مصرف لبنان
BANQUE DU LIBAN

تعميم أساسي للمصارف رقم ١٤٤

موجه أيضاً للمؤسسات المالية

نودعكم ربطاً نسخة عن القرار الاساسي رقم ١٢٧٢٥ تاريخ ٢٠١٧/١١/٢٨ المتعلق بالوقاية من الافعال الجرمية الالكترونية.

بيروت، في ٢٨ تشرين الثاني ٢٠١٧
حاكم مصرف لبنان
رياض توفيق سلامه

مصرف لبنان
BANQUE DU LIBAN

قرار أساسي رقم ١٢٧٢٥

الوقاية من الافعال الجرمية الالكترونية

ان حاكم مصرف لبنان،
بناءً على قانون النقد والتسليف سيما المواد ٧٠ و١٧٤ و١٨٢ منه،
وبناءً على احكام قانون مكافحة تبييض الاموال وتمويل الارهاب رقم ٤٤ تاريخ ٢٠١٥/١١/٢٤،
وبناءً على القرار الاساسي رقم ٧٨١٨ تاريخ ٢٠٠١/٥/١٨ وتعديلاته المتعلق بنظام مراقبة العمليات المالية والمصرفية لمكافحة تبييض الاموال وتمويل الارهاب، المرفق بالتعميم الاساسي رقم ٨٣،
وبناءً على "الدليل الارشادي للوقاية من الافعال الجرمية بواسطة البريد الالكتروني" الصادر عن مصرف لبنان وهيئة التحقيق الخاصة وجمعية مصارف لبنان ومكتب مكافحة جرائم المعلوماتية وحماية الملكية الفكرية التابع لوحدة الشرطة القضائية الذي تم اطلاقه بتاريخ ٢٠١٦/١٠/٢٠،
وبناء على قرار المجلس المركزي لمصرف لبنان المتخذ في جلسته المنعقدة بتاريخ ٢٠١٧/١١/٢١،

يقرر ما يأتي :

أولاً: سياسات واجراءات الوقاية من الافعال الجرمية الالكترونية

المادة الاولى: على المصارف والمؤسسات المالية اعداد سياسات واتخاذ تدابير واجراءات وقائية من الافعال الجرمية بالوسائل الالكترونية تتضمن، على الاقل:

أولاً: سياسات عامة تشمل:

١- تحليل مخاطر الجرائم الالكترونية المحتملة والاطلاع المستمر على آخر المستجدات في مجال تكنولوجيا أمان المعلومات.

٢- تخصيص المبالغ والموازنة اللازمة لإرساء وتطبيق سياسة ونظم وقواعد أمان تكنولوجيا المعلومات.

٣- تنظيم عقود تأمين تغطي مخاطر الافعال الجرمية بالوسائل الالكترونية.
٤- وضع الخطط اللازمة للوقاية من الافعال الجرمية الالكترونية وتحديثها باستمرار (مثل خطة الاستجابة للحوادث، خطة استمرار التشغيل اثناء وبعد حدوث كارثة، خطة التدريب على التدخل الفوري ...).
٥- انشاء فريق عمل مخصص للوقاية من الافعال الجرمية بالوسائل الالكترونية.
٦- تبادل المعلومات، المتعلقة بالأفعال الجرمية بالوسائل الالكترونية، مع الجهات المعنية داخل أو خارج المصرف أو المؤسسة المالية.
٧- توعية الموظفين والعملاء حول الوقاية من الافعال الجرمية الالكترونية.
٨- مراقبة اي تغيرات في عادات وسلوك الموظفين، سيما الذين يتمتعون بامتيازات هامة لدخول الانظمة المعلوماتية.
٩- التيقّظ والحذر لدى التعاقد مع جهات خارجية لتكليفها بمهام تتعلق بالانظمة الالكترونية والتأكد من ان هذه الجهات لا تقوم بالتعاقد مع ملتزمين ثانويين أقل موثوقية.

ثانياً: اجراءات تقنية تشمل:

١- اعتماد تقنية تعتمد على وسيلتين على الأقل للتأكد من هوية المستخدِمين من خارج المصرف أو المؤسسة المالية سيما لجهة حقهم بالدخول الى النظام.
٢- إستخدام تقنية ترميز كامل وآمن للبيانات الهامة جدا، منعاً لفقدانها أو التلاعب بها.
٣- اعتماد قواعد صارمة لجهة تفحص (Filtering) البريد الإلكتروني الوارد وضبط الوصول إلى علب البريد الإلكتروني من خارج المصرف أو المؤسسة المالية .
٤- تحديث انظمة اجهزة الكومبيوتر كافة والتحقق من امان الأجهزة الموضوعة بتصرف الموظفين لاستخدامها خارج المصرف او المؤسسة المالية.
٥- اختبار إمكانية الإختراق لكشف أي نقاط ضعف محتملة في الشبكة.
٦- مراقبة الحركة على الشبكة لكشف أي سلوك غير اعتيادي، سواء من خلال نوعية الحزم المرسلة أو عددها.
٧- التحقق من سلامة البيانات ومراقبتها بهدف كشف أي تلاعب غير مشروع بها، وتعقّب مصدر الوصول غير المشروع إليها.

ثانياً: اجراءات خاصة بالوقاية من الافعال الجرمية الالكترونية ذات الطابع المالي

المادة الثانية: على المصارف والمؤسسات المالية، كل في ما خصها، ان تقوم بشكل عام وعلى مسؤوليتها باتخاذ الاجراءات الادارية والتقنية والقضائية المناسبة للتنبه ورصد ومكافحة الجريمة الالكترونية المالية وبصورة خاصة:

١- الاخذ، بشكل خاص، بالإرشادات الواردة في البند (١) من الجزء الاول من "الدليل الارشادي للوقاية من الافعال الجرمية بواسطة البريد الالكتروني" كدلالة على افعال جرمية بالوسائل الالكترونية.

٢- اتباع "السياسات والاجراءات الوقائية من الافعال الجرمية" المحددة في البند (٢) من الجزء الاول من الدليل المنوه عنه اعلاه.

٣- وضع انظمة واجراءات داخلية مخصصة لتنفيذ طلبات تحويل الاموال الواردة اليها الكترونياً (بريد الكتروني، خدمة العمليات المصرفية الالكترونية (Electronic Banking)، ...)

٤- تضمين العقد الموقع مع العميل احكاماً خاصة تتعلق بتحديد وسائل اخرى غير البريد الالكتروني للاتصال بالعميل (كالاتصال الهاتفي مثلاً...) لتأكيد صحة طلبات التحاويل المرسلة الكترونياً على ان لا يتم تغيير هذه الوسائل الا بالاتفاق الخطي بين الطرفين.

٥- اعلام العميل عن المخاطر الناتجة عن استخدام البريد الالكتروني لطلب اجراء تحاويل مالية وتوجيهه لاستعمال وسائل اخرى اكثر اماناً والاستحصال على موافقته الخطية على تحمل هذه المخاطر.

٦- تزويد العميل بـ "الارشادات للأشخاص وسائر المؤسسات والهيئات غير المالية" موضوع الجزء الثاني من الدليل المنوه عنه اعلاه.

٧- الطلب من عملائها الابلاغ عن اية افعال جرمية بالوسائل الالكترونية قد تعرضوا لها فور علمهم أو اكتشافهم أو تبلغهم انهم وقعوا أو كادوا ان يقعوا ضحية لها.

المادة الثالثة: على المصارف والمؤسسات المالية، عند اكتشافها أو علمها أو تبلغها بأن أي من عملائها قد وقع ضحية افعال جرمية بالوسائل الالكترونية ذات طابع مالي، اتخاذ اجراءات سريعة وفعالة تشمل، على الاقل، الاجراءات التصحيحية الواردة في البند (٣) من الجزء الاول من الدليل المنوه عنه اعلاه، سيما:

١- تزويد كل من المصرف المراسل والمصرف المستفيد أو المؤسسة المالية المستفيدة بالمعلومات ذات الصلة كافة وطلب الغاء عملية التحويل واعادة قيمتها للعميل.

٢- ابلاغ هيئة التحقيق الخاصة بالمعلومات وبالمراسلات ذات الصلة ومن بينها المعلومات التقنية المتعلقة بما يلي:

- مصدر البريد الالكتروني (IP Address) المنسوب للعميل أو الذي تم عبره ارسال طلبات التحاويل المشبوهة.
- اسم الشركة مقدمة خدمة الانترنت التي تم عبرها ارسال طلبات التحاويل المشبوهة.
- اسم الشركة مقدمة خدمة الانترنت المستخدمة للولوج غير المصرح به الى حساب العميل عن طريق خدمة العمليات المصرفية الالكترونية (Electronic Banking).

٣- توجيه العميل لتقديم ابلاغ أو شكوى قضائية الى الجهات المختصة.

المادة الرابعة: تقوم "دائرة الامتثال" المنشأة لدى كل من المصارف والمؤسسات المالية بتطبيق احكام هذا القرار.

المادة الخامسة: يعمل بهذا القرار فور صدوره.

المادة السادسة: ينشر هذا القرار في الجريدة الرسمية.

بيروت، في ٢٨ تشرين الثاني ٢٠١٧
حاكم مصرف لبنان
رياض توفيق سلامه