CENTRAL BANK OF JORDAN

الرقم: ٩/٤/٥/ ١٠٤٦

التاريخ: ١٧/ ٨/ ١٤٣٨ هـ

الموافق: ١٤/ ٥/ ٢٠١٧ م

تعميم إلى شركات الصرافة المرخصة

في ضوء عمليات الهجوم التي تتعرض له المؤسسات والأفراد حول العالم تحت ما يسمى بالـ (Ransomware) والنسخ المستحدثة منه مثل (WannaCry, WCry, Wanna Decryptor)، نؤكد على ضرورة العمل بما جاء في تعميمينا السابقين رقم (٣٣٤٧/٤/٩) تاريخ ٢٠١٢/٣/٢٢ ورقم (١٢٣٢٩/٧/٢/٩) تاريخ٢٠١٣/١٠/٦، والعمل على اتخاذ الإجراءات التالية:

١. تطبيق آخر تحديثات نظام التشغيل (Windows) وعلى وجه الخصوص التحديث (MS 17-010 SMB) على كافة الأجهزة العاملة بنظام التشغيل المذكور، مع مراعاة تطبيق إجراءات التغيير بحسب الممارسات السليمة بهذا الخصوص.
٢. التأكد من تحديث برمجيات كشف الفيروسات بشكل مستمر على كافة الأجهزة، وتشغيل عمليات الفحص الدائم للبريد الإلكتروني الوارد والصادر.
٣. تفعيل قاعدة منح الصلاحيات والامتيازات بالحد الأدنى وبحسب الحاجة للعمل، ودراسة الحاجة للمستخدمين من ذوي الامتيازات العليا (Administrators).
٤. عدم تفعيل (Macro Scripts) لملفات المايكروسوفت المرسلة ضمن البريد الإلكتروني، ومراعاة فتح تلك الملفات من خلال برنامج (Office Viewer) بدلا من (Full Office Suite Applications).
٥. تطبيق برمجيات الأمن والحماية التي تعمل على كشف البرمجيات الخبيثة بالاعتماد على سلوكياتها (Behavioral Anomaly) ما أمكن.
٦. اتباع سياسة نسخ احتياطي للبيانات الحساسة بحيث تضمن أخذ نسخ احتياطية تحفظ في أماكن آمنة وغير قابلة للنفاذ إليها عبر الشبكات، مع تطبيق إجراءات التأكد من سلامة واعتمادية البيانات ووسائط تخزينها.
٧. تفحص الروابط والمرفقات ضمن البريد الإلكتروني الوارد للتأكد من عدم وجود ملفات خبيثة، وعدم فتح الروابط والملفات المرفقة غير المرغوب بها.

ص٠ب٣٧ عمان ١١١١٨ – الأردن هاتف ٩/٤٦٣٠٣٠١ * فاكس ٤٦٣٨٨٨٩ ، ٤٦٣٩٧٣٠ موقع إلكتروني www.cbj.gov.jo بريد إلكتروني info@cbj.gov.jo

٨. إنزال البرمجيات من الإنترنت عند اللزوم في أضيق الحدود المسموحة ومن مصادر موثوقة، وبحيث يتم مراعاة إجراءات التغيير المعتمدة لديكم بعد أخذ الموافقات اللازمة بهذا الخصوص.
٩. تفعيل خاصية (Automated Patches) لبرامج التشغيل ومحركات البحث على كافة الأجهزة.
١٠. العمل على تطوير برنامج توعوي يحدث باستمرار ويوجه للمستخدمين متعلق بأساليب كشف وآلية التعامل مع رسائل البريد الإلكتروني الاحتيالية والمشكوك فيها، تتضمن على وجه الخصوص محاولات التصييد والهندسة الاجتماعية.
١١. تفعيل إجراءات فحص الشبكات (Penetration Tests and Vulnerability Assessment) مرة واحدة على الأقل كل سنة.
١٢. مراجعة وفحص اعتمادية وتحديث إجراءات الاستجابة ومعالجة الحوادث الخاصة بأمن المعلومات وخطط استمرارية العمل الخاصة بالشركة وتلك الخاصة بمزودي الخدمات.
١٣. إعلام البنك المركزي فور حدوث أي إختراق أو محاولة اختراق وبحسب تعليماتنا بهذا الخصوص.

وتفضلوا بقبول فائق الاحترام،،،

المحافـــظ

د.زيـــاد فريـــز