موجز سياسات: العدد الرابع
يونيو 2019

إعداد:
د. محمد اسماعيل

صندوق النقد العربي
ARAB MONETARY FUND

الأمن السيبراني في القطاع المصرفي

- قطاع الخدمات المالية يشهد هجمات سيبرانية تفوق القطاعات الأخرى بنسبة 65 في المائة وفق تقديرات البنك الدولي.
- كلفة الهجمات السيبرانية في قطاع الخدمات المالية قد تصل إلى ما يقدر بنحو 270- إلى 350 مليار دولار سنوياً حال اتساع نطاق انتشارها وفق تقديرات صندوق النقد الدولي.
- إدراج المخاطر السيبرانية ضمن إطار المخاطر التشغيلية للمؤسسات المالية وحده يعتبر غير كافياً، حيث لابد من تبني المصارف لاستراتيجيات موثوقة مُعززة للأمن السيبراني.
- التعليمات الرقابية للمصارف المركزية العربية تُلزم المصارف بوضع لائحة من التعليمات لتأمين التطبيقات الإلكترونية، ومن أهمها تثبيت برامج حماية ضد الاختراق.
- إلزام المصارف العربية بإجراء اختبارات الضغط (Stress Testing) لتحديد حجم الآثار المترتبة على نجاح أية عمليات قرصنة تتعرض لها أنظمتها الإلكترونية.
- أهمية السعي المتواصل لتعزيز قدرات السلطات الإشرافية للرقابة على مخاطر الأمن السيبراني وبناء الكوادر في هذا المجال.

أولاً: تقديم

لقد أتاح التطور المذهل الذي شهدته صناعة التقنيات المالية الكثير من الفرص أمام المصارف نحو تعزيز مستوى الخدمات المقدمة للعملاء من خلال قنوات جديدة مبتكرة بعيداً عن القنوات التقليدية التي اعتادت عليها المصارف لتقديم الخدمات المصرفية لعملائها بما أحدث تحولاً جذرياً في طريقة عمل القطاع المصرفي. فقد ساهم التطور التقني في قيام المصارف بتقديم الخدمات المصرفية من خلال المعاملات الالكترونية، الأمر الذي أدى إلى توفير الوقت والمال والجهد من خلال تلك القنوات الجديدة المبتكرة .

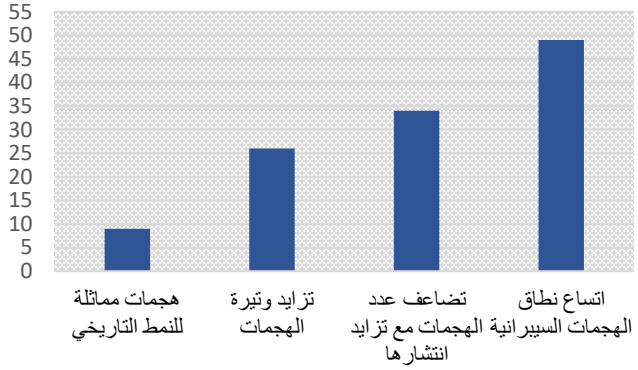
إن الفرص التي تخلقها تقنيات المعلومات والاتصالات تمثل تحدياً خاصاً للمؤسسات المصرفية، مع استمرارها في الابتكار في إيجاد وتقديم طرق جديدة للوصول إلى العملاء، فإن تلك المؤسسات تتعرض في الوقت نفسه لمخاطر جديدة. حيث إن الاستخدام الضار لتقنية المعلومات والاتصالات يمكن أن يؤدي إلى تعطيل الخدمات المالية الضرورية للأنظمة المالية الوطنية والدولية، وتقويض الأمن والثقة، وتعريض الاستقرار المالي للخطر. إن الهجمات السيبرانية تشكل تهديدًا للنظام المالي بأكمله، وهي حقيقة تؤكدها التقارير الصادرة في هذا الشأن على المستوى الدولي والإقليمي والمحلي. في هذا السياق، تشير تقارير البنك الدولي إلى تركز الهجمات السيبرانية في قطاع الخدمات المالية الذي شهد في عام 2016 هجمات سيبرانية تفوق القطاعات الأخرى بنسبة 65 في المائة بما يمثل زيادة بنسبة 29 في المائة عن العام السابق عليه[1].

من جانب آخر توضح تقديرات صندوق النقد الدولي للتكلفة الناتجة عن الهجمات السيبرانية في القطاعات المالية من واقع الخسائر المحققة جراء هجمات فعلية في 50 دولة حول العالم أن متوسط الخسائر السنوية المحتملة من الهجمات السيبرانية قد يكون كبيرًا بما يقدر بنحو 9 في المائة من صافي دخل البنوك على مستوى العالم، أو حوالي 100 مليار دولار في حال ما تشابهت هذه الهجمات مع مثيلاتها السابقة. أما في سيناريو شديد الخطورة - حيث يكون تواتر الهجمات السيبرانية أعلى مرتين مقارنة بمثيلاتها المسجلة في الماضي مع انتشار أكبر لنطاق الخسائر- يمكن أن تصل الخسائر إلى ثلاثة أضعاف هذا المستوى، أو ما يتراوح بين 270 إلى 350 مليار دولار[2].

[1] World Bank, (2018). "Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision", Feb.

[2] Lagarde C., (2018). "Estimating Cyber Risk for the Financial Sector", IMF Blog, June.

شكل رقم (1)
تكلفة الخسائر المحتملة للهجمات السيبرانية
في قطاع الخدمات المالية (كنسبة من صافي الدخل السنوي)



Lagarde C., (2018). "Estimating Cyber Risk for the Financial Sector", IMF Blog, June.

نتيجة لذلك، واعترافاً بالتهديدات الناجمة عن المخاطر السيبرانية، ومدى أهمية تعزيز قدرة الأجهزة المصرفية على تحمل هذه المخاطر والتحوط منها، فقد اتخذت السلطات الرقابية على مستوى العالم خطوات تنظيمية وإشرافية تهدف إلى تجنب أثر المخاطر السيبرانية على القطاع المصرفي. في هذا الصدد قامت المصارف المركزية العربية بإصدار التعليمات والتعاميم المصرفية التي تحث فيها البنوك نحو تعزيز قدراتها لمواجهة تلك الهجمات الالكترونية.

ثانياً: أهمية وجود معايير محددة تنظم المخاطر السيبرانية

تختلف الآراء حول كيفية تنظيم مخاطر الإنترنت، حيث يرى بعضها أن الطبيعة المتطورة للمخاطر السيبرانية ليست قابلة للتنظيم بشكل محدد، كما أن القضايا الخاصة بالإنترنت (cyber issues) يمكن معالجتها من خلال اللوائح الحالية المتعلقة بكل من المخاطر التشغيلية والتقنيات في القطاع المصرفي. فيما يشير البعض الآخر إلى أن هناك حاجة ملحة إلى وجود هيكل تنظيمي للتعامل مع الطبيعة الفريدة للمخاطر الإلكترونية، وذلك بالنظر إلى التهديدات المتزايدة الناتجة عن التحول المكثف نحو قطاع مالي رقمي في الآونة الاخيرة .

إن التطور الحادث في المخاطر السيبرانية يحفز المؤسسات المالية على البحث المستمر والمكثف نحو اتخاذ إجراءات وقائية من تلك المخاطر من خلال لوائح تجعل تلك الإجراءات أكثر وضوحاً أمام مجالس إدارات تلك المؤسسات، الأمر الذي يؤدي إلى خلق حافز أكبر على الاستثمار بشكل مستمر في تعزيز الأمن السيبراني.

إضافة إلى أن إدراج المخاطر السيبرانية ضمن المخاطر التشغيلية للمؤسسات المالية يعتبر غير كافي، حيث إن المعايير الرقابية على المصارف تتطلب أهمية تضمين الاستراتيجيات والسياسات الخاصة بتلك المصارف جزءً خاصاً بإدارة المخاطر السيبرانية، يتم مراجعتها بانتظام من قبل مجالس إدارات البنوك مع زيادة حجم المخاطر السيبرانية.

ثالثاً: الأطر والمعايير الدولية المُنظمة للمخاطر السيبرانية:

تغطي الأطر والمعايير الدولية للمخاطر السيبرانية المحاور التالية:

1. **الحوكمة الالكترونية (Cyber-governance):**
يتناول هذا البند مدى أهمية وجود استراتيجية للأمن السيبراني بحيث تضع كل مؤسسة مالية استراتيجية الأمن السيبراني الخاصة بها وفقًا لممارسات إدارة المخاطر المستندة إلى المبادئ. تقوم الجهات الرقابية بمراجعة هذه الاستراتيجيات كجزء من تقييمها للممارسات الشاملة لإدارة المخاطر في المؤسسة. كما أن جميع الجهات الرقابية تؤكد على أهمية الأدوار والمسؤوليات الإدارية والضوابط الخاصة بالحوكمة الإلكترونية. إضافة إلى أهمية تنمية الوعي الثقافي للأمن السيبراني للعملاء من خلال العاملين في القطاعات المالية.

كما تؤكد على أهمية توافر الكوادر المدربة القادرة على تحمل المسؤوليات والقيام بالمهام الوظيفية الموكلة اليها في مجال الأمن السيبراني .

2. **مفاهيم إدارة المخاطر واختبارها وكيفية التغلب على الانتهاكات (Approaches to risk management, testing and incident response and recovery):**

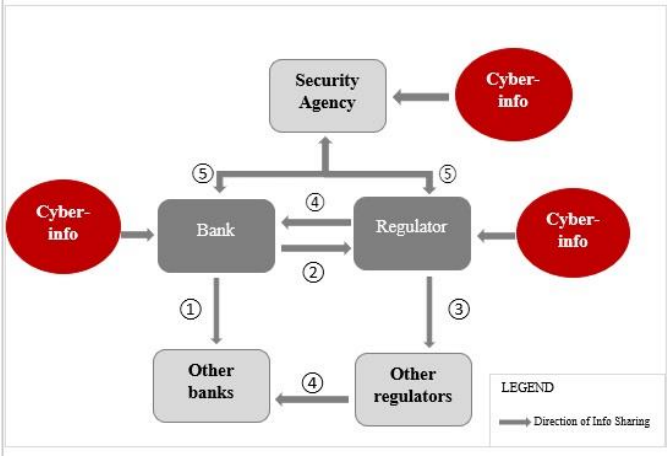
يشتمل هذا المحور أربع مفاهيم رئيسة تتمثل في طرق الرقابة على الأمن السيبراني (cyber-resilience)، ضوابط أمن المعلومات وطرق اختبارها وضمان استقلاليتها، مدى الاستجابة للتغلب على المخاطر، ومقاييس الأمن السيبراني والمرونة.

3. التواصل وتبادل المعلومات (Communication and sharing of information):

من بين الأنماط المتعارف عليها للتواصل في مجال مشاركة اهم الممارسات في مجال الامن السيبراني، يعتبر مشاركة المعلومات بين البنوك، والمشاركة بين البنك والجهات الرقابية، ومشاركة تلك المعلومات مع الأجهزة الأمنية من أكثر الممارسات المتعارف عليها في هذا المجال.

شكل رقم (2)

الأنماط المختلفة للتواصل في مجال الأمن السيبراني



The numbered circles next to the arrows indicate the "types" of info sharing.
Source: Basel Committee on Banking Supervision.

4. تعهيد أمن نظم المعلومات والأنظمة الإلكترونية إلى جهة ثالثة (Interconnections with third parties):

إن الاستخدام المكثف لخدمات التعهيد إلى طرف ثالث يزيد من التحدي أمام الهيئات والجهات الرقابية للحصول على رؤية كاملة للضوابط المعمول بها ومستوى المخاطر. تتمثل خدمات التعهيد الى جهة ثالثة في كافة أشكال الاستعانة بمصادر خارجية) بما في ذلك خدمات الحوسبة السحابية (cloud computing services، والخدمات والمنتجات المعيارية وغير المعيارية التي لا تعتبر عادةً مصادر خارجية power supply)، خطوط الاتصالات السلكية واللاسلكية، الأجهزة والبرامج التجارية، ...إلخ، والأطراف الأخرى مثل (المؤسسات المالية أو غير المالية) والمؤسسات المالية الدولية (مثل أنظمة الدفع والتسوية، منصات التداول، أمناء حفظ الأوراق المالية المركزية والأطراف المقابلة المركزية).

رابعاً: الجوانب المتعلقة بأمن الفضاء الإلكتروني في إطار المخاطر التشغيلية للبنوك المركزية العربية[3]

1. الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء السيبراني:

تتسم التعليمات الرقابية الصادرة من معظم السلطات الرقابية في الدول العربية، والخاصة بإطار المخاطر التشغيلية (Operational Risks)، بتضمنها جزءً متعلقاً بمخاطر نظم المعلومات وأمن الفضاء الإلكتروني في القطاع المصرفي يحدد المعايير اللازم توافرها لضمان أمن المعاملات المصرفية المنفذة عبر الفضاء الإلكتروني.

تتناول تلك التعاميم في معظم الدول العربية تعليمات خاصة بإدارة المعلومات والتقنية، ومخاطر الفضاء الإلكتروني، وتأدية المصارف لأعمالها من خلال الإنترنت. كما تشمل أيضاً تعليمات تتعلق بإدارة مخاطر العمل الإلكتروني والرقابة الداخلية، وكيفية مواجهة مخاطر الهجوم الإلكتروني والمخاطر الناتجة عن قرصنة البريد الإلكتروني .

إضافة إلى ذلك، تقوم معظم المصارف المركزية العربية بتضمين عمليات الرقابة على أساس المخاطر لاختبارات توضح مدى قدرة البنوك على مواجهة مخاطر أمن الفضاء الإلكتروني. حيث إن هناك تعليمات من السلطات الرقابية تلزم تلك المصارف بتضمين استراتيجيات المخاطر المُقرة من قبل مجالس إدارات البنوك، إطاراً يتعلق بالمخاطر الإلكترونية ومخاطر نظم المعلومات والهجمات الإلكترونية (Cyber attacks) ويتم التحقق من ذلك من خلال عمليات الرقابة، التي تتم بصورة دورية، بما يشمل وجود سياسة واضحة لحوكمة إدارة المخاطر السيبرانية في غالبية الدول العربية. بحيث تتضمن إجراءات لتحديد المخاطر، والحماية، واكتشاف التهديدات والتعامل معها، وخطط للمعالجة (Recovery plans) وتعيين مسؤول

[3] يعتمد هذا الجزء على نتائج استبيان أعده صندوق النقد العربي في هذا الصدد وتم استيفائه من قبل المختصين في المصارف المركزية ومؤسسات النقد العربية.

عن أمن المعلومات [Chief Information Security Officer (CISO)].

فيما يتعلق بالتعليمات الرقابية الصادرة عن السلطات الإشرافية في معظم الدول العربية، التي يتم فرضها على عمليات تعهيد أمن نظم المعلومات والأنظمة الإلكترونية للمصارف إلى جهة ثالثة(Third Party) ، فإن تلك التعليمات تلزم البنوك العربية بعقد الاتفاقات الملزمة (مع بنود المسؤولية المناسبة) والرقابة المستمرة الكافية، وضمان أن الأنظمة والإجراءات على مستوى الطرف الثالث كافية ولا تشكل أي تهديد أمني للنظام الإلكتروني للبنك.

هذا إضافة إلى قيام تلك السلطات في الدول العربية بإصدار العديد من التعليمات التي يجب اتباعها عند القيام بعمليات الإسناد الخارجي لخدمات تقنية المعلومات وتقديم الخدمات المصرفية عبر الإنترنت، من أهمها وجود إطار عمل لإدارة المخاطر وضمان جودة الخدمات المُقدمة من شركات الإسناد الخارجي، إضافة إلى القيام بعمليات دورية لتقييم المخاطر المتعلقة بالتعاقد مع مزودي هذه الخدمات. تجدر الإشارة إلى أن هناك بعض المصارف المركزية العربية التي تقوم بفرض الحصول على موافقة مسبقة منها قبل توقيع العقد مع أي شركة خارجية مزودة لتلك الخدمات وذلك على مستوى كافة المؤسسات المالية.

2. تنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الإنترنت

تتيح بعض الدول العربية للعملاء إنشاء أو فتح حساب مصرفي من خلال موقع البنك على شبكة الإنترنت، وذلك في ضوء عدد من الضوابط والتعليمات بالنسبة للمصرف والعميل. في هذا الإطار يقوم العميل باستيفاء المستندات المطلوبة لفتح الحساب عبر الوسائل الإلكترونية، وذلك بحيث لا يتم التشغيل الفعلي لحساب العميل إلّا بعد أن يقوم العميل بزيارة البنك المعني للتوقيع الخطّي على المستندات.

ويلتزم العميل باتباع الشروط والأحكام خاصة فيما يتعلق بالإبلاغ فور الشك في استخدام الحساب من قبل الغير بطريقة غير مسموح بها. تتمثل مسئولية البنك في اتخاذ الاعتبارات اللازمة نحو الحفاظ على سرية البيانات التي توثق وتحقق هوية العميل عند الاستفادة من الخدمات المصرفية عبر الإنترنت.

هذا، بينما لا يسمح البعض الآخر من الدول العربية للعميل بإنشاء أو فتح حساب مصرفي من خلال الإنترنت، ذلك لأنه وفقاً للتعليمات الصادرة عن السلطات الرقابية في تلك البلدان، فإن المصارف تلتزم بعدم السماح للعملاء الجدد بفتح حساب مصرفي باستخدام موقع البنك على شبكة الإنترنت. حيث يجب في هذا الإطار أن تطبق تلك المصارف قواعد التعرف على هوية العملاء والخاصة بمكافحة غسل الأموال وتمويل الإرهاب الصادرة من السلطات الرقابية في هذا الشأن.

فيما يخص العملاء الراغبين في الاستفادة من الخدمات المصرفية من خلال شبكة الإنترنت، تقوم البنوك في هذا الشأن بالحصول على توقيع يدوي من العميل على استمارة طلب الخدمة التي تحتوي على البيانات الأساسية للعميل كحد أدنى (البريد الإلكتروني، رقم الهاتف المحمول والأرضي، عنوان المراسلات)، كما تطبق المتطلبات والأحكام التي تحدد الحقوق والالتزامات بين المصارف والعملاء بشكل واضح .

كما تلتزم المصارف في معظم الدول العربية، وفقاً للتعليمات الصادرة عن السلطات الرقابية، بتطبيق أساليب يمكن الاعتماد عليها للتحقق من هوية وصلاحيات العملاء الراغبين في الاشتراك في خدمات الإنترنت البنكي. إضافة إلى ذلك تلتزم البنوك بتطبيق كافة الإجراءات والضوابط الرقابية التي تمكنها من تحديد هوية القائمين بأي معاملات الكترونية مرتبطة بالحسابات المصرفية، ذلك في الحالات التي يُسمح فيها لأكثر من مستخدم بالتعامل على حساب واحد. وتلتزم المصارف أيضا بالحصول على كافة المستندات القانونية اللازمة لإثبات تفويض الصلاحيات للمستخدمين بإجراء معاملات على حسابات الأشخاص الاعتبارية. يجب أيضا على البنوك في معظم الدول العربية القيام بإجراء عمليات التدقيق اللازمة للوثوق من هوية العميل عند طلبه إجراء أي تعديلات على البيانات الخاصة بخدمات الإنترنت البنكي الخاصة به، أو تعديل أي بيانات يستخدمها العميل لمتابعة أنشطة حساباته المصرفية.

3. وسائل إثبات الهوية عبر الإنترنت

تعتمد معظم البنوك في المنطقة العربية على استخدام مبدأ الدخول المزدوج (Tow Factor Authentication) للتحقق من هوية العميل المستفيد من الخدمات المصرفية من خلال الإنترنت، حيث تقوم المصارف المركزية بالدول العربية بصفتها السلطة الرقابية على الجهاز المصرفي بعملية التقييم الفني والأمني للخدمات المصرفية المقدمة من البنوك عبر الإنترنت. ذلك خاصة فيما يتعلق بالسرية والخصوصية والتحقق من الهوية وذلك قبل تقديم الخدمة للعميل. كما تقوم المصارف بالتقييم الأمني للخدمات المُقدمة من خلالها وذلك بصفة مستمرة وفق الإجراءات والقواعد الخاصة بالرقابة الداخلية المتبعة في كل بنك وقياس مدى فعالية الأداء والوسائل التقنية المستخدمة للتحقق من هوية العميل وقياس مؤشرات التعرض لحوادث أمن المعلومات. إضافة إلى ذلك تقوم معظم البنوك في الدول العربية بالاستعانة بشركات متخصصة للقيام بدراسة وتقييم مدى جاهزية الوسائل المستخدمة في التصدي للاختراق والقرصنة والبرامج الخبيثة. وغالباً تتم عملية التصديق والتحقق من هوية العميل إلكترونياً في معظم الدول العربية عن طريق قيام البنك بإرسال رسالة نصية إلى رقم الهاتف المحمول الخاص بالعميل.

كما تشير التعليمات والتعاميم الصادرة عن المؤسسات الرقابية في معظم الدول العربية، إلى أنه يتعين على كافة البنوك وضع حد أقصى للمحاولات الخاطئة للدخول على الموقع الإلكتروني للبنك وذلك بما لا يزيد عن 3 محاولات خاطئة في اليوم الواحد، ومن ثم يتم إيقاف التعاملات البنكية الإلكترونية. هذا، ولا تتم عملية إعادة التفعيل للخدمة إلا من خلال القنوات الآمنة مثل قيام العميل بالاتصال بمركز خدمة العملاء في البنك وتنفيذ الإجراءات المعتمدة والمطلوبة للتحقق من الهوية.

4. الضوابط والتعليمات الرقابية الخاصة بإدارة كلمة السر (Password)

وفقاً للتعليمات الصادرة عن معظم المصارف المركزية العربية، فإنه يجب على كل بنك مراعاة التدابير الرقابية عند التعامل مع كلمة السر الخاصة بالعملاء، بحيث يتم تطبيق الرقابة المزدوجة وأن يتم الفصل بين عملية إنشاء كلمات السر وتسليمها للعملاء وعملية تفعيل حسابات خدمات الإنترنت البنكي، وتعزيز تأمين عملية إنشاء كلمة السر لضمان عدم تعرضها للكشف. كما أنه يجب التأكد من أن كلمات السر لا يتم معالجتها أو إرسالها أو تخزينها كنص واضح، وإعطاء تعليمات لمستخدمي ومديري أنظمة الإنترنت البنكي لتغيير كلمة السر الصادرة فور الدخول إلى النظام لأول مرة، وتحديد مدة صلاحية كلمة السر من جانب المصرف. كما يجب على البنك إلزام العميل بعدم استخدام كلمة السر المنتهي صلاحيتها مرة أخرى، وفرض استخدام كلمات سر مُعقدة، وأن يتم تشفيرها باستخدام آلية تشفير قوية باستخدام التقنيات المناسبة، والحفاظ على تأمينها أثناء التسليم للعميل إما باليد أو إلكترونياً .

فيما يتعلق بالتعليمات والمواصفات الخاصة بكلمة السر التي تستخدم لمرة واحدة والصادرة باستخدام أجهزة رموز الأمان (OTP)، فقد قامت غالبية المصارف المركزية العربية بتحديد الحد الأدنى المطلوب في المواصفات الخاصة بكلمة السر لمرة واحدة، بأنه يجب ألا تقل كلمة السر عن 6 رموز وألا تزيد مدة صلاحيتها للاستخدام عن فترة 90 ثانية. كما يجب التأكد من أن النظام الخاص بإنشاء كلمة السر يوفر العشوائية الكافية من القيم الرمزية في هذا الشأن.

وبالنسبة لرموز الأمان (PIN)، تشير التعاميم الصادرة من غالبية السلطات الرقابية في الدول العربية بأنه يجب ألا يقل الرقم السري لجهاز رموز الأمان عن 4 أرقام بحيث يصعب التكهن بالأرقام. كما يجب أن يكون هناك حد أقصى للمحاولات الخاطئة لإدخال الرقم السري بحيث لا تزيد عن خمس محاولات. إضافة إلى ذلك، فإنه يجب على المصارف وضع إجراءات واضحة خاصة بإعداد الأرقام السرية الأولية، وإعادة تفعيل رموز الأمان الموقوفة، وتغيير الرقم السري عند أول استخدام وذلك في حالة إصداره عن طريق البنك .

5. عمليات تحويل الأموال من خلال خدمات الإنترنت

تلزم الضوابط والتعليمات الصادرة عن معظم السلطات الرقابية في الدول العربية البنوك التي تقدم خدمة تحويل الأموال من حسابات عملائها إلى حسابات أطراف أخرى من خلال الإنترنت، بوضع الضوابط المناسبة التي تساعد على خفض مستوى المخاطر المصاحبة لتلك الخدمة لتصل إلى مستوى مقبول ومعتمد من البنك. فقد أجازت تلك

التعليمات للمصارف استخدام وسيلة تصديق أحادية أو مزدوجة لعمليات تحويل الأموال بين الحسابات الخاصة لذات العميل داخل نطاق الدولة التابع لها، وعند سداد الالتزامات الناتجة عن بطاقات الائتمان أو القروض الخاصة بالعميل. كما أوصت تعليمات السلطات الإشرافية البنوك بتطبيق مبدأ الرقابة المزدوجة على تحويلات أموال الأشخاص الاعتبارية إلى مستفيدين آخرين، بحيث يلتزم المصرف بوضع حد أقصى يومي لعمليات تحويل الأموال من حسابات عملائها لصالح مستفيدين آخرين بحيث لا يكون هناك تعارض مع أي حدود أخرى يحددها المصرف في هذا الصدد. كما ألزمت تلك التعليمات المصارف في بعض الدول العربية بحظر تحويل أموال خارج الدولة عبر الإنترنت لا تتوافق مع التعليمات الصادرة من المصارف المركزية في هذا الخصوص.

6. سرية وسلامة المعلومات

تلزم التعليمات الصادرة عن المصارف المركزية العربية جميع المصارف باتخاذ كافة الإجراءات والتدابير الأمنية لضمان سرية وسلامة معلومات العملاء، حيث يجب على البنك القيام بعملية تقييم للمخاطر لتحديد المخاطر المحتمل وقوعها واتخاذ التدابير اللازمة للوقاية منها. كما يقوم المصرف المركزي بوضع معايير معينة لأدوات وبرامج الحماية التي يجب على البنك استخدامها، مثل كلمات السر الخاصة بالمعاملات المالية، والخدمات المقدمة من خلال الإنترنت، وخلاف ذلك من المعلومات السرية الأخرى الخاصة بالعملاء .

تتمثل الضوابط والتعليمات الصادرة عن المصارف المركزية العربية المعنية بسرية وسلامة المعلومات المرتبطة بالإنترنت البنكي، في أمن وسلامة البيانات والأنظمة، لضمان عدم تعديل معلومات العملاء وأن الأنظمة لا يمكن الوصول اليها بصورة غير مصرح بها، وكذا أهمية سرية بيانات العملاء وحفظها بشكل آمن. كما تتناول تلك التعليمات مدى أهمية موثوقية وتوافر أنظمة الخدمات المصرفية عبر الإنترنت لتوفير الوصول الفوري إلى النظم للمستخدمين المسجلين والحفاظ على الفعالية في التشغيل، وكذلك أهمية اتباع نهج استباقي للكشف عن المعاملات الاحتيالية المحتملة. إضافة الى ذلك، تتضمن التعاميم الصادرة من تلك السلطات الرقابية وسائل لتحقيق المسائلة عن طريق تصميم إجراءات التشغيل الموحدة والسياسات والضوابط لضمان إمكانية تتبع جميع المعاملات.

7. تأمين التطبيقات الإلكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الإنترنت

قامت معظم المصارف المركزية في الدول العربية بوضع لائحة من التعليمات لتأمين التطبيقات الإلكترونية الخاصة بالبنوك، ومن أهمها تثبيت برامج الحماية للحفاظ على هذه التطبيقات من الاختراق، بالإضافة إلى إجراء الاختبارات الأمنية على التطبيقات (قبل تثبيتها وبعده). كما تشير تلك التعليمات إلى ضرورة قيام البنوك بتقييم نقاط الضعف الموجودة في التطبيقات مرتين على الأقل سنوياً، والعمل على خطة للحد من نقاط الضعف ومشاركة الخطة مع الإدارة العليا. إضافة إلى العديد من التعليمات والضوابط الأخرى التي تهدف إلى حماية التطبيقات الإلكترونية المستخدمة في البنوك من الاختراقات.

قامت بعض الدول بإصدار تعاميم تؤكد أهمية اتباع منهجية تضمن توفير المتطلبات الأمنية ومتطلبات الجودة لدى تطوير أو شراء تلك التطبيقات (System Development Life Cycle)، بحيث تحقق المعايير الدولية ومتطلباتها بهذا الخصوص، وتوفير ضوابط الحماية الطبقية (أو في العمق) (Security in-depth) من خلال تفعيل ضوابط الحماية على مستويات: الشبكات، نظم التشغيل، الخوادم، قواعد البيانات، والتطبيقات، بالإضافة الى توفير ضوابط الحماية المادية والبيئية. كما يتعين على البنوك تطبيق مبادئ وقواعد الحوكمة السليمة لإدارة تكنولوجيا المعلومات داخل المصرف.

8. المخاطر المرتبطة بأمن نظم المعلومات والفضاء السيبراني

تفرض المصارف المركزية العربية على المصارف القيام بعمل اختبارات الضغط (Stress Testing) لتحديد حجم الآثار المترتبة على نجاح أية عمليات قرصنة تتعرض لها الأنظمة الإلكترونية بتلك المصارف، بصورة دورية سنوية أو نصف سنوية. كما يجب على البنك، وفقاً للتعليمات الرقابية الصادرة في هذا الشأن، الإبلاغ عن الاختراقات وأية عمليات قرصنة إلكترونية خلال ساعة من وقوعها في بعض الدول العربية (Cyber-event reporting)، في

غضـــون يوم أو يومين على الأكثر من التعرض في بعض الدول العربية الأخرى، وذلك لكافة حالات الخروقات الخاصة بأمن الفضاء الإلكتروني التي يترتب عليها خسائر ملموسة للعملاء وتؤثر سلباً على عمليات المصرف.

9. التعاون والتنسيق مع السلطات الرقابية الأخرى عبر الحدود والشركاء في صناعة تقنيات المعلومات

يتم التعاون بين المصارف المركزية العربية مع المؤسسات الإقليمية والســلطات الرقابية في الخارج وذلك من خلال المشـــاركة في اللجان المختلفة بهدف تبادل الخبرات والتعرف على أهم ما توصلت له هذه المؤسسات في مجال تطوير الأمن الإلكتروني في القطاع المالي. حيث تشـــارك الســـلطات الرقابية العربية في ورش العمل التي يتم عقدها على المســـتوى الإقليمي والدولي في مجال أمن المعلومات بهدف تبادل الخبرات ومناقشة التحديات وتوحيد الجهود في مجال الأمن السيبراني. كما يتم، من خلال التواجد في مثل هذه الفعاليات، تبادل المعلومات عن الهجمات السـيبرانية النشـــطة أو التهديدات المحتملة التي تواجهه القطاع المصـــرفي بالدول العربية، بهدف التعرف على كيفية مواجهة تلك التحديات واتخاذ ما يلزم من إجراءات واحترازات أمنية. إضـــافة الى قيام بعض المصـــارف المركزية العربية بالتواصـــل مع المصـــارف المركزية العالمية عن طريق عقد اجتماعات/المراسلات الإلكترونية لمناقشة أهم وسائل الحماية للتصدي للهجمات السيبرانية ووسائل التأمين والحماية.

إضافة إلى أنه يتم التعاون والتنسيق مع مختلف المؤسسات والمراكز البحثية من خلال توقيع اتفاقيات التدريب والتطوير والتعاون للبحث عن سبل تطوير أمن المعلومات في القطاع المالي. حيث قامت بعض الدول العربية بالتنســيق مع وزارات التربية والتعليم لتضـــمين التقنيات المالية وأمن ومخاطر أمن المعلومات في مناهج الوزارة وبمستويات مختلفة لرفع مستوى الوعي حول تقنية وأمن المعلومات. إلى جانب قيام المصـــارف المركزية العربية بالتنسيق مع الجهات الرقابية المحلية لتطبيق الاستراتيجيات الوطنية والقوانين المعتمدة في الدول العربية .

خامساً: بناء القدرات الرقابية والتحديات في مجال أمن نظم المعلومات والفضاء الإلكتروني

تقوم المصارف المركزية العربية بتدريب وتعزيز القدرات البشـــرية في القطاع المصـــرفي في مجال أمن الفضـــاء الإلكتروني مع الأخذ بالاعتبار المقترحات والمبادئ الرقابية الصادرة عن المؤسسات الدولية في هذا الشأن. ذلك من خلال تدريب العاملين في مجال الأمن الإلكتروني ومشـــاركتهم في الدورات التدريبية (الداخلية والخارجية) المتعلقة بأمن المعلومات. إضافة الى عقد البرامج التدريبية المتخصصة بالأمن السيبراني للعاملين من داخل وخارج القطاع المصـــرفي لتطوير المهارات والكفاءات الوطنية وذلك بإشراف شركات عالمية متخصصة في هذا المجال. حيث يخضع المتدربين إلى برامج تدريبية مكثفة يتم خلالها الاطلاع على أحدث الوسائل والأدوات والتقنيات، إضافة إلى التدريب الميداني والاختبارات المهنية. كما تقوم بعض المصـــارف المركزية العربية بتوجيه القطاع المصـــرفي بشـــكل عام إلى تكثيف الجهود لتهيئة وتعزيز القدرات البشـــرية في هذا المجال وذلك عن طريق دعم التعليم الأكاديمي والبعثات الدراســـية الخارجية للحصـــول على شهادات أكاديمية عليا من جامعات خارجية مرموقة.

في هذا الســـياق، تتمثل أهم التحديات التي تواجه الدول العربية في هذا الشأن في:

- التطور السريع في مجال تقنية المعلومات والاعتماد المتزايد على التقنيات للقيام بمعظم العمليات المالية، مما يؤدي إلى زيادة التعرض للتهديدات والحوادث الإلكترونية.
- الهجمات والقرصنة الإلكترونية الدولية التي تتعرض لها المصارف ببعض الدول العربية وآليه البنوك في التصدي لها ومدى فعالية الجدار الأمني في هذا الشأن.
- حداثة مفهوم الأمن السيبراني على مستوى الدول العربية والحاجة إلى تقوية الخبرات المصرفية في هذا المجال ببعض الدول العربية.
- ضمان تحقق الأمن السيبراني عند قيام المصارف بإجراء عقود لأطراف ثالثه تختص بأمن نظم المعلومات، للحد من وجود عمليات احتيال وقرصنة على الأنظمة الإلكترونية في تلك البنوك.

- الارتفاع النسبي في تكلفة تطبيق تقنيات أمن نظم المعلومات والفضاء السيبراني بصورة ملحوظة.
- صعوبة تطبيق ضوابط أمن نظم المعلومات والفضاء السيبراني نظراً لضعف ثقافة الأمن السيبراني لدى بعض العاملين في القطاع المالي والمصرفي.
- الحاجة إلى وجود آلية رقابة واضحة على البنوك والشركات المالية للتأكد من وجود ضوابط وسياسات لتحقيق الأمن السيبراني.

رابعاً: الانعكاسات على صعيد السياسات

- أهمية قيام الأجهزة الرقابية والمؤسسات بتوفير الدورات التدريبية العالية المستوى وتنظيم الندوات، وورش العمل والمؤتمرات بمشاركة الشركات والمؤسسات الدولية المتطورة في مجال تقنيات المعلومات لاطلاع الكوادر الفنية على أحدث التقنيات لمواكبة التطور السريع والتعرف على التقنيات الحديثة في مجال الخدمات الإلكترونية على المستوى العالمي. وذلك بهدف خلق كوادر فنية عالية قادرة على التصدي للتحديات الجديدة المرتبطة بهذه التقنيات وكيفية التغلب عليها.
- أهمية وضع الأجهزة الرقابية العربية لآلية رقابية واضحة على البنوك والمؤسسات المالية للتأكد من وجود ضوابط وسياسات لتحقيق الأمن السيبراني.
- أهمية حصول المؤسسات المالية والمصارف بالدول العربية على أحدث التقنيات الحديثة سواء فيما يتعلق بالأجهزة (Hardware)، أو البرامج (Software) لمواجهة أحدث التطورات والأساليب المتبعة في مجال الهجمات والقرصنة الإلكترونية الدولية، بهدف اقتناء جدار أمني أكثر فعالية وقادر على التصدي لأحدث الأساليب المتبعة في هذا الشأن.
- أهمية استحداث تخصص الأمن السيبراني في الجامعات العربية المتخصصة في مجال تقنية المعلومات أسوة بالجامعات العالمية، بهدف خلق الكوادر العربية المتخصصة ذات المستوى العالي في هذا المجال.
- قيام الهيئات والجهات الرقابية في الدول العربية بإصدار التعليمات والقواعد المنظمة الخاصة بقيام المصارف والمؤسسات المالية بإجراء عقود لأطراف ثالثه تختص بأمن نظم المعلومات، على تخضع تلك الشركات التي يتم التعهيد اليها للرقابة الصارمة من قبل الأجهزة الأمنية العربية للقضاء على عمليات الاحتيال والقرصنة على الأنظمة الإلكترونية في تلك البنوك والمؤسسات.
- أهمية قيام المصارف والمؤسسات المالية العربية بتخصيص الموارد والمخصصات الكافية للحصول على أحدث التقنيات في مجال أمن نظم المعلومات والفضاء السيبراني، حيث تتسم تلك التقنيات بالارتفاع الملحوظ في تكلفة اقتناءها.
- العمل على تكثيف التوعية لدى العملاء من خلال البرامج المسموعة والمرئية والندوات التثقيفية لرفع المستوى الخاص بثقافة الأمن السيبراني لدى المتعاملين بالقطاع المالي والمصرفي، بهدف تفهم الضوابط والتعليمات الخاصة بأمن نظم المعلومات والفضاء السيبراني.
- التأكيد على أهمية القيام باختبارات أوضاع ضاغطة جزئية وكلية تتضمن أثر المخاطر السيبرانية على البنوك.

للاطلاع على الإصدارات الأخرى من هذه السلسلة برجاء زيارة الموقع الإلكتروني لصندوق النقد العربي من خلال الرابط التالي:
www.amf.org.ae

صدر من هذه السلسلة:

- العدد الأول: النهوض بالمشروعات الصغيرة والمتوسطة في الدول العربية من خلال زيادة فرص نفاذها إلى التمويل. (مارس 2019).
- العدد الثاني: رقمنة المالية العامة. (ابريل 2019).
- العدد الثالث: العدالة الضريبية. (مايو 2019).
- العدد الرابع: أمن الفضاء السيبراني (يونيو 2019).