9041009847

بسم الله الرحمن الرحيم

مؤسسة النقد العربي السعودي

المركز الرئيسي

إدارة الإشراف البنكي

الرقم : ..... م أ ش .....

المرفقات : .....

تعميم لجميع البنوك العاملة بالمملكة

سعادة / **الموقر**

بعد التحية:

الموضوع: متطلبات للحد من هجمات تعطيل او حجب الخدمات الإلكترونية (DDoS Attack)

إشارة إلى حرص المؤسسة لرفع مستوى حماية الخدمات الإلكترونية التي تقدمها البنوك العاملة في المملكة على مدار الساعة، وذلك من خلال إتباع أفضل الحلول والممارسات العالمية في حفظ البنية التحتية من الهجمات الإلكترونية والتي يكون أهدافها تخريبية، وحيث لوحظ في الآونة الأخيرة ازدياد الهجمات على الجهات المالية والتي من أهدافها تعطيل او حجب الخدمات الالكترونية، ونظراً لاختلاف البنوك في تطبيق الحلول المناسبة والتي من شأنها تقلل من مخاطر هذه الهجمات. لذا يتعين على البنك الأخذ بالاعتبار تطبيق المتطلبات التالية كحد أدنى من الإجراءات التي يجب القيام بها، وهي كالآتي:

١. التعاقد مع أحد الشركات العالمية المتخصصة في مجال تنقية البيانات (DDoS Scrubbing Center) وذلك لتمرير وتنقية البيانات الواردة والمشبوهة لموقع/ لخدمات البنك وذلك لاستخدامه في حالة وجود هجوم إلكتروني يهدف الى حجب او تعطيل الخدمات الالكترونية، مع الأخذ بعين الاعتبار أن أجهزة الحماية والتي تعرف بـ (DDoS Appliances) غير كافية.
٢. يجب أن تنص الاتفاقية مع مركز تنقية البيانات (DDoS Scrubbing Center) مقدرة البنك على زيادة السعة الاستيعابية فوراً عند مواجهة هجوم إلكتروني أكبر من السعة الاستيعابية المتفق عليها.
٣. يجب أن تشمل خدمة تنقية البيانات (DDoS Scrubbing Center) كلاً من مركز البيانات الرئيسي (Data Center) وكذلك المركز الاحتياطي (Disaster Recovery Site) للبنك.

بسم الله الرحمن الرحيم

مؤسسة النقد العربي السعودي

للمركز الرئيسي

إدارة الإشراف البنكي

الرقم : ..... م أ ش .....

التاريخ : .....

المرفقات : .....

الموافق : .....

٤. يجب مراقبة الأنشطة والبيانات الواردة والمشبوهة لموقع البنك على مدار الساعة ٧/٢٤ من خلال مركز المراقبة الامنية الخاص بالبنك (Security Operation Center) ومركز المراقبة لدى مزود الخدمة (ISP) بالإضافة إلى مركز تنقية البيانات (DDoS Scrubbing Center)، على أن يقوم المزود بإرسال تقارير وتنبيهات مستمرة عن الأنشطة بحيث يتفق على الآلية ضمن اتفاقية الخدمة.

٥. ضبط إعدادات البنية التحتية للبنك (Routers, Firewalls, IPS/IDS, etc) بما يتوافق مع أفضل الممارسات (Best Practice) في هذا المجال، للتقليل من مخاطر هذه الهجمات، ومراجعة وتقييم الإعدادات بشكل دوري وذلك في موقع البيانات الرئيسي والاحتياطي للبنك.

٦. عمل سياسة وتحديد إجراءات واضحة تغطي عدة سيناريوهات يتم التدرب عليها للعمل بها في حال وجود هجوم إلكتروني على البنك.

٧. يجب اختبار عملية إعادة توجيه البيانات (Reroute traffic) إلى مركز تنقية البيانات مرتين في السنة على الأقل للتأكد من توافق الإعدادات وسهولة الانتقال في حال وجود هجوم.

٨. يجب إبلاغ المؤسسة فوراً – مسئول أمن المعلومات في الإدارة العامة للرقابة على البنوك – في حال تعرض البنك لأي هجوم إلكتروني.

٩. على البنك تطبيق التعليمات أعلاه في مده أقصاها ٢٠١٥/٢/٢٨م

عليه آمل تزويد مقام المؤسسة بكامل الإجراءات المطبقة في التاريخ المذكور أعلاه، وللتنسيق والاستفسار يمكنكم التواصل مع مسئول أمن المعلومات في الإدارة العامة للرقابة على البنوك المفتش/مروان اللحيدان هاتف/ ٤٦٣٣٠٠٠ تحويلة ٥٨١٨ أو البريد الإلكتروني maalohaidan@sama.gov.sa

وتقبلوا تحياتي،،،

عبدالعزيز بن عبدالرحمن الحليسي

وكيل المحافظ للرقابة

- نطاق التوزيع:
- جميع البنوك العاملة في المملكة