الرقم: ٩/٤/٥/ ٨٤١٣

التاريخ: ١٦ /٩ /١٤٣٨ هـ

الموافق: ١١ / ٦ / ٢٠١٧ م

تعميم إلى شركات الصرافة المرخصة

في ضوء عمليات الاحتيال التي تتم بواسطة رسائل بريد الكتروني وهمية او مزورة او متقمصة لشخصية موثوقة سواء كانت داخلية ام خارجية ، والتي تهدف الى الوصول لمعلومات حساسة او تمرير ملفات خبيثة تمهيدا لتنفيذ اختراقات الكترونية ذات مخاطر اكثر ضرراً على الشركة وعملياتها وسمعتها ، اؤكد على ضرورة توفير الضوابط اللازمة بهذا الخصوص ومنها اتخاذ الاجراءات التالية :

أولاً : تطبيق سياسة لإدارة وتعريف تطبيقات وبروتوكولات ونطاق البريد الالكتروني الذي يحمل اسم شركة الصرافة على الانترنت متضمنا الضوابط التالية بالحد الادنى :

١. تفعيل بروتوكول البريد الالكتروني بحيث يسمح للمستخدم بالنفاذ لحسابه فقط بعد التوثق من هويته ومن خلال اتباع سياسة توثق / تحقق للهوية يصعب على الغير اختراقها ، كأن يتم من خلال اسم تعريف فريد وغير معروف للغير ورمز سري يجبر المستخدم على تغييره كل فترة زمنية معينة ، وبحيث يتكون بالحد الادنى من ٨ خانات من الارقام والحروف والرموز وان لا يتشابه مع عدد محدد من الرموز التاريخية المستخدمة سابقاً او مع اي مكون من اسم التعريف او بيانات هوية المستخدم وقد يتم استخدام طريقة توثق / تحقق الهوية المتعدد (Multi-Factor Authentication) وخاصة لمستخدمي البريد الالكتروني والتي تعتبر طبيعة عملهم حساسة وذات اثر ومخاطر على عمليات الشركة وسمعتها .

٢. استخدام بروتوكولات تشفير قوية (مثل TLS) بحيث تكون محدثة باستمرار بحسب اخر نسخة مصدرة – ما امكن – لضمان حماية عمليات الاتصال بالبريد الالكتروني .

٣. تفعيل خاصية (Reverse DNS Check) للتحقق من مطابقة العنوان الرقمي (IP) لمرسل البريد الالكتروني (الوارد) مع اسمي النطاق والجهاز الصادر عنهما .

٤. اتخاذ ما يمكن من اجراءات فنية تحول دون استلام البريد الالكتروني من مصادر تسمح بتمرير البريد الوارد بواسطة ما يعرف بتقنية ال (Open Mail Relay) .

٥. اتخاذ الاجراءات الفنية اللازمة وبما لا يسمح باستقبال البريد الالكتروني عبر تقنية (Open Mail Relay) ما امكن .

ص.ب٣٧ عمان ١١١١٨ – الأردن هاتف ٩/٤٦٣٠٣٠١ * فاكس ٤٦٣٨٨٨٩ ، ٤٦٣٩٧٣٠ موقع الكتروني www.cbj.gov.jo بريد الكتروني info@cbj.gov.jo

٦. تفعيل خاصية (Real –time Blocking list (RBL) Check) بحيث يتم من خلالها حجب الرسائل الواردة من مصادر مشبوهة اعتمادا على قوائم بيانات دولية موثوقة ومحدثة بهذا الشأن بالإضافة لقوائم داخلية تبنى وتحدث لتحقيق ذات الغرض .

٧. تفعيل خاصية (Sender Policy Framework (SPF) Check) لتقليل احتمالية استلام رسائل بريد الكتروني من غير مصادرها الاصلية .

٨. حجب المرفقات والروابط المشبوهة ضمن رسائل البريد الالكتروني من خلال فحصها بواسطة برمجيات معتمد عليها بهذا الخصوص ، وحظر الملفات ذات الامتدادات التنفيذية (Executable Files) وتحديد سقف مسموح لحجم المرفق ، مع ضرورة تفعيل سياسة مناسبة على نظام البريد الالكتروني للتعامل مع تلك الرسائل بناءً على درجة مخاطرها .

٩. النظر في امكانية تعريف سقوف لعدد الاتصالات بخادم البريد الالكتروني من المصدر الواحد وبما يتناسب ومواصفات خادم البريد الالكتروني ومتطلبات العمل حيثما لزم ، مع ضرورة توظيف خصائص التوافرية وخطط استمرارية العمل لخدمات البريد الالكتروني .

١٠. النظر في امكانية تفعيل خاصية (DNSSEC) ضمن مكونات البيئة التقنية لديكم ما امكن.

١١. الاحتفاظ بسجلات التتبع لأنظمة البريد الالكتروني لفترة زمنية تحدد ضمن سياسة الاحتفاظ بالبيانات لا تقل عن ثلاثة اشهر .

ثانياً : إجراء اختبارات الاختراق اللازمة من قبل جهة محايدة بشكل دوري للتأكد من تفعيل خصائص الحماية والتي منها ما ورد في البند اولاً اعلاه .

ثالثاً : العمل وفق مبدأ الدفاع بالعمق (Defense in Depth) من خلال تشغيل أنظمة حماية من مصادر متنوعة ضمن مستويات مختلفة (Different Security Tires) .

رابعاً : تضمين سياسة أمن المعلومات بسياسة استخدام البريد الالكتروني اعتمادا على افضل الممارسات الدولية بهذا المجال مع الالتزام بسياسة تصنيف البيانات لدى ارسال رسائل ذات محتوى سري وتشفير تلك الرسائل حيثما لزم .

خامساً : تضمين برامج التدقيق الداخلي والخارجي بإجراءات فحص مخاطر البريد الالكتروني تشمل الامور المذكورة اعلاه بالحد الادنى .

وتفضلوا بقبول فائق الاحترام،،،

المحافظ

د.زياد فريز

ص.ب ٣٧٠٠ عمان ١١١١٨ – الأردن هاتف ٩/٤٦٣٠٣٠١ * فاكس ٤٦٣٨٨٨٩ ، ٤٦٣٩٧٣٠ موقع الكتروني www.cbi.gov.jo بريد الكتروني info@cbi.gov.jo