بسم الله الرحمن الرحيم

١٢٣٢٩

الرقـــم: ٩/٢/٧/

التاريخ: ١ /١٢/١٤٣٤ هـ

الموافق: ٦ /١٠/ ٢٠١٣ م

تعميم الى شركات الصرافة المرخصة

الموضوع : ارشادات للحد من مخاطر عمليات اختراق انظمة الحوالات السريعة

تـحيـه وبـعـد ،،،

حرصا من البنك المركزي الاردني على سلامة وكفاءة التعاملات الصيرفية التي تنفذها شركات الصرافة وحفاظا على حقوق المتعاملين ، ارجو مراعاة الارشادات التالية وذلك للحد من المخاطر التي تتعرض لها تعاملاتكم في مجال خدمة الحوالات السريعة :

١-ضرورة أن تكون كافة أجهزة الحواسيب الشخصية المستخدمة في انظمة الحوالات السريعة مجهزة بشكل أصولي بكافة البرمجيات اللازمة مثل نظام التشغيل ونظام الحماية من الفايروسات والبرامج الخبيثة بما فيها انظمة الحوالات السريعة وباستخدام برمجيات أصلية ومرخصة وفق الأصول ومثبته وفق الخطوات المحددة من قبل الشركات المنتجة لهذه البرمجيات.

٢-ضرورة الاستمرار في تحديث أنظمة التشغيل وأنظمة الحماية من الفايروسات والبرامج الخبيثة وأنظمة الحوالات السريعة بشكل دوري وأصولي وفق توصيات الشركات المنتجة.

٣-ضرورة ان يتم استخدام انظمة الحوالات السريعة وفق توصيات وتوجيهات الشركة المنتجة وتوفير التدريب الكافي للموظفين لاستخدام النظام. (Proper Usage).

٤-ضرورة أن لا تحتوي الحواسيب المستخدمة لأنظمة الحوالات السريعة على أنظمة وبرامج أخرى غير لازمة لها وكذلك عدم استخدام هذه الحواسيب لأغراض أخرى.

٥-ضرورة عدم السماح باستخدام وسائط التخزين الخارجية مثل الأقراص الضوئية و USB Flash من جهات غيْر موثوق بها لإمكانية إحتوائها على برمجيات خبيثة.

٦-ضرورة حفظ وسائط التخزين الأصلية وأية وثائق قد تحتوي على كلمات أو أرقام سرية والتي يتم تزويدكم بها من قبل كافة الشركات الموردة للأجهزة والأنظمة في مكان امن بعد عملية تثبيت الأنظمة وعدم السماح بإخراجها أو نسخها إلا عند الضرورة.

٧-ضرورة أن يتم حماية الاتصال الشبكي مع الأجهزة المستخدمة في انظمة الحوالات السريعة من خلال تركيب أجهزة حماية مختلفة بينها و بين نقطة الاتصال مع هذه الانظمة مثل أجهزة الجدار الناري (Firewalls) وأجهزة منع واكتشاف المتسللين (IPS/IDS) وضرورة أن تكون هناك جهة فنية لديكم لتعريف وإدارة ومتابعة هذه التجهيزات وفق متطلبات الشركات المنتجة.

٨- ضرورة حماية التجهيزات المستخدمة لأنظمة الحوالات السريعة بشكل امن وبحيث لا يسمح بالوصول إليه مادياً إلا لمن يملك الصلاحية لاستخدامها. (Physical Security).

٩- ضرورة الاعتناء بصلاحيات استخدام الأجهزة والأنظمة والتي تبين من يمكنه استخدام أية أجهزة وفي أية وقت (Access Controls) وكذلك بعمليات التحقق من الشخصية للمستخدم لهذه الأجهزة (Authentication) وضرورة وجود جهة فنية لديكم لمتابعة عمليات إعطاء وإلغاء الصلاحيات ، كذلك التأكيد على كافة المستخدمين لديكم بعدم مشاركة نفس اسم المستخدم وكلمة السر من قبل أكثر من شخص وكذلك إلغاء الحسابات عن الأجهزة والأنظمة وتغيير كلمات السر للموظفين عند حصول أي تعديل في الموظفين مثل الاستقالة.

١٠- ضرورة أن تكون عملية الاتصال مع شركات الحوالات السريعة محمية، ووفق متطلبات الحماية الصادرة عن الشركة المنتجة (Security Requirements) مثل استخدام تقنيات التشفير (Encryption).

١١- ضرورة توفير التدريب الكافي المتخصص للموظفين العاملين على الأجهزة بخصوص الطرق السليمة لاستخدام الأجهزة والأنظمة وكذلك ضرورة زيادة وعي الموظفين بخصوص مخاطر البرامج الخبيثة والمؤذية وطرق الوقاية منها.

وتفضلوا بقبول فائق الاحترام ،،،

المحافظ

د. زياد فريز

ص.ب ٣٧٥٠ عمان ١١١١٨ – الأردن هاتف ٩/٤٦٣٠٣٠١ * فاكس ٤٦٣٨٨٨٩ ، ٤٦٣٩٧٣٠ موقع إلكتروني www.cbj.gov.jo بريد إلكتروني info@cbj.gov.jo