Director - Banking Supervision

مصرف البحرين المركزي
Central Bank of Bahrain

EDBS/KH/C/34/2014
28th April 2014

Chief Executive Officer
All Retail Banks and Financing Companies
Manama
Kingdom of Bahrain

Dear Sir,

Upgrade of ATMs and application software that run on Windows XP

As Microsoft has ceased supporting Windows XP operating systems effective April 8, 2014, the CBB hereby directs, with immediate effect, that all ATMs and internal applications that run on Windows XP must be upgraded by no later than 1st April 2015.

All licensees addressed in this circular must purchase an extended warranty from Microsoft to cover Windows XP support until the completion of the upgrade. In the interim period, the liability for any breach of security occurring as a result of continuing to use Windows XP will be borne by the licensee. Attached herewith are security recommendations that you may wish to consider in the interim period.

Furthermore, all licensees must immediately send to the CBB a written notification in case of any breach of security in Windows XP and in all near-miss ATM fraud/scams. Licensees must also provide the CBB by no later than 30th May 2014:

(1) a list of all applications on the internal network that run on Windows XP along with the timeline to upgrade them; and
(2) the target date for the upgrade of all the ATMs.

Licensees which do not currently use Windows XP operating systems should provide written confirmation to the CBB accordingly.

Finally, all licensees must provide the CBB a report on a monthly basis detailing the status of the upgrade plan.

All notifications and reports required in this letter should be submitted electronically to Mr. Riyad Al Maraj, Head - IT Project at "TechRisk@cbb.gov.bh". In addition, any incident of ATM fraud/scams must continue to be provided to the Director of Compliance at the CBB as well by email to: Compliance@cbb.gov.bh.

Yours faithfully,

Khalid Hamad

Encl: General Security Recommendations

ص.ب : ٢٧، المنامة - مملكة البحرين
هاتف : ١٧٥٤٧٤٠٠ (٩٧٣+) - فاكس: ١٧٥٣٢٦٠٥ (٩٧٣+)
P.O. Box : 27, Manama - Kingdom of Bahrain
Tel: (+973) 17547400 - Fax: (+973) 17532605
website: www.cbb.gov.bh
E-mail: khalid.hamad@cbb.gov.bh

General Security Recommendations

- ATM Vulnerability Assessment to be performed post April 8, 2014 and all the risks should be appropriately addressed with due communication to senior management.
- ATMs OS built in firewalls should be activated.
- All OS services that are not required for the ATMs operation should be disabled/uninstalled as applicable.
- All ATMs OS user IDs should be configured with strong passwords.
- Implement Security technologies like Firewalls and Intrusion Prevention (i.e. the ATM network should be protected with at least one layer of both firewall and IPS)
- Segregate ATM Network from Internal Network through the use of non-routing VLANs.
- Make sure that the ATM VLANs do not have internet/email access, access to network printers or is used for any purpose other than hosting the ATMs.
- Ensure that the ATM does not allow rebooting using smart cards or other external devices
- Block all direct connectivity to ATMs like USBs
- Control and log physical access for loading/unloading cash
- Implement appropriate anti-malware and anti-virus software as applicable and certified by the ATMs supplier.
- Ensure that the Operating System has the latest available patches as applicable and certified by the ATMs supplier.
- All unnecessary users account on ATMs OS should be deleted or disabled (only if deletion is not possible).
- The installation of software on the ATMs should be disabled (at least disable the Windows installer service).
- Remote login to the ATMs should be disabled (at least disable the remote desktop service).

- Sharing of ATMs folders over the network should be disabled by disabling the file and print service.
- Access to the ATMs external storage such as CD/DVD drives or USB ports should be disabled except for the ports needed for the ATMs operation.
- BIOS (Basic Input/output System) should be locked down in ATMs to prevent them from being booted through unauthorized media such as CD ROMs or USB sticks.
- ATM Physical Security:
  - Ensure 24X7 Monitoring of physical access to ATMs
  - Ensure that the Power Source of the ATM is secured
  - Implement anti-skimming devices along with regular physical checks

Internal Application Security:

- Applications that do not run on newer versions of Windows should have User Access based on least privilege required and physical segregation like use of VLANs
- Control and log User Access to Applications and implement Strong User Authentication for IT Administration/connections
- All Windows XP machines that can be used as standalone PCs should be taken off the internal network.
- Banks should consider using virtual environments for legacy applications that do not run on newer Windows versions (e.g. Examples of virtual environments are Citrix, Virtual PC, VMware…etc.)