أمانة مجلس محافظي المصارف المركزية
ومؤسسات النقد العربية

الجوانب المتعلقة بأمن الفضاء الالكتروني في إطار المخاطر التشغيلية: تجارب رقابية عربية

اللجنة العربية للرقابة المصرفية

إعداد: د. محمد إسماعيل

صندوق النقد العربي
ARAB MONETARY FUND

مجلس محافظي المصارف المركزية ومؤسسات النقد العربية
Council of Arab Central Banks and Monetary Authorities Governors

رقم
112
2019

أمانة
مجلس محافظي المصارف المركزية
ومؤسسات النقد العربية

الجوانب المتعلقة بأمن الفضاء الالكتروني في إطار المخاطر التشغيلية: تجارب رقابية عربية

اللجنة العربية للرقابة المصرفية

إعداد
د. محمد إسماعيل

صندوق النقد العربي
أبوظبي – دولة الإمارات العربية المتحدة

تـقديـم

أرسـى مجلس محافظي المصـارف المركزية ومؤسـسـات النقد العربية تقليداً منذ عدة سـنوات، بدعوة أحد أصـحاب المعالي والسـعادة المحافظين لتقديم ورقة عمل حول تجربة دولته في أحد المجالات ذات العلاقة بعمل المجلس. كما يصـدر عن اللجان وفرق العمل المنبثقة عن المجلس، أوراق عمل تتناول الموضوعات والقضايا التي تناقشها هذه اللجان والفرق. إضافة إلى ذلك، يعد صندوق النقد العربي ضمن ممارسته لنشاطه كأمانة فنية لهذا المجلس، عدداً من التقارير والأوراق في مختلف الجوانب النقدية والمصـــرفية التي تتعلق بأنشـطة المصـارف المركزية ومؤسـسـات النقد العربية. وتعد هذه التقارير والأوراق من أجل تسهيل اتخاذ القرارات والتوصيات التي يصدرها المجلس. وفي ضـــوء ما تضـــمنته كل هذه الأوراق والتقارير من معلومات مفيدة عن موضوعات ذات صلة بأعمال المصارف المركزية، فقد رأى المجلس أنه من المناســب أن تتاح لها أكبر فرصـــة من النشـــر والتوزيع. لذلك، فقد باشـــر الصـــندوق بنشـــر هذه الســـلســـة التي تتضـــمن الأوراق التي يقدمها الســـادة المحافظين إلى جانب التقارير والأوراق التي تعدها اللجان والصـــندوق حول القضـــايا النقدية والمصـــرفية ذات الأهمية. ويتمثل الغرض من النشـــر، في توفير المعلومات وزيادة الوعي بهذه القضـــايا. فالهدف الرئيســـي منها هو تزويد القارئ بأكبر قدر من المعلومات المتاحة حول الموضـــوع. نأمل أن تساعد هذه السلسة على تعميق الثقافة المالية والنقدية والمصرفية العربية.

والله ولي التوفيق،

عبد الرحمن بن عبد الله الحميدي
المدير العام رئيس مجلس الإدارة
صندوق النقد العربي

المحتـــــــويات

تمهيد

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 أن 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 المستويات الدولي والإقليمي والمحلي.

نتيجة لذلك، واعترافاً بالتهديد الناجم 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 تلك المخاطر السيبرانية على المصارف. في هذا الصدد قامت المصارف المركزية العربية بإصدار التعليمات والتعاميم المصرفية التي تحث فيها البنوك على تعزيز قدراتها لمواجهة تلك الهجمات الالكترونية.

في ضوء ما سبق، قام صندوق النقد العربي بإعداد استبيان حول الجوانب المتعلقة بأمن الفضاء الالكتروني (Cyber Security) في إطار المخاطر التشغيلية بهدف استعراض التجارب الرقابية العربية. تستعرض هذه الدراسة نتائج الاستبيان، حيث سيتم البدء باستعراض الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني، والضوابط والتعليمات الخاصة بتنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الانترنت في الدول العربية. ثم يتم تناول الضوابط والتعليمات الخاصة بتنظيم وسائل اثبات الهوية عبر الانترنت، وإدارة كلمة السر، وعمليات تحويل الأموال من خلال خدمات الانترنت.

إضافة الى ذلك، تستعرض الدراسة الضوابط والتعليمات الرقابية الخاصة بسرية وسلامة المعلومات، وبتأمين التطبيقات الالكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الإنترنت. كما يتناول تقييم السلطات الرقابية في الدول العربية للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني والوضع الراهن، والتعاون والتنسيق مع السلطات الرقابية الأخرى عبر الحدود والشركاء في صناعة تقنيات المعلومات فيما يتعلق بالمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني، وبناء القدرات الرقابية في هذا المجال. بعد ذلك تتطرق الدراسة إلى التحديات الرقابية التي تواجه الأجهزة المصرفية العربية في مجال أمن نظم المعلومات والفضاء الإلكتروني. في نهاية الدراسة، سيتم عرض تجارب الدول العربية في الجوانب المتعلقة بأمن الفضاء الالكتروني.

أولاً: الجوانب المتعلقة بأمن الفضاء الالكتروني في إطار المخاطر التشغيلية للبنوك المركزية العربية

1. الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

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 المصرفي 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 أن 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 المصرفية، التي تتم بصورة دورية، بما يشمل وجود سياسة واضحة لحوكمة إدارة مخاطر أمن الفضاء الإلكتروني في غالبية الدول العربية. بحيث تتضمن إجراءات لتحديد المخاطر، والحماية، واكتشاف

التهديدات والتعامل معها، وخطط للمعالجة (Recovery plans) وتعيين مسؤول عن أمن المعلومات [Chief Information Security Officer (CISO)].

فيما يتعلق بالتعليمات الرقابية الصادرة عن السلطات الإشرافية في معظم الدول العربية، والتي يتم فرضها على عمليات تعهيد أمن نظم المعلومات والأنظمة الإلكترونية للمصرف 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 أهم تلك التعليمات وجود إطار عمل لإدارة المخاطر وضمان جودة الخدمات المُقدمة من شركات الاسناد الخارجي، إضافة إلى القيام بعمليات دورية لتقييم المخاطر المتعلقة بالتعاقد مع تلك الشركات. 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 مشروعة. 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 الشروط والأحكام التي تحدد الحقوق والالتزامات بين المصارف والعملاء بشكل واضح.

كما تلتزم البنوك 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 يصرح فيها لأكثر من مستخدم بالتعامل على حساب واحد. وتلتزم المصارف أيضاً بالحصول على كافة المستندات القانونية اللازمة لإثبات تفويض الصلاحيات للمستخدمين بإجراء معاملات على حسابات الأشخاص الاعتبارية. يجب أيضاً 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 Factors Authentication) في التحقق 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 البنوك 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 الى النظام لأول مرة، وتحديد مدة صلاحية كلمة السر من جانب البنك. 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 يدوياً 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 تكون كلمة السر أقل من 6 رموز وألا تزيد مدة صلاحيتها للاستخدام عن زمن 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)، أشارت التعاميم الصادرة من غالبية السلطات الرقابية في الدول العربية بأنه يجب ألا يقل الرقم السري لجهاز رموز الأمان عن 4 أرقام بحيث تكون أرقام يصعب التكهن بها. كما يجب أن يكون هناك حد أقصى للمحاولات الخاطئة لإدخال الرقم السري بحيث لا تزيد عن خمس محاولات. إضافة إلى ذلك، فإنه يجب على البنوك 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، وضع الضوابط المناسبة التي تساعد على خفض مستوى المخاطر المصاحبة لتلك الخدمة لتصل إلى مستوى مقبول ومعتمد من البنك. فقد أجازت تلك التعليمات للبنوك 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 أخرين، 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 البنوك المركزية في هذا الخصوص.

6. سرية وسلامة المعلومات

التعليمات الصادرة عن البنوك المركزية العربية تلزم 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 البنوك 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 الإلكتروني

تفرض البنوك 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 غضون 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 البنوك المركزية العربية مع المؤسسات الإقليمية والسلطات الرقابية في الخارج وذلك من خلال المشاركة في اللجان المختلفة بهدف تبادل الخبرات والتعرف على أهم ما توصلت له هذه المؤسسات في مجال تطوير الأمن الإلكتروني في القطاع المالي. حيث تشارك السلطات الرقابية العربية في ورش العمل التي يتم عقدها على المستوى 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 السيبرانية النشطة أو التهديدات المحتملة التي تواجهه القطاع المصرفي بالدول العربية، بهدف التعرف على كيفية مواجهة تلك التحديات واتخاذ ما يلزم من إجراءات واحترازات أمنية. إضافة الى قيام بعض البنوك المركزية العربية بالتواصل مع البنوك 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 بالتنسيق مع وزارات التربية والتعليم لتضمين التقنيات المالية وأمن ومخاطر أمن المعلومات في مناهج الوزارة وبمستويات مختلفة لرفع مستوى الوعي حول تقنية وأمن المعلومات. إلى جانب قيام البنوك المركزية العربية بالتنسيق مع الجهات الرقابية المحلية لتطبيق الاستراتيجيات الوطنية والقوانين المعتمدة في الدول العربية.

10.بناء القدرات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

تقوم المصارف المركزية العربية بتدريب وتعزيز القدرات البشرية في القطاع المصرفي في مجال أمن الفضاء الإلكتروني مع الأخذ بالاعتبار المقترحات والمبادئ الرقابية الصادرة عن المؤسسات الدولية في هذا الشأن. ذلك من خلال تدريب العاملين في مجال الأمن الإلكتروني ومشاركتهم في الدورات التدريبية (الداخلية والخارجية) المتعلقة بأمن المعلومات. إضافة الى عقد البرامج التدريبية المتخصصة بالأمن السيبراني للعاملين من داخل وخارج القطاع

المصرفي 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 المصارف المركزية العربية بتوجيه القطاع المصرفي بشكل عام إلى تكثيف الجهود لتهيئة وتعزيز القدرات البشرية في هذا المجال وذلك عن طريق دعم التعليم الأكاديمي والبعثات الدراسية الخارجية للحصول على شهادات أكاديمية عليا من جامعات خارجية مرموقة.

11.التحديات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

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، فيما يلي عرض لأهم تلك التحديات:

- التطور السريع وظهور تقنيات جديدة في مجال الخدمات الإلكترونية على المستوى العالمي، مما أدى إلى ظهور تحديات جديدة مرتبطة بهذه التقنيات وكيفية التعامل معها.
- الهجمات والقرصنة الإلكترونية الدولية التي تتعرض لها المصارف ببعض الدول العربية وآليه البنوك في التصدي لها ومدى فعالية الجدار الأمني في هذا الشأن.
- ضعف مستوى الخبرات المصرفية في هذا المجال ببعض الدول العربية.
- حداثة مفهوم الأمن السيبراني على مستوى الدول العربية.

- قيام بعض المصارف في بعض الدول بإجراء عقود لأطراف ثالثه تختص بأمن نظم المعلومات مما أدى إلى وجود عمليات احتيال وقرصنة على الأنظمة الإلكترونية في تلك البنوك.
- الارتفاع النسبي في تكلفة تطبيق تقنيات أمن نظم المعلومات والفضاء الإلكتروني بصورة ملحوظة.
- تواجه معظم الدول العربية صعوبة في تطبيق ضوابط أمن نظم المعلومات والفضاء السيبراني نظراً لضعف ثقافة الأمن السيبراني لدى القطاع المالي والمصرفي في هذا المجال.
- تواجه بعض الدول العربية التحدي الخاص بعدم وجود آلية رقابة واضحة على البنوك والشركات المالية للتأكد من وجود ضوابط وسياسات لتحقيق الأمن السيبراني في هذا الصدد.
- عدم وجود سياسات لنظم الأمن السيبراني لدى بعض المصارف، في بعض الدول العربية، والتي تعتبر متطلب رقابي.

ثانياً: استعراض تجارب المصارف المركزية العربية في مجال أمن الفضاء الإلكتروني

الأردن

1. الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

تتضمن التعليمات الرقابية الخاصة بإطار المخاطر التشغيلية في الأردن جزءً متعلقاً بمخاطر نظم المعلومات وأمن الفضاء الإلكتروني في القطاع المصرفي، بهدف تحديد المعايير اللازم توافرها لضمان أمن الفضاء الإلكتروني. تتمثل

أبرز التعليمات الرقابية الصادرة عن البنك المركزي الأردني في هذا الخصوص في كل من تعليمات الحاكمية المتعلقة بإدارة المعلومات والتقنيات المصاحبة لها، وتعليمات التكيف مع المخاطر السيبرانية، وتعليمات ممارسة البنوك لأعمالها بوسائل إلكترونية، وتعليمات خطة استمرارية العمل. إضافة الى تعميم مبادئ إدارة مخاطر العمل المصرفي الإلكتروني، وتعليمات أنظمة الضبط والرقابة الداخلية، وتعليمات أجهزة الصراف الآلي، وتعميم مخاطر الاختراق الإلكتروني، وتعميم التحوط لمواجهة مخاطر الهجوم الإلكتروني (Ransomware)، وتعميم التحوط لمخاطر احتيال البريد الإلكتروني، والدليل الإرشادي للحوسبة السحابية، وتعاميم الحصول على شهادة الامتثال لمعيار أمن وحماية بيانات بطاقات الدفع.

كما تتضمن عمليات الرقابة على أساس المخاطر (ongoing risk-based supervisory activities) اختبارات توضح مدى قدرة المصارف على مواجهة مخاطر أمن الفضاء الإلكتروني من خلال تعليمات الحاكمية وإدارة المعلومات والتقنيات المصاحبة لها، تنص على أن تكرار التدقيق لكافة المحاور أو جزء منها كحد أدنى مرة واحدة سنوياً على الأقل في حال تم تقييم المخاطر بدرجة (4 أو5) بحسب سلم تقييم المخاطر، ومرة واحدة كل سنتين على الأقل في حال تم تقييم المخاطر بدرجة (3)، ومرة واحدة كل ثلاث سنوات على الأقل في حال تم تقييم المخاطر بدرجة (1 أو2).

فيما يتعلق بتنظم تقديم الخدمات المصرفية من خلال الإنترنت، أصدرت السلطات الرقابية بالأردن تعليمات وقواعد في هذا الخصوص في عامي 2001 و2005. تمثلت الخدمات المصرفية المشمولة في نطاق تطبيق هذه القواعد في كل من الخدمات التنفيذية مثل التحويل من حساب عميل لحساب آخر في بنك

آخر، والخدمات الاتصالية مثل البريد الإلكتروني، والخدمات المعلوماتية مثل الاستعلام عن الخدمات.

بالنسبة للتعليمات الرقابية التي تُفرض على عمليات تعهيد أمن نظم المعلومات والأنظمة الإلكترونية للمصرف إلى جهة ثالثة (Third Party)، فإن كافة التعليمات المُصدرة بهذا الخصوص تفرض ضوابط على البنوك واجبة التطبيق سواء تم تنفيذها من قبل الاستعانة بموارد البنك أو بموارد الغير، ويتم ذكر ذلك صراحة عند إصدار تلك التعاميم والتعليمات، منها على سبيل المثال تعليمات الحاكمية وإدارة المعلومات والتقنيات المصاحبة لها، والتعليمات الخاصة بالتكيف مع المخاطر السيبرانية التي تتضمن تعليمات الإسناد الخارجي الفني والتقني لشركات خدمات الدفع والتحويل الإلكتروني للأموال (فيما يخص البنوك في حال كانت مُشغلة أو مديرة لأنظمة الدفع).

إضافة الى ذلك، يتم خلال عمليات الرقابة المصرفية التحقق من وجود استراتيجية للمخاطر مُقرة من قبل مجالس إدارات البنوك تتضمن مستوى المخاطر المتعلقة بأمن الفضاء الإلكتروني وإجراءات موازية لدعم مستويات أمن الفضاء الإلكتروني (cyber resilience) بما يشمل وجود سياسة واضحة لحوكمة إدارة مخاطر أمن الفضاء الإلكتروني وتعيين مسؤول عن أمن المعلومات [Chief Information Security Officer (CISO)].

2. الضوابط والتعليمات الخاصة بتنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الإنترنت

أشار البنك المركزي الأردني بأنه لا يوجد ما يمنع البنوك بموجب التعليمات الرقابية من فتح الحسابات للعملاء عبر الإنترنت طالما تم الامتثال لمتطلبات التعليمات الصادرة في هذا الشأن، وخاصة فيما يتعلق بعمليات التوثيق والتحقق

من هوية العميل صاحب الحساب عبر وسائل تقنية المعلومات المتاحة وقبل إجراء أي عمليات تشغيلية أو مالية على حسابات وبيانات العميل لدى البنك، وطالما تم توفير الضوابط بمستوياتها المختلفة المطلوبة بموجب التعليمات (الضوابط الرادعة والمانعة والكاشفة والتصحيحية).

تتمثل الضوابط والتعليمات (الشروط والأحكام) التي يطبقها البنك على العميل الراغب في الاستفادة من الخدمات المصرفية من خلال شبكة الإنترنت في وجوب تغيير الرمز السري لدى أول استخدام للخدمة الإلكترونية وتغييره في حال الشك بمعرفته من قبل الغير، وإبلاغ البنك فور ضياع وسيلة توثيق هوية العميل أو فور الشك باستخدام الغير لحسابات العميل بطريقة غير مشروعة. إضافة إلى أن إدارة مخاطر الخدمات المصرفية الإلكترونية من مسؤولية إدارة البنك، ممثلة بمجلس الإدارة والإدارة التنفيذية العليا، الأمر الذي يتطلب بذل العناية اللازمة للاحتفاظ بسرية البيانات التي توثق وتحقق هوية العميل لدى التعامل بالوسائل الإلكترونية. كما أنه يجب القيام ببرامج توعوية تقدم من قبل البنك لعميله بخصوص الاستخدام الآمن للخدمات المصرفية الإلكترونية.

فيما يخص الضوابط والأساليب التي يعتمد عليها البنك في التحقق من هوية وصلاحية العميل الراغب في الاستفادة من الخدمات المصرفية (أو الراغب في تنفيذ أنشطة مصرفية) من خلال شبكة الإنترنت، فإن تلك الضوابط تتمثل في اسم المستخدم والرمز السري، وجهاز توليد الرقم السري (Token)، وكلمة السر المستخدمة لمرة واحدة [One Time Password (OTP)]. وتطبق تلك الضوابط والأساليب أيضاً في التحقق من هوية وصلاحية المخولين بالاستفادة من الخدمات المصرفية (أو الراغبين في تنفيذ أنشطة مصرفية) من

خلال شبكة الانترنت وذلك في حالة وجود أكثر من شخص يمكنهم التعامل على نفس الحساب، وفي حالة الحسابات الخاصة بالأشخاص الاعتباريين.

كما أنه يتم تفعيل الضوابط الكافية للتأكد من هوية العميل قبل تنفيذ التعديلات الخاصة ببيانات حساب العميل (أو إعادة تفعيل الحساب – اصدار كلمة سر جديدة – أي تعديلات أخرى)، وقد يلزم ذلك قيام العميل بمراجعة فرع البنك شخصياً لإجراء التعديل المطلوب أو استكماله، وفي حال تم تلقي طلب التعديل عبر مركز الخدمة يتم ذلك بعد التحقق من قيام العميل بالإجابة على عدد من الأسئلة الشخصية المعروفة إجابتها للعميل وتكون محفوظة بسرية لدى البنك.

3. الضوابط والتعليمات الخاصة بتنظيم وسائل إثبات الهوية عبر الإنترنت

تشمل الوسائل التي تعتمد عليها البنوك في التحقق من هوية العميل المستفيد من الخدمات المصرفية من خلال الإنترنت كل من إسم المستخدم والرمز السري، والرمز السري لمرة واحدة (OTP)، وجهاز توليد الرقم السري (Token). تقوم البنوك بتقييم الوسائل التي تعتمد عليها في التحقق من هوية العميل بحيث تكون مناسبة من الناحية الأمنية وغير معرضه للقرصنة أو للتهديد عن طريق البرامج الخبيثة وبرامج التجسس من خلال إلزام البنوك بموجب التعليمات وبموجب تقارير التفتيش الدورية بما يلي:

- إجراء فحوصات اختبار وتحديد للثغرات (Penetration Test and Vulnerability Assessment) للأنظمة المعرضة للشبكات الخارجية وللإنترنت بشكل دوري.
- اتباع دليل محكم في تطوير وشراء وفحص وتشغيل البرامج والأنظمة التابعة لها يحاكي أفضل الممارسات الدولية بهذا الخصوص لتوفير متطلبات أمن المعلومات ومتطلبات الجودة.

- تقييم ضوابط الخدمات المصرفية الإلكترونية من قبل التدقيق الداخلي والخارجي في البنك بشكل دوري.

كما تقوم البنوك بشكل مستمر بتوعية عملائها وإبلاغهم بأنها لا تطلب منهم تقديم أية بيانات تتعلق بهوية العميل عبر البريد الإلكتروني أو الهاتف أو الإنترنت، وفي حال تلقي العميل مثل هذه الرسائل التجسسية بغرض معرفة هويته الإلكترونية، يجب عليه عدم التجاوب وإبلاغ البنك فوراً. إضافة إلى ذلك، فإنه بخلاف الوسائل التي يوفرها البنك لعملائه للتحقق من هويته على العميل عدم التجاوب مع أي وسائل أخرى مشبوهة بهذا الخصوص.

في هذا الإطار، تقوم البنوك بتوثيق هوية العميل عبر الإنترنت في الغالب من خلال وسيلتين لتوثيق الهوية (Dual Factor Authentication) مثلاً: (إسم تعريف غير مرتبط ببيانات هوية العميل ومعروف للعميل فقط، متبوع برمز سري ثابت، متبوعاً برمز سري متغير باستمرار من خلال جهاز توليد الرمز السري الموجود بحوزة العميل ويسمى (Token) أو OTP). كما تقوم بعض البنوك بتفعيل ضابط إقفال الحساب بشكل مؤقت أو بشكل دائم في حال عدد محدد (3 أو 5) محاولات نفاذ فاشلة، ويلزم بعدها العميل الاتصال أو مراجعة فرعه لإثبات هويته وإعادة تفعيل حسابه عبر الإنترنت، إلا أن تفعيل مثل هذا الضابط يعطل ويحجب استخدام العميل لحساباته عبر قناة الإنترنت. بالإضافة إلى قيام البنوك بتوفير الضوابط الكاشفة من خلال إبلاغ العميل بنفاذه أو بأية تغييرات تطرأ على حساباته من خلال الرسائل النصية القصيرة (SMS) وما شابهها.

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

تشير التعليمات الصادرة في هذا الصدد إلى أن كلمة السر (Password) يجب أن تحتوي على أرقام وحروف بحد أدنى 8 خانات، تحتوي على رموز عليا ودنيا (Upper and lower cases)، لا تحتوي على عناصر مكررة أو مأخوذة من بيانات هوية العميل وتاريخ ميلاده، ألا تتشابه مع آخر (7) رموز سرية سابقة، وأن يتم تغييرها بشكل مستمر، وأن تكون مقنعة (Masked). أما بالنسبة لكلمة السر التي تستخدم لمرة واحدة والصادرة باستخدام أجهزة رموز الأمان (OTP)، فإنها تستخدم لمرة واحدة، وتكون مرتبطة بعملية أو حركة واحدة فقط، وتكون صالحة للاستخدام لفترة زمنية محددة.

5. الضوابط والتعليمات الرقابية الخاصة بعمليات تحويل الأموال من خلال خدمات الإنترنت

تتمثل الضوابط والتعليمات الصادرة عن البنك المركزي والخاصة بتحويل الأموال من حسابات العملاء إلى حسابات أطراف أخرى من خلال خدمات الإنترنت البنكي بهدف الحد من المخاطر المصاحبة لعملية التحويل، فيما يلي:

- إسم المستخدم والرمز السري.
- الرمز السري لمرة واحدة (OTP).
- جهاز توليد الرقم السري (Token).
- سقوف تحويل يومي.
- إبلاغ العميل عن كل حركة مالية فور تحققها من خلال الرسائل النصية القصيرة (SMS) على سبيل المثال.

- بعض البنوك توفر هذه الخدمة للاتصال فقط، أي يتم تقديم طلب الحوالة عبر الإنترنت (Real-time on-line) ويتم في اليوم التالي استكمال تنفيذها (Off-line) من خلال عمليات وأقسام البنك الداخلية بحضور العميل شخصياً لفرع البنك لإثبات طلب التحويل.
- تعليمات المتطلبات الفنية والتقنية لشركات خدمات الدفع والتحويل الإلكتروني للأموال.

6. الضوابط والتعليمات الرقابية الخاصة بسرية وسلامة المعلومات المتعلقة بالإنترنت البنكي

تتمثل الضوابط والتعليمات الصادرة عن البنك المركزي الأردني في هذا الشأن، في أن يتم توعية العميل بضرورة التأكد من أصلية موقع البنك عبر الإنترنت قبل الشروع بإدخال بيانات توثق وتحقق هويته، من خلال التأكد من البرتوكول المستخدم (0https) على سبيل المثال. إضافة الى تشفير بيانات وجلسة الاتصال بين جهاز العميل وجهاز البنك باستخدام بروتوكولات مثل (https) بطول مفتاح تشفير مناسب. كما يقوم البنك بتوفير البنية التحتية التقنية الضامنة لحماية وسرية البيانات المنقولة مثل أجهزة (Firewalls) و(IDS, IPS). كما يقوم بتوفير خدمات أمن وحماية المعلومات من خلال ما يسمى (Security Operations Center) وغيرها من الضوابط الإدارية والتنظيمية المتعلقة بحوكمة تقنيات المعلومات.

7. الضوابط والتعليمات الرقابية الخاصة بتأمين التطبيقات الإلكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الإنترنت

تشمل الضوابط والتعليمات الصادرة بشأن تأمين التطبيقات الإلكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الإنترنت لضمان الحماية الفعالة لهذه التطبيقات ما يلي:

- اتباع منهجية تضمن توفير المتطلبات الأمنية ومتطلبات الجودة لدى تطوير أو شراء تلك التطبيقات (System Development Life Cycle)، تحقق المعايير الدولية ومتطلباتها بهذا الخصوص.
- توفير ضوابط الحماية الطبقية (أو في العمق) (Security in-depth) من خلال تفعيل ضوابط الحماية على مستويات: الشبكات، نظم التشغيل، الخوادم، قواعد البيانات، التطبيقات بالإضافة لتوفير ضوابط الحماية المادية والبيئية.
- تطبيق قواعد الحوكمة السليمة لإدارة موارد تقنيات المعلومات.

8. تقييم السلطات الرقابية للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني والوضع الراهن

تمثلت أبرز حالات الانتهاكات الخاصة بأمن الفضاء الإلكتروني التي تعرض لها القطاع المصرفي الأردني خلال عامي 2017 و2018، مرتبة حسب أهميتها، فيما يلي:

جدول رقم (1)
أبرز حالات الانتهاكات الخاصة بأمن الفضاء الإلكتروني التي تعرض لها القطاع المصرفي الأردني
خلال عامي 2017 و2018

نوع الهجمات	يتم تقييم أهمية حدوث كل حالة كما يلي: 1 (ترمز الى تكرار الحدوث) 2 (متوسطة الحدوث) 3 (نادرة الحدوث)
• برمجيات خبيثة (Malware)	**2**
• هجوم إلكتروني سطحي (اختراق سطحي لموقع المصرف على الانترنت يتسبب في إيقاف عمل الموقع، أو تغيير الصفحة الرئيسية).	**3**
• هجوم إلكتروني يتسبب في وقف نظام آلي عن العمل (نظام مدفوعات، نظام شراء إلكتروني، من خلال إرسال طلبات وهمية ضخمة في الثانية الواحدة).	**3**
• اختراقات/ سرقة بيانات العملاء أو الحسابات المصرفية.	**2**

نوع الهجمات	يتم تقييم أهمية حدوث كل حالة كما يلي: 1 (ترمز الى تكرار الحدوث) 2 (متوسطة الحدوث) 3 (نادرة الحدوث)
• أخرى (يرجى ذكرها: رسائل الاصطياد عبر البريد الالكتروني (Phishing Email)	1
• هجمات الكترونية على الخدمات المنشورة عبر شبكة الانترنت.	2

المصدر: البنك المركزي الأردني من خلال. "استبيان الجوانب المتعلقة بأمن الفضاء الإلكتروني Cyber Security في إطار المخاطر التشغيلية: تجارب رقابية عربية"، (2018).

في هذا الإطار، تفرض السلطة الرقابية بالأردن على المصارف القيام باختبارات الضغط (Stress Testing) لتحديد حجم الآثار المترتبة على نجاح أية عمليات قرصنة تتعرض لها الأنظمة الإلكترونية وذلك بصفة دورية سنوية. كما يلزم البنك المركزي المصارف القيام بالإبلاغ عن تعرضها لأية عمليات قرصنة إلكترونية (Cyber-event reporting) خلال 72 ساعة من التعرض. ذلك بالنسبة لكافة حالات الخروقات الخاصة بأمن الفضاء الإلكتروني، والتي يترتب عليها خسائر ملموسة للعملاء، وتؤثر سلباً على عمليات المصرف، وأي حدث سيبراني أو أي محاولة للهجوم السيبراني تتسم بدرجة خطورة عالية على أنظمتها أو شبكاتها.

9. التعاون والتنسيق مع السلطات الرقابية الأخرى عبر الحدود والشركاء في صناعة تقنية المعلومات فيما يتعلق بالمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

تتمثل أوجه التعاون والتنسيق في هذا الإطار في إجراء الزيارات وعقد الاجتماعات وتبادل الخبرات والمعارف، حيث تقوم البنوك في الأردن بشكل مستمر بالاستعانة بخدمات صناعة تقنية المعلومات محلياً وعالمياً لتطبيق ضوابط الحماية والتشغيل اللازمة.

10. بناء القدرات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

يعمل البنك المركزي الأردني على تعزيز القدرات البشرية العاملة في مجال أمن الفضاء الإلكتروني من خلال الوسائل التالية:

- توفير أقسام خاصة بالرقابة على المعلومات والتقنيات المصاحبة لها.
- توفير التدريب اللازم للكوادر بشكل متخصص ووضع آليات تعنى بالحصول على شهادات مهنية دولية بهذا الخصوص.
- توفير الاشتراكات لمصادر المعرفة عبر الإنترنت بمواضيع إدارة مخاطر تكنولوجيا المعلومات والرقابة والتدقيق عليها.

- إنشاء وحدة متخصصة في البنك المركزي تحت مسمى "دائرة أمن المعلومات والأمن السيبراني".
- يجري العمل حاليا على إنشاء فريق متخصص للاستجابة لحوادث الأمن السيبراني (FinCert) بالتعاون مع القطاع المالي، والقطاع الحكومي والجيش للاستفادة من تجاربهم في هذا المجال.
- توفير فرص لتدريب موظفي البنك المركزي، والاطلاع على مختلف التجارب على الصعيد الوطني والعالمي في هذا الصدد.

- إضافة إلى ما سبق، يقوم البنك المركزي الأردني بالأخذ بالاعتبار المقترحات والمبادئ الرقابية الصادرة عن المؤسسات الدولية، والمتعلقة بدعم قدرات السلطات الإشرافية للتعامل مع مخاطر أمن الفضاء الإلكتروني.

11.التحديات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

تشمل أهم التحديات التي واجهت الأردن فيما يتعلق بدعم أمن الفضاء الإلكتروني في القطاع المصرفي النقاط التالية:

- حداثة مفهوم الأمن السيبراني على المستوى الوطني.
- ظهور تقنيات جديدة في مجال الخدمات الإلكترونية على مستوى المملكة، مما أدى إلى ظهور تحديات جديدة مرتبطة بهذه التقنيات.
- كلفة تطبيق تقنيات أمن نظم المعلومات والفضاء الالكتروني مرتفعة نسبياً مقارنة بالتقنيات الأخرى.
- صعوبة تطبيق ضوابط أمن نظم المعلومات والفضاء السيبراني نظراً لضعف ثقافة الأمن السيبراني لدى القطاع المالي والمصرفي في هذا المجال.
- عدم وجود آلية رقابة واضحة على البنوك والشركات المالية للتأكد من وجود ضوابط وسياسات لتحقيق الأمن السيبراني فيها.

تعامل البنك المركزي الأردني مع هذه التحديات من خلال إتباع ما يلي:

- إصدار التعاميم والتعليمات اللازمة في حينه بهذا الخصوص.
- فحص عمليات البنوك بهذا الخصوص ميدانياً من خلال آليات التفتيش الدوري.

- ترخيص تلك الخدمات وفرض الضوابط التي يراها البنك مناسبة والتي تتطلب زيادة السيطرة على المخاطر.
- إصدار تعليمات في مجال أمن نظم المعلومات والفضاء السيبراني وذلك لضمان تطبيق والتزام الجهات التي تخضع لإشراف ورقابة البنك المركزي بالضوابط والإجراءات التي تُعزز أمن نظم المعلومات والأمن السيبراني لديها، مثل "تعليمات التكيف مع المخاطر السيبرانية" التي صدرت عام 2018.
- الاطلاع على مختلف التجارب في هذا المجال على الصعيد العالمي.
- تعريف كافة الجهات ذات العلاقة بأهمية أمن الفضاء السيبراني وحثهم على الاستثمار في هذا المجال على الصعيد المادي والبشري.
- التشاور مع كافة المعنيين في القطاع المالي فيما يتعلق بإمكانية تطبيق الحلول التي تدعم مجال أمن نظم المعلومات والفضاء السيبراني.
- تدريب الموظفين على تحقيق الأمن السيبراني في القطاع المالي والمصرفي بالإضافة إلى حضورهم لمؤتمرات محلية ودولية بهذا الخصوص.

12.التجارب الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

- قام البنك المركزي الأردني في عام 2016 بإصدار تعليمات مفصلة تتكون من (62) صفحة تتعلق بحاكمية وإدارة المعلومات والتقنيات المصاحبة لها، والتي استندت إلى أفضل الممارسات الدولية المقبولة والحديثة بهذا المجال [Control Objectives for Information and Related Technologies (COBIT 5)]، ما يساعد بشكل كبير في تعزيز

ضوابط إدارة مخاطر التشغيل ومخاطر تقنية المعلومات والأمن السيبراني على وجه التحديد.

- إصدار تعليمات التكيف مع المخاطر السيبرانية، والتي تهدف بشكل رئيس إلى دعم البنوك والمؤسسات المالية على مواصلة تقديم خدماتها وعملياتها على الرغم من تهديدات الهجوم الإلكتروني التي قد تتعرض لها، ذلك من خلال تحسين ضوابطها الأمنية والاجراءات والتدابير المناسبة وتطوير الآليات الكفؤة والفعالة لديها لمكافحة الانتهاكات السيبرانية التي قد تعترضها، بالإضافة إلى تعزيز منظومتها الأمنية للتأهب والاستجابة للحوادث والمخاطر الناشئة والمحتملة التي تهدد بشكل أساسي أمن مجتمعها المعلوماتي.
- تم إعداد مسودة "تعليمات التوثق المحكم من العميل لعمليات الدفع الإلكتروني" وجاري العمل على اعتمادها، وذلك حرصا من البنك المركزي الأردني على الحفاظ المستمر على مستويات أمن وكفاءة أنظمة وأدوات الدفع الإلكتروني في المملكة وحماية عمليات الدفع والتحويل الالكتروني للأموال من مخاطر الاحتيال والتزوير من خلال الالتزام بتوفير أساليب التحقق المُحكم من العميل للحد من هذه المخاطر، وحماية كافة الأطراف المشاركة في هذه العمليات (العملاء، البنوك ومقدمي خدمات الدفع، التجار والمحصلين).

الإمارات

1. الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

تتضمن التعليمات الرقابية الخاصة بإطار المخاطر التشغيلية (Operational Risks) جزءً متعلقاً بمخاطر نظم المعلومات وأمن الفضاء الإلكتروني في القطاع المصرفي، تمثلت أبرزها فيما يلي:

- تم إصدار تعميم الي كافة البنوك والمؤسسات المالية الأخرى العاملة بالدولة بضرورة الالتزام بتطبيق كافة متطلبات (SIA) المتعلقة بأمن الفضاء الإلكتروني ونظم المعلومات.
- تم إصدار نظام بشأن المخاطر التشغيلية تلتزم به كافة البنوك العاملة بالإمارات، تضمن جزء منه موضوع تقنية المعلومات وضرورة التزام البنك بوجود سياسات لتقييم ومراقبة وإدارة مخاطر التقنية وتوفير البنية التحتية الملائمة لتقنية المعلومات، تضمن سلامة وأمن وتوفر البيانات والنظم.
- يقوم المصرف المركزي بصفة منتظمة بإصدار إشعارات إلى البنوك والمؤسسات المالية الأخرى العاملة بالدولة لتحذيرها من التهديدات الإلكترونية التي تستهدف القطاع المالي والواردة إليها من السلطات المعنية بالدولة، واتخاذ الإجراءات اللازمة التي تضمن حماية أنظمة المؤسسات المالية من مثل هذه التهديدات الإلكترونية.
- جاري حالياً إعداد تعميم جديد إلى البنوك والمؤسسات المالية الأخرى يتضمن ضرورة التزام كافة المؤسسات المالية بالدولة من تطبيق متطلبات (SIA) وسوف يعهد المصرف المركزي إلى أحد شركات

المراجعة المتخصصة بالدولة لإجراء عملية فحص لهذه المؤسسات للتأكد من الالتزام بهذه المتطلبات.

- يتم تضمين عمليات الرقابة على أساس المخاطر لاختبارات توضح مدى قدرة المصارف على مواجهة مخاطر أمن الفضاء الإلكتروني وذلك بصورة ربع سنوية. كما أن هناك توجيهات رقابية تلزم 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 المصرفية بما يشمل وجود سياسة واضحة لحوكمة إدارة مخاطر أمن الفضاء الإلكتروني.

2. الضوابط والتعليمات الخاصة بتنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الإنترنت

يسمح للعملاء بإنشاء أو فتح حساب مصرفي من خلال موقع البنك على شبكة الإنترنت، تمثلت الضوابط الخاصة بذلك في إصدار عدة تعاميم إلى البنوك والمؤسسات العاملة بالدولة لاعتماد استخدام بطاقة هوية دولة الإمارات لفتح الحسابات المصرفية، حيث تحتوي هذه البطاقة على خصائص تسمح باستخدامها بشكل آمن على الإنترنت. وعلى البنك أن يتبع هذه العملية باستكمال متطلبات أعرف عميلك، حتى يتمكن من إجراء عملية الفحص الفعلي للوثائق طبقاً لتعميم المصرف المركزي بشأن نظام إجراءات مواجهة غسل الأموال، الذي يشير إلى ضرورة قيام البنك بالتأكد من المعلومات وفحص الوثائق فعلياً وذلك لمنع فتح حسابات بأسماء مستعارة. كما أن بعض البنوك العاملة في الدولة ولأنواع محددة من الحسابات تسمح للعميل بفتح حساب لديها من خلال الإنترنت

ويتم فحص الوثائق عن طريق مندوب شركة الشحن (طرف ثالث) قبل تسليم العميل للبطاقة المصرفية الخاصة به عن طريق قارئ مخصص لقراءة بيانات بطاقات الهوية الخاصة بالعملاء والحصول على نسخة من الأوراق الثبوتية في هذا الشأن.

بالنسبة للضوابط والأساليب التي يلتزم البنك بتطبيقها للتحقق من هوية العميل الراغب في إجراء أحد التعديلات الخاصة ببيانات حساب خدمات الإنترنت البنكي الخاصة به، وإعادة تفعيل الحساب، وإعادة اصدار كلمة سر جديدة وخلافه، فتتمثل في ضرورة تواجد العميل (صاحب الحساب) شخصياً حتى يمكن للبنك إجراء عملية الفحص الفعلي للوثائق طبقاً لتعميم المصرف المركزي بشأن نظام إجراءات مواجهة غسل الأموال.

3. التعاون والتنسيق مع السلطات الرقابية الأخرى عبر الحدود والشركاء في صناعة تقنية المعلومات فيما يتعلق بالمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

يتم التعاون والتنسيق مع الجهات الرقابية الأخرى عبر الحدود، وفيما بين القطاع المصرفي وصناعة تقنية المعلومات وذلك بالنسبة لدعم أمن الفضاء الإلكتروني، من خلال التعاون في مجال التدريب والمعلومات بخصوص سبل الحماية من الإختراق.

4. بناء القدرات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

تعمل السلطة الرقابية المسؤولة عن القطاع المصرفي على تعزيز القدرات البشرية لديها في مجال أمن الفضاء الإلكتروني من خلال التدريب وتعيين خبراء أمن المعلومات.

البحرين

1. الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

تشمل التعليمات الرقابية الصادرة عن مصرف البحرين المركزي توجيهات خاصة بإدارة المخاطر الأمنية الإلكترونية ضمن الجزء الخاص بإدارة المخاطر التشغيلية، حيث يولي المصرف اهتماماً كبيراً لإدارة المخاطر الأمنية الإلكترونية لما لها من أهمية بالغة في حماية البيانات الشخصية للعملاء، وحماية أصولهم لدى البنوك وتعزيز الثقة في القطاع المصرفي بشكل عام. ونظرا لتزايد الهجمات التي تستهدف أنظمة تقنيات المعلومات للمؤسسات والشبكات، وذلك بهدف تحويل الأموال بطريقة غير مشروعة، تعطيل أو تدمير أو السيطرة بشكل ضار على نظام تقنيات المعلومات لتدمير سلامة بيانات المؤسسات أو لسرقة المعلومات منه. حيث أصدر المصرف في أكتوبر 2016 توجيهات عامة في فصل إدارة المخاطر التشغيلية تتضمن إدارة المخاطر المرتبطة مع الهجمات الإلكترونية والمخاطر ذات الصلة، والتي تغطي جميع قطاعات الأعمال ذات الصلة ولا تقتصر فقط على وظيفة تقنيات المعلومات والمسائلة الإدارية والتقييمات الدورية بهذا الشأن ورصد ضوابط أمن المعلومات واستمرارية الأعمال. كما تتضمن هذه التوجيهات وجوب تقديم

تقارير فصلية للمصرف عن الخطوات والإجراءات المتخذة في تنفيذ هذه المتطلبات في حال عدم تطبيقها من قبل المرخص له.

السعودية

1. الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

تتضمن التعليمات الرقابية الخاصة بإطار المخاطر التشغيلية (Operational Risks) جزءً متعلقاً بمخاطر نظم المعلومات وأمن الفضاء الإلكتروني في القطاع المصرفي، تتمثل أبرز تلك التعليمات الرقابية فيما يلي:

- الدليل التنظيمي لأمن المعلومات (SAMA Cyber Security Framework).
- الدليل التنظيمي لاستمرارية الأعمال (Business Continuity Management Framework).

كما تتضمن عمليات الرقابة على أساس المخاطر (ongoing risk-based supervisory activities) لاختبارات توضح مدى قدرة المصارف على مواجهة مخاطر أمن الفضاء الإلكتروني (تجارب محاكاة لهجمات افتراضية). وقد أصدرت السلطات الرقابية في مايو 2017 تعليمات وقواعد تنظم تقديم الخدمات المصرفية، بحيث شملت كل من الخدمات المصرفية عبر الإنترنت والجوال، واستخدام تقنية البيئة المعزولة، ونظم المدفوعات، والصرافات الآلية (ATMs).

إضافة الى ذلك تتمثل التعليمات الرقابية التي يتم فرضها على عمليات تعهيد أمن نظم المعلومات والأنظمة الإلكترونية للمصرف إلى جهة ثالثة (Third Party) فيما يلي:

- يجب وضع متطلبات الامن الالكتروني ضمن سياسة وعملية الاسناد الى أطراف ثالثة، واعتمادها، وتطبيقها، وتعميمها في المنشأة العضو.
- يجب قياس ضوابط الأمن الالكتروني لسياسة وعملية الاسناد إلى أطراف ثالثة وتقييمها دوريا.
- يجب أن تتضمن عملية الاسناد الى أطراف ثالثة ما يلي:
  - الحصول على موافقة المؤسسة قبل إسناد أي اعمال أساسية.
  - اشراك إدارة أمن المعلومات.
  - متطلبات الامن السيبراني الأساسية التي يجب تطبيقها في جميع الحالات.
  - الحق في اجراء مراجعة وتدقيق متطلبات الامن السيبراني دوريا.
  - الالتزام بتعليمات المؤسسة بحسب ما ورد بالدليل التنظيمي لأمن المعلومات، والالتزام بتعاميم ضوابط الاسناد لطرف ثالث.

كما أصدرت السلطات توجيهات رقابية تلزم المصارف بتضمين استراتيجيات المخاطر المُقرة من قبل مجالس إدارات البنوك إطارا يتعلق بالمخاطر الإلكترونية ومخاطر نظم المعلومات والهجمات الإلكترونية (Cyber-attacks)، ويتم التحقق من وجود تلك الاستراتيجيات من خلال عمليات الرقابة المصرفية بحيث تكون مُقرة من قبل مجالس إدارات البنوك تتضمن مستوى

المخاطر المتعلقة بأمن الفضاء الإلكتروني وإجراءات موازية لدعم مستويات أمن الفضاء الإلكتروني بما يشمل وجود سياسة واضحة للحوكمة في هذا الشأن. وتلزم ايضاً تلك التعليمات الرقابية المصارف بتعيين مسؤول عن أمن المعلومات Chief Information Security Officer (CISO).

2. الضوابط والتعليمات الخاصة بتنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الإنترنت

تسمح التعليمات والضوابط الصادرة في هذا الشأن للعملاء بإنشاء أو فتح حساب مصرفي من خلال موقع البنك على شبكة الانترنت، ذلك لأنه بحسب إحدى مبادرات تطوير القطاع المالي (Sandbox)، وهي بيئة تجريبية مختصة في القطاع المالي ليتم عن طريقها اختبار المنتجات الجديدة، وعن طريقها يستطيع العملاء فتح حساب مصرفي من خلال موقع البنك على شبكة الانترنت باستخدام جهة موثوقة للتحقق من هوية العملاء. والتأكيد على الجهات المالية بالالتزام بالضوابط والتعاميم الصادرة بهذا الشأن. وتتمثل تلك الضوابط والتعليمات (الشروط والاحكام) التي يطبقها البنك على العميل الراغب في الاستفادة من الخدمات المصرفية من خلال شبكة الانترنت، فيما يلي:

- يجب وضع معايير الأمن الإلكتروني للخدمات المصرفية الإلكترونية واعتمادها وتطبيقها.
- يجب متابعة الالتزام بمعايير الأمن الإلكتروني للخدمات المصرفية الإلكترونية.
- يجب قياس فعالية معيار الأمن الإلكتروني للخدمات المصرفية الإلكترونية وتقييمها دوريًّا.

- تطبيق ما ورد بالدليل التنظيمي لأمن المعلومات المتعلقة بضوابط الخدمات الالكترونية المصرفية.

أما بالنسبة للضوابط والأساليب التي يعتمد عليها البنك في التحقق من هوية وصلاحية العميل الراغب في الاستفادة من الخدمات المصرفية (أو الراغب في تنفيذ أنشطة مصرفية) من خلال شبكة الانترنت، بحيث يتم استخدام آليات المصادقة متعددة العوامل المتمثلة فيما يلي:

أ- يجب استخدام المصادقة متعددة العوامل أثناء عملية تسجيل العملاء لاستخدام الخدمات المصرفية الإلكترونية.

ب- يجب تطبيق المصادقة متعددة العوامل في جميع الخدمات المصرفية الإلكترونية المتاحة للعملاء.

ج- يجب أن يكون جهاز التوكن أو التوكن الرقمي محمياً بكلمة مرور.

د- إيقاف دخول العملاء بعد إدخال كلمة المرور أو رقم التعريف الشخصي بشكل خاطئ لثلاث مرات متتالية.

ه- يتم تغيير أرقام الجوال الخاصة بالعملاء عبر الفروع أو أجهزة الصرف الآلي فقط.

و- يتم تنفيذ إجراءات طلب وتفعيل المصادقة متعددة العوامل عن طريق قنوات تنفيذ مختلفة.

ز- يجب تطبيق المصادقة متعددة العوامل في العمليات التالية:

1 . تسجيل الدخول.

2 . إضافة أو تعديل المستفيدين.

3 . إضافة خدمات سداد رسوم الخدمات الحكومية أو الخدمات العامة.

4 . العمليات مرتفعة المخاطر (عندما تتجاوز حدودا معينة)

5 . إعادة تعيين كلمة المرور.

ح - الالتزام بالضوابط الصادرة بهذا الشأن مثل الدليل التنظيمي لأمن المعلومات.

فيما يتعلق بالضوابط والأساليب التي يعتمد عليها البنك في التحقق من هوية وصلاحية المخولين بالاستفادة من الخدمات

المصرفية من خلال شبكة الانترنت، فانه تتم الاستفادة من الخدمات المصرفية عبر شبكة الانترنت لصاحب الحساب فقط ولا يمكن ان يتم الاستفادة لشخصين في نفس الحساب. عليه، تنص اللوائح والأنظمة في مؤسسة النقد على ان لا يتم مشاركة اسم المستخدم والرقم السري مع أي شخص آخر، وإلزام المؤسسات المالية بإجراء التوعية الدورية بهذا الخصوص. أما بالنسبة للشخصيات الاعتبارية يتم التحقق من عمليات الدخول للحسابات الخاصة بهم كل حالة على حدة، وبحسب الإجراءات الداخلية المتبعة بكل بنك. مع التأكيد على تطبيق ما ورد بالدليل التنظيمي لأمن المعلومات. كما أنه للتحقق من هوية العميل الراغب في اجراء أي تعديل على البيانات الخاصة به والمتعلقة بالإنترنت البنكي او إعادة تفعيل الحساب، او إعادة اصدار كلمة سر جديدة، فإنه يتم تطبيق التعليمات التالية:

- لتعديل بيانات العملاء وإعادة تفعيل الحسابات المصرفية يتم ذلك عن طريق الفروع.
- لإعادة اصدار كلمة سر جديدة يتم ذلك من خلال التسجيل من جديد للخدمات الإلكترونية وتطبيق ما سبق ذكره من ضوابط متبعة بحسب ما ورد من تعاميم صادرة بهذا الشأن وبما ورد بالدليل التنظيمي لأمن المعلومات.

- يتم تغيير ارقام الاتصال الخاصة بالعملاء والعناوين عبر الفروع او أجهزة الصرف الآلي فقط.
- تغيير البريد الالكتروني يتم بعد الدخول الى صفح العميل المصرفية والالتزام بما ورد بالدليل التنظيمي لأمن المعلومات.

3. الضوابط والتعليمات الخاصة بتنظيم وسائل إثبات الهوية عبر الإنترنت

تستخدم المصادقة متعددة العوامل أثناء عملية تسجيل العملاء لاستخدام الخدمات المصرفية الإلكترونية وإتباع التعليمات الواردة بالدليل التنظيمي لأمن المعلومات، وذلك بهدف التحقق من هوية العميل المستفيد من الخدمات المصرفية من خلال الانترنت. كما تقوم البنوك بتقييم الوسائل التي تعتمد عليها في التحقق من هوية العميل، بحيث تكون مناسبة من الناحية الأمنية وغير عُرضه للقرصنة أو للتهديد عن طريق البرامج الخبيثة وبرامج التجسس، من خلال قياس فعالية ضوابط الأمن الإلكتروني في عملية إدارة الأحداث الأمنية وتقييمها دوريًّا مع التأكيد بما ورد بالدليل التنظيمي لأمن المعلومات فيما يتعلق بتقييم الوسائل دورياً. أما فيما يخص الدخول على حسابات العملاء من خلال الانترنت، فيتم من خلال تطبيق أكثر من معيار من معايير التحقق من الهوية بالإضافة إلى رسائل اشعار ترسل لهواتف العملاء في حال تمت عمليات مالية على حساب العملاء.

إضافة الى ذلك، تلتزم البنوك بتطبيق ما ورد بالدليل التنظيمي لأمن المعلومات والذي يتعلق بعدد مرات الدخول الفاشلة. حيث إنه في حال محاولة العميل لثلاث محاولات دخول فاشلة يتم إيقاف الحساب بشكل مؤقت، ويتعين على المصرف

انشاء آلية توثيق الدخول مرة أخرى وإشعاره من خلال رقم الجوال المسجل مسبقا بالمصرف.

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

يتضمن الدليل التنظيمي لأمن المعلومات الصادر من مؤسسة النقد العربي السعودي ضوابط لسياسيات لإدارة كلمات المرور على ان تكون متوافقة مع أفضل الممارسات والمعايير الدولية وإجراء التقييمات الدورية لاختبار مدى التوافقية. أما بالنسبة لكلمات السر التي تستخدم لمرة واحدة (OTP) فإنه يتم إنشاؤها بشكل عشوائي ومتغير عند كل طلب.

5. الضوابط والتعليمات الرقابية الخاصة بعمليات تحويل الأموال من خلال خدمات الإنترنت

تنص الضوابط الصادرة من مؤسسة النقد على عدد من معايير التحقق مثل:

- آلية تحويل الأموال تستوجب استخدام كلمة سر لمرة واحدة (OTP) .
- اشعار عن طريق الرسائل لجوال العميل المسجل والموثق مسبقا (SMS Notification).
- تطبيق ما ورد بالدليل التنظيمي لأمن المعلومات.

6. الضوابط والتعليمات الرقابية الخاصة بسرية وسلامة المعلومات

أصدرت المؤسسة دليل تنظيمي شامل لأمن الفضاء الإلكتروني والمبني على ضوابط للتقنيات المستخدمة في المصرف مثل حوكمة أمن المعلومات بالمصرف، إدارة وأمن التطبيقات، أمن البنية التحتية، فحص الثغرات، اختبارات الاختراق، مراجعة الإعدادات التقنية، إدارة الحوادث، استمرارية

الأعمال، والتخلص الأمثل للبيانات. وتعمل تلك الإجراءات على زيادة حماية وخصوصية وسرية تلك البيانات.

7. الضوابط والتعليمات الرقابية الخاصة بتأمين التطبيقات الإلكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الانترنت

أصدرت المؤسسة دليل تنظيمي شامل لأمن الفضاء الإلكتروني (Cybersecurity) والمبني على ضوابط للتقنيات المستخدمة في المصرف مثل حوكمة أمن المعلومات بالمصرف، إدارة التطبيقات، فحص الثغرات، اختبارات الاختراق، مراجعة الإعدادات التقنية، إدارة الحوادث، استمرارية الأعمال.

8. التعاون والتنسيق مع السلطات الرقابية الأخرى عبر الحدود والشركاء في صناعة تقنية المعلومات فيما يتعلق بالمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

في هذا الخصوص، يتم التعاون والتنسيق مع الجهات الرقابية الأخرى عبر الحدود، فيما يلي عرض لأبرز ملامح هذا التعاون:

- يشمل التعاون بين السلطات الرقابية الأخرى بمشاركة المعلومات والتطورات، والتعاون على تطوير منهجية العمل وتأسيس الأنظمة الدولية والمحلية.
- المشاركة كعضو في لجنة بازل الدولية لمخاطر الأمن السيبراني وكذلك المشاركة الدولية في المؤتمرات ذات العلاقة.
- كما قامت المؤسسة بإنشاء عدد من الندوات وورش العمل، مع السادة مسؤولي السلطات الرقابية الأخرى، لإثراء المعرفة.

كما أن هناك تنسيق وتعاون بين القطاع المصرفي وصناعة تقنية المعلومات فيما يتعلق بأمن الفضاء الالكتروني، حيث تتمثل أهم ملامحه في التالي:

- مشاركة المعرفة فيما يتعلق بأحدث التقنيات والوسائل الأمنية (Share Knowledge) من خلال عقد اجتماعات دورية لمسؤولي أمن المعلومات في المصارف.
- يتم مشاركة التحذيرات والتنبيهات من خلال قناة مؤسسة النقد (Sama Alert) لمسؤولي إدارة تقنية المعلومات وأمن المعلومات في القطاع المالي.
- قام مسؤولي إدارات أمن المعلومات وتقنية المعلومات بالقطاع المصرفي بالتعاون مع مسؤولي مؤسسة النقد، بإنشاء لجنة دورية تهدف الى مناقشة التطورات فيما يتعلق بأمن الفضاء الإلكتروني وأمن المعلومات. إضافة إلى أنه يتم دعوة صناع تقنية المعلومات بالمنطقة للمشاركة (بحالات فردية).
- أنشاء لجنة أمن المعلومات للقطاع البنكي، لقطاع التأمين، ولقطاع التمويل لمناقشة اخر المستجدات بخصوص امن المعلومات.

9. بناء القدرات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

- تقوم السلطة الرقابية (مؤسسة النقد العربي السعودي) بإعداد دورات وبرامج لتطوير القدرات البشرية بشكل مستمر لتطوير رأس المال البشري لاكتساب المعرفة في مجال أمن الفضاء الإلكتروني.

- يتم عقد ورش عمل دورية لتطوير رأس المال البشري (Workshop).

- قامت مؤسسة النقد بإعداد استراتيجية الأمن السيبراني للقطاع المالي، حيث تشمل تلك الاستراتيجية عدد من المبادرات ومن ضمنها تعزيز

القدرات البشرية، إقامة ورش العمل، وغيرها مما يعزز مشاركة المعرفة والخبرات بين القطاع.

10.التحديات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

تتمثل اهم التحديات التي تواجه المملكة فيما يتعلق بدعم امن الفضاء الالكتروني في القطاع المصرفي، فيما يلي:

- في عصر ثورة الخدمات الرقمية وتعزيز التقنية، تجلب التقنية العديد من المخاطر المصاحبة، وحماية الفضاء الإلكتروني على سبيل المثال يشمل الحفاظ على سرية المعلومات، بيانات العاملين في المؤسسة المالية، البيانات وضمان عدم الإخلال في مصادقة تلك البيانات.
- تتبنى المملكة العربية السعودية من خلال رؤية 2030 وبرنامج تطوير القطاع المالي 2020 تعزيز التقنية في المجالات المالية، مما يعني ذلك، تقديم الخدمات المالية من خلال التقنية، على سبيل المثال (Fin Tech)، والذي بالطبع سيصاحبه العديد من مخاطر أمن الفضاء الإلكتروني.
- امن الفضاء الإلكتروني، هو جزء متجدد بشكل سريع، ويتطلب المتابعة على مدار الساعة واستخدام الأدوات التقنية المتطورة، وتوفير الموارد بشتى أنواعها مثل استقطاب الخبراء في المجال.

وقد تعاملت السلطة الرقابية مع هذه التحديات من خلال إنشاء عدد من اللجان في المؤسسة، لمتابعة تلك التحديات عن قرب وبشكل تفصيلي واعداد خطط العمل المناسبة.

11.التجارب الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

قامت المؤسسة بإعداد خطة عمل شاملة لرفع مستوى النضج الأمني الإلكتروني في القطاع المالي عبر عدد من النقاط الآتية: -

- قامت المؤسسة بإعداد برامج فحص دورية للقطاع المالي لتحديد مواطن الضعف المشتركة وتسجيلها بسجلات المخاطر.
- قامت المؤسسة ممثله باللجنة المشكلة لأمن معلومات القطاع المصرفي بدراسة تلك المواضيع وتحديد خطة العمل المناسبة.
- عملت المؤسسة على إنشاء استراتيجية خاصة لأمن المعلومات والتي اشتملت على إصدار الدليل التنظيمي لأمن المعلومات والدليل التنظيمي لاستمرارية الاعمال لضمان الفضاء الالكتروني في القطاع المصرفي.

السودان

1. الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

تتضمن أبرز التعليمات الرقابية الصادرة عن بنك السودان المركزي الخاصة بمخاطر نظم المعلومات وأمن الفضاء الإلكتروني في القطاع المصرفي وذلك في إطار المخاطر التشغيلية (Operational Risks) الجوانب التالية:

- تأمين وحماية مواقع الإنترنت المصرفية باستخدام نظم تأمين موثوقة.
- الاهتداء بجميع ما جاء في متطلبات (PCI – DSS) النسخة رقم 300.

- تأمين وتحديد صلاحيات الدخول على جميع طرفيات الخدمة.
- الضبط الفني الخاص بمؤقت قطع الاتصال وتسجيل الخروج لمستخدم الخدمة بعد مرور 20 ثانية لم يتم فيها التفاعل مع صفحة الخدمة.
- يجب أن تكون استضافة الخدمة داخل السودان.

كما تتضمن عمليات الرقابة على أساس المخاطر (ongoing risk-based supervisory activities)، التي تقوم به السلطة الرقابية ببنك السودان المركزي، اختبارات توضح مدى قدرة المصارف على مواجهة مخاطر أمن الفضاء الإلكتروني (تجارب ومحاكاة لهجمات افتراضية).

فيما يخص القواعد المُنظمة لتقديم الخدمات المصرفية من خلال الإنترنت، أصدرت السلطات الرقابية تعليمات خلال عام 2014 شملت جميع الخدمات الإلكترونية المقدمة من قبل المصارف والتي يكون فيها الإنترنت وسيلة الاتصال بين المصرف والعميل.

تشير التعليمات الرقابية إلى أنه يجوز لبنك السودان المركزي رفض الإسناد الخارجي للعمليات التشغيلية الجوهرية إذا ما رأى أنها قد تؤثر على جودة آليات الرقابة الداخلية لمقدمي خدمات الدفع، أو مشغل نظم الدفع، أو التأثير على قدرة البنك المركزي في الرقابة على نظم الدفع لضمان الامتثال بالالتزامات المنصوص عليها بموجب هذه اللائحة، أو المعايير والسياسات المتعلقة بالرقابة والإشراف على نظم الدفع. كما أنه في حالة قيام مشغل نظام دفع أو مقدم خدمات نظم الدفع بإسناد وظائف تشغيلية جوهرية، فعلى البنك التأكد من امتثاله للشروط الآتية:

(أ) ألا يكون الإسناد تفويضاً للقيام بمسؤوليات الإدارة العليا.

(ب) ألا يؤثر الإسناد على علاقة والتزام مشغل نظام دفع أو مقدم خدمات دفع، مع مستخدمي النظام وعملائه.

(ج) ألا يؤثر الإسناد على قدرة مشغل النظام أو مقدم الخدمة في الامتثال لشروط منح الترخيص أو لأحكام هذه اللائحة.

(د) ألا يتم تعديل أو حذف لأي من شروط منح الترخيص.

2. الضوابط والتعليمات الخاصة بتنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الإنترنت

تشير نتائج الاستبيان إلى أنه، في ضوء الضوابط والتعليمات الصادرة عن الجهة الرقابية، لا يسمح للعملاء بإنشاء أو فتح حساب مصرفي من خلال موقع البنك على شبكة الإنترنت وذلك نظراً لوجود معاملات متعلقة بسياسة أعرف عميلك [Know Your Customer (KYC)]. إضافة إلى عدم توفر الربط الشبكي، ودعم البيانات بين المصارف، ومصادر الهوية الشخصية للعميل (السجل المدني، وزارة الداخلية ...إلخ).

تتمثل الضوابط والتعليمات (الشروط والاحكام) التي يطبقها البنك على العميل الراغب في الاستفادة من الخدمات المصرفية من خلال شبكة الإنترنت، فيما يلي:

- بعض المصارف تقدم الخدمات عبر تطبيقات الموبايل مما يتطلب خطوات إجرائية معينة كتنزيل التطبيق والتسجيل وإنشاء حساب وكلمة المرور.

- إنشاء رقم المرور الخاص بالصيرفة الإلكترونية عبر الإنترنت (IPIN).
- بعض الخدمات الإلكترونية تتطلب فتح حساب جاري بالبنك المعني وربطه بالخدمات الإلكترونية.

كما يلتزم البنك بالضوابط والأساليب التالية للتحقق من هوية وصلاحية العميل الراغب في الاستفادة من الخدمات المصرفية (أو الراغب في تنفيذ أنشطة مصرفية) من خلال شبكة الإنترنت:

- ضرورة إنشاء حساب إلكتروني على مستوى الوسائل الطرفية المقدمة للخدمة (موبايل، ويب، ... إلخ).
- إنشاء كلمة المرور الخاصة بالصيرفة عبر الإنترنت (IPIN).
- طلب الخدمة وفق رقم حساب البطاقة المصرفية (PAN).
- التحقق من تاريخ صلاحية البطاقة.

وفي حالة وجود أكثر من شخص يمكنهم التعامل على نفس الحساب، يتطلب ما يلي:

- إصدار بطاقة منفصلة لكل شخص معرفة بـ (PAN) منفصل.
- إنشاء كلمة مرور منفصلة لكل شخص يتم ربطها بالحساب.
- تحديد سقف معين للسحوبات لكل شخص.
- ربط جميع الحركات وتلخيصها في تقرير وكشف حساب موحد يصدر عن الحساب.

أما بالنسبة للحسابات الخاصة بالأشخاص الاعتبارية، يجب التالي:

- تحديد شخص مكلف بإدارة الحساب والتعاملات الإلكترونية.

- ربط الحساب برقم موبايل محدد لإرسال كلمات المرور والتحقق منها.
- إنشاء كلمة مرور محددة للمصرح لهم بالولوج للخدمات المصرفية الإلكترونية.
- إرسال كلمة مرور تعريفية لمرة واحدة (OTP) عند كل مرة يتم فيها الدخول لمنصة الخدمات الإلكترونية.

عند إجراء العميل أي تعديل على البيانات أو الحسابات الخاصة به، يتم التحقق من هوية العميل من خلال واحدة أو أكثر من الوسائل التالية:

- رقم الهاتف المرتبط بالحساب المصرفي والمسجل عند إنشاء الحساب.
- كلمة المرور.
- استيفاء وملء بعض الاستمارات الخاصة بالتعديلات.
- بعض المعاملات تحتاج إلى إثبات هوية العميل وحضوره شخصياً إلى المصرف.

3. الضوابط والتعليمات الخاصة بتنظيم وسائل إثبات الهوية عبر الإنترنت

تتمثل الوسائل التي تعتمد عليها البنوك في التحقق من هوية العميل المستفيد من الخدمات المصرفية من خلال الإنترنت من خلال الوسيلتين التاليتين:

- ينشأ من قبل العميل، كإنشاء إسم المستخدم وكلمة المرور.
- ينشأ من قبل المشغل، مثل كلمة المرور الخاصة بالإنترنت المصرفي (IPIN).

أما بالنسبة للآلية التي تعتمد عليها البنوك في التحقق من تصديق العميل إلكترونياً من خلال الإنترنت، فتتم من خلال الوسائل التالية:

- الرسائل القصيرة (SMS).
- البريد الإلكتروني.
- الإشعار الورقي الذي ينتج عن بعض الماكينات التي تقدم الخدمات المصرفية الإلكترونية.

في هذا السياق، يتم الحد من محاولات الدخول غير المصرح به من خلال تصميم خوارزمية معينة داخل النظام بهدف ضبط عدد المحاولات الفاشلة في الدخول (بعدد ثلاث محاولات)، من خلال تهيئة النظام الخاص بذلك في محول القيود القومي والمصارف ذات المحولات الخاصة.

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

تطبق التعليمات والتدابير الرقابية التالية وذلك فيما يتعلق بإدارة كلمة السر (Password) ومواصفاتها:

- ربط كلمة المرور لمرة واحدة (OTP) برقم الهاتف الخاص بالعميل مباشرة والمعرف عند فتح الحساب.
- إلزام العميل بتغيير كلمة المرور المصدرة مع البطاقة المصرفية مع أول استخدام للبطاقة.
- تحديد عدد معين للمعاملات الفاشلة.

وبخصوص كلمة السر التي تستخدم لمرة واحدة والصادرة باستخدام أجهزة رموز الأمان (OTP)، تطبق التعليمات والمواصفات التالية:

- يتم إنشاءها إلكترونياً وبصورة عشوائية.
- تصدر بفترة صلاحية محدودة أقصاها 10 دقائق.
- ترسل فقط على رقم الهاتف الجوال المرتبط بإنشاء الحساب.

- يتم إرسالها في صيغة مشفرة.

5. الضوابط والتعليمات الرقابية الخاصة بعمليات تحويل الأموال من خلال خدمات الإنترنت

فيما يتعلق بالضوابط والتعليمات الخاصة بتحويل الأموال من حسابات العملاء إلى حسابات أطراف أخرى من خلال خدمات الإنترنت البنكي بهدف الحد من المخاطر المصاحبة لعملية التحويل، تطبق التعليمات التالية:

- تحديد سقف معين للتحويلات.
- إدخال الرقم السري للإنترنت المصرفي.
- إرسال (OTP) في كل معاملة خاصة بالتحويل من حساب لحساب آخر.
- إرسال إشعار الخصم والإضافة في صورة رسائل قصيرة (SMS) بعد نهاية كل معاملة.

6. الضوابط والتعليمات الرقابية الخاصة بسرية وسلامة المعلومات

بالنسبة لسرية وسلامة المعلومات الخاصة بالإنترنت البنكي، تطبق الضوابط والتعليمات التالية:

- حسب تصنيف بيانات البطاقات، يتم التعامل معها بالكيفية الواردة في المعايير وفق حساسية المعلومة.
- هنالك موجهات مكتوبة للتعامل مع كل نوع حسب درجة حساسيته.
- استخدام الأدوات التقنية لإنفاذ السياسات والموجهات أعلاه.

7. الضوابط والتعليمات الرقابية الخاصة بتأمين التطبيقات الإلكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الانترنت

لتأمين التطبيقات الإلكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الإنترنت ولضمان الحماية الفعالة لهذه التطبيقات، تطبق الضوابط والتعليمات التالية:

- الالتزام بموجهات اللوائح المنصوص عليها وفق (PCI –PA).
- الفصل الكامل للبيئة الواقعية عن البيئات الاختبارية.
- إجراء اختبارات الموائمة قبل الربط على البيئة الواقعية.
- المحافظة على المراجعة الدورية في البيئة الواقعية.

8. بناء القدرات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

يتم تأهيل وتعزيز المعرفة وصقل المهارات التدريبية بالنسبة للموظفين الذين ترتبط مهامهم بالمشاريع القومية المتعلقة بالصيرفة الإلكترونية أثناء فترة تكوين المشروع والبدء بالعمل به. كما يتم الأخذ بالاعتبار المقترحات والمبادئ الرقابية الصادرة عن المؤسسات الدولية، والمتعلقة بدعم قدرات السلطات الإشرافية للتعامل مع مخاطر أمن الفضاء الإلكتروني.

9. التحديات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

تتمثل أهم تلك التحديات في الحصول على الأنظمة والبرمجيات الخاصة بأمن الفضاء الإلكتروني في ظل الحظر الاقتصادي المفروض على السودان. بالإضافة إلى التكلفة العالية التي ترتبط بها تلك الأنواع من الأنظمة. كما تواجه

بعض العقبات المعرفية المتعلقة بتطوير المورد البشري الخاص بأمن المعلومات في ظل التطور التقني المتسارع.

يتم التعامل مع هذه التحديات من خلال محاولة توفير احتياجات القطاع المصرفي والبنية التحتية المتعلقة بالأنظمة ووسائل الحماية اللازمة لها من خلال الأسواق الوسيطة بأسعار مرتفعة جداً. إضافة الى بذل الجهود في محاولة تدريب وتأهيل أكبر عدد من المختصين في المجال.

عُمان

1. الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

تتضمن التعليمات الرقابية الخاصة بإطار المخاطر التشغيلية (Operational Risks) جزءً متعلقاً بمخاطر نظم المعلومات وأمن الفضاء الإلكتروني في القطاع المصرفي يحدد المعايير اللازم توافرها لضمان أمن الفضاء الإلكتروني، من أبرز تلك التعليمات الرقابية الصادرة عن البنك المركزي العُماني في هذا الصدد، ما يلي:

- يجب على البنوك إجراء اختبار الاختراق من خلال الاستعانة بخبراء خارجيين سنوياً.
- يجب على البنوك إجراء تقييم الثغرات على أساس ربع سنوي بواسطة فريق الأمن الداخلي.
- تُلزم البنوك باتخاذ خطوات لتعزيز الوعي الأمني حول عمليات الاحتيال عبر الإنترنت للعملاء والموظفين والموردين من خلال

التوعية ورسائل البريد الإلكتروني والرسائل القصيرة وعلى أجهزة الصراف الآلي والموقع الإلكتروني.

- يجب على البنوك إخطار العملاء باستخدام الرسائل القصيرة والبريد الإلكتروني بجميع المعاملات المالية وغير المالية.
- يجب على البنوك المحلية أن تنشئ إدارة لأمن المعلومات لديها موارد بشرية من ذوي الخبرة والكفاءة المناسبة.
- يجب أن يكون لدى فروع البنوك الأجنبية إطاراً تنظيمياً ملائماً لقطاع أمن المعلومات بما يتفق مع حجم العمليات في السلطنة.
- يجب على البنوك تحديد الحد الأدنى من المعايير الأساسية للأمن لجميع القنوات والأنظمة والمعدات والشبكات التي يجب أن يتم فحصها من قبل فريق الأمن للامتثال للمعايير الأمنية.
- تحتاج البنوك إلى توثيق سجلات جميع قنوات التسليم والنظم وقاعدة البيانات ومعدات الشبكات ويجب أن تخضع هذه السجلات لمراقبة مستمرة من قبل فريق أمن المعلومات من خلال نظام مراقبة آلي مستقل.
- يجب أن يكون لدى البنوك تأمين إلكتروني.
- يجب على البنوك إجراء اختبارات سيبرانيه وهمية في ظروف واقعية تتضمن سيناريوهات، مثل رسائل البريد الإلكتروني التصيدية واستخدام مثل هذه الاختبارات لقياس الوعي الأمني للموظفين.
- يجب على البنوك وضع بنية أمنية قوية مع استراتيجية دفاعية عميقة لتعزيز إطارها الأمني.

- يجب على البنوك وضع إجراءات / خطط موثقة للتعامل مع حوادث الأمن السيبراني والتي تعطي تفاصيل تامه عن هذه الحوادث مع تضمين دور تخفيف هذه الحوادث وتحديد المسؤوليات المناطة.
- يجب على البنوك أن تضع إطارًا قويًا للأمن السيبراني والذي يتضمن -بالإضافة إلى سياسة أمن المعلومات- سياسة أمنية إلكترونية منفصلة متحوطة لإحباط الهجمات السيبرانية. يجب على البنوك أيضاً أن تضع إطاراً متكاملاً للإبلاغ عن الحوادث وإدارتها واستردادها في حال حدوثها.
- يجب على البنوك اتخاذ الخطوات الكافية لمواكبة التطورات العالمية فيما يتعلق بالاحتيال السيبراني وتقييم الضوابط الداخلية لتفادي حدوثها في سلطنة عمان.

يتم تضمين عمليات الرقابة على أساس المخاطر لاختبارات سنوية توضح مدى قدرة المصارف على مواجهة مخاطر أمن الفضاء الإلكتروني. كما أصدر البنك المركزي خلال الفترة (2015-2017) تعليمات وقواعد تنظم تقديم الخدمات المصرفية من خلال الإنترنت. شملت تلك القواعد جميع القنوات المصرفية الإلكترونية بما في ذلك الخدمات المصرفية عبر الإنترنت والخدمات المصرفية عبر الهاتف / الهاتف المحمول والبطاقات وأنظمة نقاط البيع.

بالنسبة للتعليمات الرقابية التي يتم فرضها على عمليات تعهيد أمن نظم المعلومات والأنظمة الإلكترونية للمصرف إلى جهة ثالثة (Third Party)، فإنها تلزم المصارف 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 المصرفي الإلكتروني للبنك. كما أن هناك توجيهات رقابية تُلزم المصارف بتضمين استراتيجيات المخاطر المُقرة من قبل مجالس إدارات البنوك إطاراً يتعلق بالمخاطر الإلكترونية ومخاطر نظم المعلومات والهجمات الإلكترونية (Cyber-attacks)، والتحقق من وجودها بما يشمل وجود سياسة واضحة لحوكمة إدارة مخاطر أمن الفضاء الإلكتروني (إجراءات لتحديد المخاطر، والحماية، واكتشاف التهديدات والتعامل معها، وخطط للمعالجة (Recovery plans) وكذا تعيين مسؤول عن أمن المعلومات [Chief Information Security Officer (CISO)].

2. الضوابط والتعليمات الخاصة بتنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الإنترنت

لا يسمح للعملاء بإنشاء أو فتح حساب مصرفي من خلال موقع البنك على شبكة الإنترنت، لتفادي الصدام في المعلومات المعبأة من قبل العملاء، ولتفادي عدم الالتزام بسياسه البنك المركزي أو البنك نفسه من حيث المعلومات والمستندات الواجب تسليمها عند فتح الحساب مما قد يؤدي لانزعاج العميل من التأخير الذي قد يحصل وتأثر رضا العملاء من هذه الناحية. وتتمثل الضوابط والتعليمات (الشروط والأحكام) التي يطبقها البنك على العميل الراغب في الاستفادة من الخدمات المصرفية من خلال شبكة الإنترنت في النقاط التالية:

- يجب حفظ الأرقام السرية بطريقه آمنه في كل الأوقات.

- يجب على العميل تسجيل الخروج من خدمة إجراء المعاملات بالإنترنت عندما لا يكون متواجداً أمام جهازه.
- إذا علم العميل بأن أرقامه السرية قد اكتشفت بواسطة طرف آخر عليه أن يبلغ البنك فوراً.

يتحقق البنك من هوية وصلاحية العميل الراغب في الاستفادة من الخدمات المصرفية (أو الراغب في تنفيذ أنشطة مصرفية) من خلال شبكة الإنترنت، من خلال الضوابط الخاصة بكل من كلمة المرور، رقم تعريف شخصي لمره واحدة، رقم البطاقة الشخصية، رقم البطاقة المصرفية وكلمة المرور الخاصة بالبطاقة نفسها، والإسم التعريفي. في حالات الحسابات المشتركة أو حسابات الأعمال التجارية والأشخاص الاعتبارية فإنه يتم تزويد كل مستخدم برقم سري وكلمه سر منفردة ومستقله عن الآخر، وقد يضع البنك حدوداً لكل عميل فيما يتعلق بالمعاملات المالية. كما أنه في حالة إجراء العميل أي تعديلات على بيانات حساب خدمات الإنترنت البنكي أو أي بيانات أخرى، فإن البنك يتحقق من هوية العميل من خلال إرسال كلمة المرور (OTP) لمرة واحدة إلى هاتف المحمول للعميل في حاله إصدار كلمه سر أو يتم التواصل مع مركز خدمة العملاء لتغيير أي بيانات خاصه بالعميل.

3. الضوابط والتعليمات الخاصة بتنظيم وسائل إثبات الهوية عبر الإنترنت

تعتمد البنوك على عدد من الإجراءات المناسبة للاحتراز والسلامة لإثبات الهوية للعملاء المستفيدين من الخدمات المصرفية من خلال الإنترنت، مثل رقم بطاقة الخصم والرقم السري، ورقم التعريف الشخصي لمرة واحده، ورقم بطاقة الهوية الوطنية. وتقوم البنوك بتقييم هذه الوسائل، بحيث تكون مناسبة من الناحية الأمنية وغير عُرضه للقرصنة من خلال إجراء اختبار الاختراق

من خلال الاستعانة بالخبرات الخارجية ذلك بصورة سنوية. إضافة الى ذلك فانه يجب على البنوك إجراء تقييم الثغرات على أساس ربع سنوي بواسطة فريق الأمن الداخلي، واتخاذ خطوات لتعزيز الوعي الأمني حول عمليات الاحتيال عبر الإنترنت للعملاء والموظفين والموردين من خلال التوعية ورسائل البريد الإلكتروني والرسائل القصيرة وعلى أجهزة الصراف الآلي والموقع الإلكتروني. كما تقوم البنوك بالتحقق من تصديق العميل إلكترونياً من خلال الإنترنت عن طريق إخطار العميل من خلال البريد الإلكتروني وإرسال رسالة نصيه إلى هاتفه المحمول. تتحكم البنوك في عدد مرات المحاولات الفاشلة للدخول إلى الحساب من خلال الإنترنت بهدف الحد من القرصنة الإلكترونية، حيث يتم تعليق التعامل الإلكتروني للحساب بعد ثلاث محاولات فاشلة للدخول إلى الحساب. كما يتم إخطار العميل بعدد المحاولات الفاشلة عن طريق البريد الإلكتروني وإرسال رسالة نصيه للهاتف المحمول.

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

تتمثل التعليمات والتدابير الرقابية الخاصة بإدارة كلمة السر في وجوب قيام البنوك بفرض ضوابط قوية على كلمة المرور، حيث تمثل كلمات المرور خط الدفاع الأول، وإذا لم يتم تنفيذها بشكل مناسب، فيمكن أن تكون الحلقة الأضعف في المؤسسة. كما يجب أن تتضمن عناصر التحكم في كلمة المرور تغيير كلمة المرور عند تسجيل الدخول لأول مرة، والحد الأدنى لطول كلمة المرور والتاريخ، وتعقيد كلمة المرور بالإضافة إلى فترة الصلاحية القصوى. إضافة إلى ذلك، يجب تنفيذ كلمة مرور ديناميكية لمرة واحدة غير متكررة، لا تزيد صلاحيتها عن دقيقه واحده (لا يوجد متطلب رقابي لتحديد مده الصلاحية).

5. الضوابط والتعليمات الرقابية الخاصة بعمليات تحويل الأموال من خلال خدمات الإنترنت

فيما يتعلق ببعض الخدمات (عمليات تحويل الأموال إلى حسابات أطراف أخرى)، يجب أن يدعم باستخدام كلمة المرور الثانية أو OTP ليتم إرسالها إلى العميل عبر الرسائل القصيرة عبر الهاتف المحمول. يجب أن تنتهي صلاحية OTP بعد فترة زمنية ويجب أن يكون هناك حد عند تحويل الأموال إلى حسابات أخرى. إلى جانب، مراقبة المعاملات من خلال نظام مكافحة غسل الأموال ونظام مراقبة الاحتيال. كما يوجد متطلب رقابي ينص على ضرورة التأكد من المستفيد عند الإضافة لأول مره وذلك بتفعيل التحويل بعد مرور 24 ساعة.

6. الضوابط والتعليمات الرقابية الخاصة بسرية وسلامة المعلومات

الضوابط والتعليمات الخاصة بسرية وسلامة المعلومات الخاصة بالإنترنت البنكي، تتمثل فيما يلي:

- أمن وسلامة البيانات والأنظمة، لضمان عدم تعديل معلومات العملاء وأن الأنظمة خالية من الوصول غير المصرح به.
- سرية بيانات العملاء خلال عمليات التخزين وأثناء التجهيز والنقل.
- موثوقية وتوافر أنظمة الخدمات المصرفية عبر الإنترنت لتوفير الوصول الفوري إلى النظم للمستخدمين المسجلين والحفاظ على الفعالية التشغيلية.
- نهج استباقي للكشف عن الوصول غير المصرح به وتحديد المعاملات الاحتيالية المحتملة.

- المساءلة عن طريق تصميم إجراءات التشغيل الموحدة، والسياسات، والضوابط لضمان إمكانية تتبع جميع المعاملات.
- منع وصول الأطراف الثالثة لمعلومات العملاء. في حالة الرغبة بتشغيل طرف ثالث بخدمه تختص بمعلومات العملاء، يجب على البنك الحصول على الموافقة من البنك المركزي لتلك العقود.

7. الضوابط والتعليمات الرقابية الخاصة بتأمين التطبيقات الإلكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الإنترنت

تتمثل الضوابط والتعليمات الخاصة بتأمين التطبيقات الإلكترونية المستخدمة فيما يلي:

- يجب أن يضمن النظام عدم الكشف عن بيانات نصية واضحة حساسة، قبل تشفيرها.
- يجب أن تضمن منشأة التشفير التي يستدعيها النظام عدم تمكن المستخدمين غير المصرح لهم من الوصول إلى مفاتيح التشفير اللازمة لفك تشفير البيانات.
- تشفير الدورة الكاملة لجميع معاملات الويب القائمة على الشبكة التي يتم فيها نقل المعلومات الحساسة.
- يجب على البنوك أن تضع في كل طبقة من خلال تجزئة الشبكة المحلية / نشر أنظمة منع وكشف الحماية / التسلل.

- ينبغي على البنوك إجراء مراجعة مستمرة حول مدى ملائمة التقنيات والبنية التحتية للخدمات المصرفية الإلكترونية للحماية من التهديدات السيبرانية الناشئة.
- تحتاج البنوك إلى إنشاء سجلات لجميع قنوات تقديم الخدمة، والأنظمة، وقاعدة البيانات، ومعدات الشبكات. ويجب مراجعة السجلات على أسس مستمرة بواسطة فريق الأمن المعلوماتي.

8. بناء القدرات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

تعمل السلطة الرقابية المسؤولة عن القطاع المصرفي في عُمان على تعزيز القدرات البشرية لديها في مجال أمن الفضاء الإلكتروني عن طريق الدورات التدريبية المنتظمة والشهادات التخصصية في أمن المعلومات/ الأمن السيبراني/ الهجومات الإلكترونية، وغيرها فيما يختص بهذا المجال.

9. التحديات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

فيما يلي عرض لأهم التحديات التي تواجه الجهاز المصرفي في عُمان بخصوص دعم أمن الفضاء الإلكتروني:

- ضعف الخبرات المصرفية في هذا المجال.
- وجود عقود لأطراف ثالثه تختص بأمن نظم المعلومات مما أدى إلى وجود عمليات احتيال.
- عدم وجود سياسات لنظم الامن السيبراني لدى بعض المصارف بما يعتبر إخلالاً بالمتطلبات الرقابية.
- الهجمات السيبرانية وآلية البنوك في التصدي لها ومدى فعالية الجدار الأمني

تعاملت السلطة الرقابية في عُمان مع هذه التحديات، من خلال اتخاذ الإجراءات التالية:

- إصدار عدد من التعليمات الرقابية فيما يختص بأمن نظم المعلومات والعقود مع الطرف الثالث.
- فرض غرامات ماليه في حالة عدم الالتزام بالمتطلبات الرقابية.
- المتابعة الدورية لتطبيق الملاحظات التي أصدرها فريق التفتيش الميداني.

قطر

1. الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

تتمثل أبرز التعليمات الرقابية الصادرة في هذا الشأن فيما يلي:

- إنشاء إطار عمل لإدارة الأزمات والمخاطر.
- تحديد الأصول (الممتلكات) عالية الأهمية.
- مراقبة وتوثيق الأزمات.
- الحفاظ على أمن وسلامة المعلومات.
- إدارة التهديدات الأمنية ونقاط الضعف.

تتضمن عمليات الرقابة على أساس المخاطر (ongoing risk-based supervisory activities) اختبارات توضح مدى قدرة المصارف على مواجهة مخاطر أمن الفضاء الإلكتروني. كما أصدرت السلطات الرقابية خلال عام 2012 تعليمات وقواعد تنظم تقديم الخدمات المصرفية من خلال

الإنترنت، وتم تحديث تلك التعليمات في عام 2018. شملت تلك القواعد الخدمات المصرفية التالية:

- إدارة الحسابات إلكترونياً.
- المدفوعات والتحويل.
- طلب دفتر شيكات.
- طلب قرض.
- طلب إصدار بطاقة.

فيما يتعلق بالتعليمات الرقابية التي يتم فرضها على عمليات تعهيد أمن نظم المعلومات والأنظمة الإلكترونية للمصرف إلى جهة خارجية هناك العديد من التعليمات التي يتم فرضها عند القيام بعمليات الإسناد الخارجي، من أهمها وجود إطار عمل لإدارة المخاطر وضمان جودة الخدمات المقدمة من شركات الإسناد الخارجي، بالإضافة إلى القيام بعملية لتقييم المخاطر المتعلقة بأي تعاقد مع شركات الإسناد الخارجي. والجدير بالذكر أن مصرف قطر المركزي يفرض على جميع المؤسسات المالية الحصول على موافقة من قبله قبل توقيع العقد مع أي شركة خارجية.

كما توجد توجيهات رقابية تلزم المصارف بتضمين استراتيجيات المخاطر المُقرة من قبل مجالس إدارات البنوك إطاراً يتعلق بالمخاطر الإلكترونية ومخاطر نظم المعلومات والهجمات الإلكترونية. يتم التحقق من وجود تلك الاستراتيجيات بحيث تكون متضمنة مستوى المخاطر المتعلقة بأمن الفضاء الإلكتروني وإجراءات موازية لدعم مستويات أمن الفضاء الإلكتروني (cyber resilience) بما يشمل وجود سياسة واضحة لحوكمة إدارة مخاطر

أمن الفضاء الإلكتروني، وقيام المصارف بتعيين مسؤول عن أمن المعلومات [Chief Information Security Officer (CISO)].

2. الضوابط والتعليمات الخاصة بتنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الإنترنت

لا يسمح للعملاء بإنشاء أو فتح حساب مصرفي من خلال موقع البنك على شبكة الإنترنت، لصعوبة التأكد من هوية العميل، بالإضافة إلى وجود ضمانات يطلبها البنك من العميل يصعب التحقق من وجودها عن طريق الإنترنت البنكي. هناك بعض الضوابط والتعليمات (الشروط والأحكام) التي يطبقها البنك على العميل الراغب في الاستفادة من الخدمات المصرفية، إضافة إلى تلك الضوابط الخاصة بالتحقق من هوية وصلاحية العميل الراغب في الاستفادة من الخدمات المصرفية، أو إجراء أي تعديل على الحساب من خلال شبكة الإنترنت. تتمثل تلك التعليمات فيما يلي:

- التوعية بخصوص مخاطر الأمن الإلكتروني.
- آلية صارمة للتحقق من الهوية.
- عملية التوثيق المزدوجة (two-factor authentication).
- قائمة بأفضل الممارسات والقواعد.
- استخدام كلمة مرور إضافية لإجراء أي عملية مالية.
- استخدام بصمة اليد أو الوجه.
- إرسال رسالة نصية للتحقق من هوية المستخدم.
- استخدام نظام الرموز (Token) وهو نظام يستخدم لإدارة الصلاحيات.

3. الضوابط والتعليمات الخاصة بتنظيم وسائل إثبات الهوية عبر الإنترنت

تعتمد البنوك في التحقق من هوية العميل المستفيد من الخدمات المصرفية من خلال الإنترنت على استخدام كل من عملية التوثيق التي تعتمد على عاملين مختلفين للتأكد من هوية العميل (two-factor authentication)، وكلمة مرور إضافية لإجراء أي عملية مالية. إضافة إلى ذلك تقوم البنوك بتقييم تلك الوسائل عن طريق القيام بإصدار وتطبيق استراتيجية أمنية لحفظ البيانات، ووضع ضوابط للتأكد من سلامة البرامج الموجودة على الإنترنت، بالإضافة إلى الأنظمة المساندة والتي تشمل برامج التحقق من هوية العملاء وتفعيل نظام لمراقبة الأنظمة حيث يعمل هذا النظام على إرسال التنبيهات في حال حدوث أي نشاط غير معتاد. كما تقوم البنوك بإجراء اختبارات الاختراق وتقييم المخاطر لهذه الأنظمة الإلكترونية للتأكد من عدم تعرضها للاختراقات.

تتمثل الآلية التي تعتمد عليها البنوك في التحقق من تصديق العميل إلكترونياً من خلال الإنترنت، في إرسال رسالة نصية إلى الهاتف المحمول الخاص بالعميل للتحقق من تصديق العميل إلكترونياً من خلال الإنترنت. وبالنسبة لآلية تحكم المصارف في عدد مرات المحاولات الفاشلة للدخول إلى الحساب من خلال الإنترنت، فإنها تختلف من بنك إلى آخر، ولكن بشكل عام، تقوم البنوك بتعليق الحساب لفترة معينة بعد القيام بثلاث محاولات تسجيل دخول فاشلة، وذلك لمنع محاولات الاختراق من خلال تخمين كلمة السر.

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

يلزم مصرف قطر المركزي البنوك بوضع سياسة شاملة لإدارة كلمة السر، حيث تضم هذه السياسة بعض الشروط مثل تغيير كلمة السر كل ستين يوم. كما يلزم المصرف المركزي البنوك باستخدام كلمة السر لمرة واحدة عند

اجراء أي تحويل مالي بحيث لا تكون مكررة، ولكن بالنسبة لمواصفات هذه الكلمة، فهي راجعة لسياسة كل بنك.

5. الضوابط والتعليمات الرقابية الخاصة بعمليات تحويل الأموال من خلال خدمات الإنترنت

أثناء تحويل الأموال من حساب إلى حساب آخر عن طريق الانترنت، يتم استخدام عملية التوثيق المزدوجة وذلك للتحقق من هوية منفذ العملية (two-factor authentication)، كما أن هناك حد أقصى للمبالغ التي يستطيع العميل تحويلها إلى حساب آخر عن طريق الإنترنت البنكي.

6. الضوابط والتعليمات الرقابية الخاصة بسرية وسلامة المعلومات

يلزم مصرف قطر المركزي جميع البنوك باتخاذ كافة الإجراءات والتدابير الأمنية لضمان سرية وسلامة معلومات العملاء، حيث يجب على البنوك القيام بعملية تقييم للمخاطر لتحديد المخاطر المحتمل وقوعها واتخاذ التدابير اللازمة للوقاية منها. كما يقوم مصرف قطر المركزي بوضع معايير معينة لأدوات وبرامج الحماية التي يجب على البنوك استخدامها.

7. الضوابط والتعليمات الرقابية الخاصة بتأمين التطبيقات الإلكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الإنترنت

قام مصرف قطر المركزي بوضع لائحة من التعليمات لتأمين التطبيقات الإلكترونية الخاصة بالبنوك، من أهمها تثبيت برامج الحماية للحفاظ على هذه التطبيقات من الاختراق، بالإضافة إلى إجراء الاختبارات الأمنية على التطبيقات (قبل تثبيتها وبعده). كما يجب على البنوك تقييم نقاط الضعف

الموجودة في التطبيقات مرتين على الأقل سنوياً، والعمل على وضع خطة للحد من نقاط الضعف ومشاركة الخطة مع الإدارة العليا، بالإضافة إلى العديد من التعليمات والضوابط الأخرى التي تهدف إلى حماية التطبيقات الإلكترونية المستخدمة في البنوك من الاختراقات.

8. تقييم السلطات الرقابية للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني والوضع الراهن

تفرض السلطة الرقابية في قطر على المصارف القيام باختبارات الضغط (Stress Testing) لتحديد حجم الآثار المترتبة على نجاح أية عمليات قرصنة تتعرض لها الأنظمة الإلكترونية، ذلك بصورة دورية نصف سنوية. ويجب على البنك الإبلاغ عن الاختراقات وعمليات القرصنة بالغة الأهمية خلال ساعة من وقوعها (مثل الحالات التي يترتب عليها خسائر ملموسة للعملاء والتي تؤثر سلباً على عمليات المصرف).

9. التعاون والتنسيق مع السلطات الرقابية الأخرى عبر الحدود والشركاء في صناعة تقنية المعلومات فيما يتعلق بالمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

يتم التعاون مع المؤسسات الإقليمية والسلطات الرقابية خارج الدولة وذلك من خلال تشكيل اللجان المختلفة لمشاركة الخبرات ومعرفة أهم ما توصلت له هذه المؤسسات بهدف تطوير الأمن الإلكتروني في القطاع المالي. كما انه يتم التعاون مع مختلف المؤسسات والمراكز البحثية من خلال توقيع اتفاقيات التدريب والتطوير والتعاون للبحث عن سبل تطوير أمن المعلومات في القطاع المالي في دولة قطر.

10. بناء القدرات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

تعمل السلطة الرقابية على تعزيز القدرات البشرية لديها في مجال أمن الفضاء الإلكتروني سواءً في المرحلة الحالية أو المستقبلية، من خلال اتباع ما يلي:

- بناء قدرات موظفي الأمن الإلكتروني من خلال مشاركتهم في الدورات التدريبية (الداخلية والخارجية) المتعلقة بأمن المعلومات.
- إعطاء المجال للموظفين لاستكمال الدراسات العليا في مجال أمن المعلومات مما يعزز فرص تطويرهم ويصقل خبراتهم.
- تشجيع الموظفين على حضور المؤتمرات السنوية المتعلقة بمجال أمن المعلومات للاطلاع على آخر التطورات في هذا المجال.

11. التحديات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

من أهم التحديات التي تواجه القطاع المالي في الدولة التطور السريع في مجال تقنية المعلومات والاعتماد المتزايد على التقنيات للقيام بمعظم العمليات المالية، مما يؤدي إلى زيادة التعرض للتهديدات والحوادث الإلكترونية. تعاملت السلطة الرقابية مع هذه التحديات من خلال وضع تعليمات خاصة بأمن المعلومات وتطبيقها على جميع المؤسسات المالية في الدولة وتحديثها بشكل دوري، وتشكيل فريق متخصص في مجال أمن المعلومات لمتابعة مدى تطبيق المؤسسات المالية لقوانين الأمن الإلكتروني.

الكويت

1. الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

تتضمن التعليمات الرقابية الخاصة بإطار المخاطر التشغيلية (Operational Risks) جزءً متعلقاً بمخاطر نظم المعلومات وأمن الفضاء الإلكتروني في القطاع المصرفي، يحدد المعايير اللازم توافرها لضمان أمن الفضاء الإلكتروني. أبرز تلك التعليمات الرقابية تتمثل فيما يلي:

- تقضي التعليمات الخاصة بأمن المعلومات والمتضمنة بضرورة وجود سياسة شاملة لأمن المعلومات في البنوك على أن تكون معتمدة من الإدارة العليا في كل بنك ويتم تحديثها بصفة سنوية وفقا للمستجدات. ويجب أن تشمل السياسة الإجراءات اللازمة لتحقيق الجوانب الرئيسة المتعلقة بأمن وسلامة وتوافر المعلومات والحد من المخاطر الأمنية والتعامل مع الهجمات السيبرانية وتطبيق أعلى ضوابط الحماية للأنظمة وللخدمات والتطبيقات البنكية بما يتوافق مع مبادئ أمن المعلومات المتعلقة بالفصل في المهام وعدم التعارض مع المصالح.
- تعليمات للبنوك بشأن استمرارية الأعمال والتعافي من الكوارث مع ضرورة اعتماد تلك الخطط من مجلس إدارة البنك، وتحديث هذه الخطط بما يتوافق مع أنشطة ومنتجات البنك المتغيرة والتأكد من اختبار الخطة عن طريق عمل الاختبارات اللازمة للتأكد من فعاليتها بما يضمن استمرار تقديم الخدمات البنكية.

- التعليمات المتعلقة بحماية الخصوصية وسرية المعلومات بما يشمل وضع أنظمة الرقابة الداخلية للبنوك والآليات المناسبة بما يكفل حماية المعلومات المالية والشخصية للعملاء.
- تعليمات بشأن سياسة شاملة لأعمال البيئة الاحتياطية أو النسخ الاحتياطي لاسترجاع البيانات وفق إجراءات معتمدة، مع وجود بيئة عمل احتياطية مماثلة لكافة الأنظمة المالية والأنظمة الحساسة. والتأكد من سلامة المعلومات المحفوظة عن طريق الاختبارات اللازمة، وحفظ هذه النسخ في بيئة آمنه داخل وخارج دولة الكويت وتحديد المخولين من البنك باسترجاعها والدخول عليها عند الحاجة.
- تعليمات بشأن تأمين البطاقات المصرفية وضوابط الحماية عليها فيما يتعلق بآلية اصدار وتفعيل وإلغاء البطاقات وذلك بما يضمن سريتها وتشفير ما تحمله من معلومات، والخواص الأمنية المتعلقة بالأرقام السرية، والتحقق من العميل، وصحة البيانات، وذلك باستخدام التقنيات الحديثة والتأكد من تطبيق ضوابط الحماية اللازمة.
- تعليمات بخصوص مكافحة عمليات الاحتيال على البطاقات المصرفية (بطاقات السحب الآلي والبطاقات الائتمان).
- تعليمات بشأن تأمين المواقع الإلكترونية الرسمية للبنوك والتطبيقات المرتبطة بها.
- التعليمات المتعلقة بشأن تأمين غرفة التشغيل الرئيسية للأنظمة (Data Center).

كما أصدر البنك المركزي تعاميم تنص على أن تتضمن عمليات الرقابة على أساس المخاطر (ongoing risk-based supervisory activities) لاختبارات توضح مدى قدرة المصارف على مواجهة مخاطر أمن الفضاء

الإلكتروني (تجارب محاكاة لهجمات افتراضية). إضافة إلى ذلك، صدر عدد من التعاميم تنظم تقديم الخدمات المصرفية من خلال الإنترنت، شملت نطاق تطبيق هذه القواعد الخدمات المصرفية التالية:

- الخدمات المصرفية المتعلقة باستخدام المواقع الإلكترونية للبنوك (التسجيل في الخدمة، وضوابط الاستخدام المقبول، وتفعيل المستخدمين الجدد، والتأكد من صحة البيانات).
- خدمات إنشاء حسابات بنكية جديدة عبر الموقع الإلكتروني للبنك.
- خدمات التحويلات المالية الإلكترونية.
- خدمات إيقاف البطاقات المصرفية.
- خدمات إنشاء حساب مصرفي جديد.
- خدمات مرتبطة بإدخال شفرة سرية (OTP) تصل للهاتف لتنظيم حدود الدفع على قناة الدفع الإلكتروني، وتحديد سقف أعلى يومي وعدد عمليات.
- توفير متابعة ومراجعة للعمليات من خلال توفير نظم آلية لتقصي عمليات الاحتيال.

فيما يتعلق بالتعليمات التي يتم فرضها من جانب السلطات الرقابية على عمليات تعهيد أمن نظم المعلومات والأنظمة الإلكترونية للمصرف إلى جهة ثالثة (Third Party)، فقد تمثلت فيما يلي:

- تعليمات خاصة بالسرية وعدم الإفصاح بين البنك والجهات المراد تكليفها بالأعمال.
- تعليمات بشأن التأكد من كفاءة الجهة المُكلفة بالقيام بأعمال متعلقة بأمن المعلومات مثل القيام باختبارات الاختراق أو التقييم الأمني.

- تعليمات بشأن تغيير الجهة المكلفة للقيام بالأعمال كل سنتين على الأقل وذلك لضمان توفير حماية أفضل للبنك.
- فرض نوع من الرقابة والمتابعة لأداء الأطراف الأخرى عند الاستعانة بهم في تقديم الخدمات المصرفية عن طريق الإنترنت أو أجهزة الهاتف.

تلزم التوجيهات الرقابية المصارف بتضمين استراتيجيات المخاطر المُقرة من قبل مجالس إدارات البنوك إطاراً يتعلق بالمخاطر الإلكترونية ومخاطر نظم المعلومات والهجمات الإلكترونية (Cyber-attacks)، يتم التحقق منها من خلال عمليات الرقابة المصرفية بحيث تكون شاملة مستوى المخاطر والإجراءات الموازية لدعم مستويات أمن الفضاء الإلكتروني (cyber resilience)، بما يشمل وجود سياسة واضحة للحوكمة في هذا الشأن.

2. الضوابط والتعليمات الخاصة بتنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الإنترنت

يسمح للعملاء بإنشاء أو فتح حساب مصرفي، والاستفادة من الخدمات المصرفية من خلال موقع البنك على شبكة الإنترنت، ذلك في ضوء الضوابط التالية:

- في حال كان عميل سابق في البنك، يسمح له فتح حساب.
- أما في حال كان عميل جديد للبنك، فيجب مراجعة العميل لأحد فروع البنك للتأكد من أوراق العميل الثبوتية الخاصة به مثل البطاقة المدنية واعتماد الهاتف النقال الذي سيتم التعامل معه لإرسال الشفرات المطلوبة لتنفيذ العمليات التي تتم عن طريق شبكة الإنترنت، والتوقيع على فتح الحساب.

- التسجيل في الخدمات المصرفية الإلكترونية وتفعيلها من خلال إدخال الشفرة السرية (OTP) التي ترسل إلى هاتف العميل، ومن ثم يقوم بإدخالها عبر تطبيق تقديم الخدمة الخاص بالبنك.
- تطبيق معايير التحقق للدخول على المواقع الإلكترونية للخدمات المصرفية.
- استخدام شفرات إضافية لإضافة المستفيدين الجدد والتحويلات المالية.

إضافة إلى ذلك، يتحقق البنك من هوية وصلاحية العميل الراغب في الاستفادة من الخدمات المصرفية من خلال شبكة الإنترنت، من خلال اعتماد الضوابط والأساليب التالية:

- عدم إتمام عمليات التسجيل على الموقع الإلكتروني والتطبيقات المرتبطة به من خلال رقم بطاقة السحب الآلي والرقم السري الخاص بها فقط، وإنما يتم استخدام وسائل أخرى للتحقق من هوية العميل، مثل رقم هوية العميل، رقم جواز السفر، وأي معلومات أخري.
- عدم السماح للعميل بتخطي الخطوات الخاصة بالدخول على الموقع الإلكتروني وتطبيقاته، مثل الأسئلة الشخصية التي تم الإجابة عليها من قبل العميل عند التسجيل بالخدمة.
- عدم السماح للعميل بتكرار ذات الإجابة على الأسئلة الأمنية عند التسجيل بالاشتراك في خدمات الموقع الإلكتروني والتطبيقات المرتبطة به.

- تطبيق (Site Key) صورة وجملة، كمفتاح للموقع الإلكتروني والذي تم اختياره مسبقاً من قبل العميل لتعريف العميل بالموقع الأصلي للجهة، ومكافحة مخاطر التصيد الالكتروني.
- إرسال رسالة نصية قصيرة للعميل لتأكيد نجاح عملية التسجيل في الخدمة وفق لبيانات الاتصال المحفوظة لدى البنك.
- استخدام الشفرات السرية (OTP) التي ترسل إلى الهاتف النقال أو البريد الإلكتروني المعتمد لكل مستفيد.
- اسم المستفيد، الإجابة على الأسئلة الشخصية، التحقق من (Site Key)، إدخال الرقم السري. إدخال الشفرة السرية التي تصل إلى الهاتف النقال لتنفيذ العمليات المصرفية.

كما يجب على العميل زيارة الفرع للتحقق من إسم المستخدم والبيانات الرئيسية (مثل البطاقة المدنية أو الرقم الجواز) والتي تم استخدامها عند التسجيل في الخدمة بالإضافة إلى رقم الحساب البنكي. وأيضاً من خلال الأسئلة الشخصية بالاتصال بمركز الاتصال أو من خلال إدخال الشفرة السرية التي تصل إلى الهاتف النقال أو من خلال الفرع. كما يتعين على العميل إتمام عملية الدخول بالموقع الإلكتروني أو التطبيقات المرتبطة به، ثم إدخال كلمة السر القديمة ثم اختيار كلمة السر الجديدة وتأكيد طلب تنفيذ العملية. أما فيما يخص تغيير بيانات العميل لدى البنك، فإنه يمكن تغييرها من خلال الموقع الإلكتروني باستثناء أرقام الهاتف النقال، التي يتعين تغييرها من خلال الحضور الشخصي للعميل لأحد فروع البنك.

3. الضوابط والتعليمات الخاصة بتنظيم وسائل إثبات الهوية عبر الإنترنت

تعتمد البنوك على استخدام مبدأ الدخول المزدوج (Tow Factors Authentication) في التحقق من هوية العميل المستفيد من الخدمات المصرفية من خلال الإنترنت. يقوم البنك المركزي بصفته الجهة الرقابية للقطاع المصرفي بالتقييم الفني والأمني للخدمات المصرفية المقدمة من البنوك خاصة فيما يتعلق بالسرية والخصوصية والتحقق من الهوية وذلك قبل إصدار الخدمة. ثم يقوم كل بنك بالتقييم الأمني للخدمات الخاصة به بصفة مستمرة وفق الإجراءات والقواعد الداخلية المتبعة في كل بنك وقياس أداء الخدمات والوسائل التقنية المستخدمة للتحقق من هوية العميل عن طريق الاختبارات اللازمة للتأكد من فعالية هذه الوسائل، وقياس مؤشرات التعرض لحوادث أمن المعلومات أو دراسة وتحليل الأساليب التي تعرض لها البنك إن وجدت. كما يقوم البنك بالاستعانة بشركات متخصصة لتقييم مدى جاهزية شبكة البنك في التصدي للاختراق والقرصنة والبرامج الخبيثة والتجسس. تتم عملية التصديق والتحقق من هوية العميل إلكترونياً عن طريق قيام البنك بإرسال رسالة إلى هاتف العميل المحمول وفقا لبيانات العميل المحفوظة لدى البنك.

إضافة إلى ذلك، تشير التعليمات الرقابية إلى انه يتعين على البنوك وضع حد أقصى لمحاولات الدخول الخاطئة على الموقع الإلكتروني والتطبيقات المرتبطة به بما لا يزيد عن 3 محاولات لليوم الواحد، ومن ثم يتم إيقاف التعاملات البنكية الإلكترونية ولا تتم إعادة التفعيل إلا من خلال القنوات الأمنة، مثل قيام العميل بالاتصال بمركز خدمة العملاء في البنك وتنفيذ الإجراءات

المعتمدة للتحقق من الهوية، ومن ثم إعادة تفعيل الحساب على الموقع الإلكتروني، أو زيارة الفرع أو من خلال التطبيق الإلكتروني.

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

وفقاً لتعليمات البنك المركزي، يتعين على البنوك استخدام الضوابط المناسبة لكلمات السر الخاصة باستخدام الخدمات المصرفية عبر الإنترنت، بحيث تشمل التالي:

- وضع الحد الأدنى المناسب لعدد الخانات الخاصة بكلمة السر.
- عدم السماح بالتكرار باستخدام كلمات السر المستخدمة من قبل.
- عدم السماح بالتوالي في كلمة السر.
- التنويع باستخدام أحرف كبيرة وصغيرة.
- استخدام الأرقام والرموز الخاصة.

أما بالنسبة للتعليمات والمواصفات الخاصة بكلمة السر التي تستخدم لمرة واحدة والصادرة باستخدام أجهزة رموز الأمان (OTP)، يتم إرسال تلك الشفرة السرية (OTP) للهاتف المسجل للعميل لدى البنك ولا يتم تغييرها إلا بمراجعة العميل للبنك. من مسؤولية العميل، تحديث الهاتف النقال لدى البنك في حال استبدال ذلك الرقم.

5. الضوابط والتعليمات الرقابية الخاصة بعمليات تحويل الأموال من خلال خدمات الإنترنت

تتمثل الضوابط والتعليمات الخاصة بتحويل الأموال من حسابات العملاء إلى حسابات أطراف أخرى من خلال خدمات الإنترنت البنكي، بالالتزام بالتعليمات

الخاصة بمكافحة غسيل الأموال، وبالتعليمات الخاصة بدخول الموقع الإلكتروني.

6. الضوابط والتعليمات الرقابية الخاصة بسرية وسلامة المعلومات

تتمثل أهم الضوابط والتعليمات الخاصة بسرية وسلامة المعلومات الخاصة بالإنترنت البنكي، فيما يلي:

- توفير أنظمة آمنة للتعاملات الإلكترونية، والتأكد من كفاءتها لمواكبة التغيرات في الأساليب الاحتيالية.
- وضع أنظمة الرقابة الداخلية الفعالة التي تكفل الحد من عمليات الاحتيال والاختلاس أو إساءة استخدام الخدمات المالية.
- توفير البيئة الداخلية التي تكفل تحقيق الأمن والسرية لكافة المعلومات والبيانات، بحيث يتم اختبار هذه البيئة بشكل مستمر للتأكد من صلاحيتها.
- التأكد من التزام الجهات الخارجية بالمبادئ التي يشملها دليل حماية العملاء وأنها تعمل لما فيه مصلحة عملاء البنك وأنها تتحمل مسئولية حمايتهم بما فيها المحافظة على السرية المصرفية لمعلوماتهم.
- التأكد من استيفاء كلمات السر للمعايير العالمية أو المتحفظة من حيث التنوع في استخدام الأحرف والأرقام والرموز الأخرى.

7. الضوابط والتعليمات الرقابية الخاصة بتأمين التطبيقات الإلكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الإنترنت

بهدف تأمين التطبيقات الإلكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الإنترنت، صدرت التعليمات والضوابط التالية:

- استخدام برامج الحماية التي تضمن المحافظة على خصوصية وسرية بيانات العملاء وحمايتها من الاختراق.
- توثيق المعاملات، وإمكانية تحديد الأطراف المقابلة، والرقابة على الدخول للأنظمة المستخدمة.
- وضع قواعد واضحة ومحددة لمعالجة أية حالات للخطأ أو الاحتيال في حالة وقوعه.

8. التعاون والتنسيق مع السلطات الرقابية الأخرى عبر الحدود والشركاء في صناعة تقنية المعلومات فيما يتعلق بالمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

يتم في هذا الشأن عقد ورش عمل سنوية للمختصين في أمن المعلومات من البنوك المركزية لدول مجلس التعاون لدول الخليج العربية لمناقشة التحديات وتبادل الخبرات وتوحيد الجهود في مجال الأمن السيبراني. كما يتم تبادل المعلومات عن الهجمات السيبرانية النشطة أو التهديدات المحتملة التي تواجهه القطاع المصرفي مع الجهات الرقابية المصرفية ذات الصلة (البنوك المركزية لدول مجلس التعاون لدول الخليج العربية)، ذلك لاتخاذ ما يلزم من إجراءات واحترازات أمنية. إضافة إلى التواصل مع البنوك المركزية العالمية في أوروبا

عن طريق عقد اجتماعات/المراسلات الإلكترونية لمناقشة أهم وسائل الحماية للتصدي للهجمات السيبرانية ووسائل التأمين والحماية.

بالنسبة لأهم ملامح التعاون والتنسيق بين القطاع المصرفي وصناعة تقنية المعلومات فيما يتعلق بأمن الفضاء الإلكتروني، فانه يتم التنسيق مع وزارة التربية والتعليم في الكويت لتضمين التقنيات المالية وأمن ومخاطر أمن المعلومات في مناهج الوزارة وبمستويات مختلفة وذلك لرفع مستوى الوعي حول تقنية وأمن المعلومات. وكذا التنسيق مع الجهات الرقابية المحلية لتطبيق الاستراتيجيات الوطنية والقوانين المعتمدة في الدولة. كما يتم العمل حالياً على مشروع بناء الإطار الاستراتيجي للأمن السيبراني للقطاع المصرفي في دولة الكويت والذي من المتوقع أن يقوم بعمل تقويم شامل لوضع الأمن السيبراني. كما سيتم إصدار دليل لمعايير أمن المعلومات الخاصة في القطاع المصرفي ومن ثم يتم مراقبة تطبيق هذه المعايير وكفاءة الأمن السيبراني لدى القطاع المصرفي.

9. بناء القدرات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

يعمل البنك المركزي الكويتي على تعزيز القدرات البشرية في القطاع المصرفي بمجال أمن الفضاء الإلكتروني مع الأخذ بالاعتبار المقترحات والمبادئ الرقابية الصادرة عن المؤسسات الدولية في هذا الشأن، وذلك من خلال الوسائل التالية:

- تدشين البرامج التدريبية المتخصصة بالأمن السيبراني للعاملين من داخل وخارج القطاع المصرفي لتطوير المهارات والكفاءات الوطنية وذلك بإشراف شركات عالمية متخصصة في هذا المجال.

حيث يخضع المتدربين إلى برامج تدريبية مكثفة داخل وخارج الدولة يتم خلالها الاطلاع على أحدث الوسائل والأدوات والتقنيات بالإضافة إلى التدريب الميداني والاختبارات المهنية.

- توجيه القطاع المصرفي بشكل عام الى تكثيف الجهود لتهيئة وتعزيز القدرات البشرية في هذا المجال وذلك عن طريق دعم التعليم الأكاديمي والبعثات الدراسية الخارجية للحصول على شهادات أكاديمية عليا من جامعات خارجية مرموقة.
- استخدام وسائل متنوعة لنشر التوعية الأمنية المستمرة مثل عقد مؤتمرات، دورات تدريبية، منشورات ووسائل التواصل الاجتماعي المعتمدة لتوعية العاملين في القطاع المصرفي.

10. التحديات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

يعتبر التطور المتسارع في مجال الأمن السيبراني وأساليب الهجمات والتهديدات من أهم التحديات التي تواجه الجهات الرقابية وخاصة فيما يتعلق بدعم أمن الفضاء الإلكتروني في القطاع المصرفي. وقد تعاملت السلطة الرقابية مع هذه التحديات من خلال الوسائل التالية:

- تكثيف وسائل التعليم والتدريب للتعرف على أحدث التقنيات والأدوات لمواكبة التطور التكنولوجي المتسارع عن طريق تكثيف البرامج التدريبية المهنية المتخصصة بالأمن السيبراني.
- الاستعانة بالشركات المتخصصة لتقديم خدمات الاستشارات اللازمة والاستفادة من الخبرات فيما يخص أمن المعلومات.

- العمل على خلق كوادر بشرية متخصصة في مجال الأمن السيبراني عن طريق إعداد وطرح البرامج التدريبية الأكاديمية وذلك بدعم التعليم الأكاديمي والبعثات الدراسية الخارجية للحصول على شهادات أكاديمية عليا من جامعات عالمية.
- التنسيق مع الجهات الرقابية الخارجية ذات الاختصاص (دول مجلس التعاون لدول الخليج العربية) لتبادل الخبرات والمعلومات المتعلقة بأمن المعلومات وأساليب الهجمات ووسائل الحماية.

لبنان

1. الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

تتمثل أبرز التعليمات الرقابية الصادرة عن السلطات الرقابية في لبنان والخاصة بمخاطر نظم المعلومات وأمن الفضاء الإلكتروني في القطاع المصرفي، في إصدار تعاميم خاصة بالعمليات المالية والمصرفية بالوسائل الإلكترونية، والوقاية من أفعال الجرائم الإلكترونية وضمان أمان أنظمة تكنولوجيا المعلومات لدى المصارف والمؤسسات المالية ومؤسسات الوساطة المالية. إضافة إلى الدليل الإرشادي للوقاية من الأفعال الإجرامية بواسطة البريد الإلكتروني الصادر عن مصرف لبنان وهيئة التحقيق الخاصّة، وجمعية مصارف لبنان، ومكتب مكافحة جرائم المعلوماتية، وحماية الملكية الفكرية التابع لوحدة الشرطة القضائية خلال عام 2016. كما أن هناك تعميم تطبيقي لقرار مصرف لبنان المتعلّق بالوقاية من أفعال الجرائم الإلكترونية "التدابير والإجراءات التقنية الاحترازية المتعلّقة بأمان الخدمات المالية والمصرفية بالوسائل الإلكترونية".

كما تمّ إصدار الدليل الإرشادي للوقاية من الأفعال الإجرامية خلال 2016، وقرار مركّز على الوقاية من الأفعال الإجرامية الإلكترونية خلال عام 2017. فيما يلي عرض للخدمات المصرفية المشمولة في نطاق تطبيق هذه القواعد:

- الاطلاع على الحسابات المصرفية وطلب الكشوفات التفصيلية لها.
- عمليات الدفع بأنواعها (السندات، والصكوك التجارية).
- عمليات التحويل بين حسابات في نفس المصرف وبين حسابات بين مصارف مختلفة [ولكن دائماً في هذه الحال عبر شبكة SWIFT)].
- طلب القروض المصرفية.
- المباشرة بإعداد مستندات فتح الحسابات (على أن يتمّ تنفيذها بعد حضور العميل شخصياً لأخذ توقيعه الخطي).
- وضع سقوف معينة للخدمات المصرفية المقدمة عبر الوسائل الإلكترونية، بما يشمل كافة العمليات المصرفية، وبشرط تأمين التوقيع الخطّي للعميل على اتفاقية التعامل مع المصرف (Terms & Conditions) واستكمال مستندات "أعرف عميلك" (Know Your Customer).

بالنسبة للخدمات المصرفية غير المشمولة في نطاق تطبيق هذه القواعد، فإنها تتفاوت من مصرف إلى آخر حسب مدى جاهزية هذه المصارف لتقديم الخدمات المصرفية عبر شبكة الإنترنت. فبينما خطت المصارف الكبرى نحو إنشاء فروع إلكترونية (e-branch) تقدّم كافة خدمات الفرع وتستقبل المستندات بحضور موظف مُرشد عن بُعد (عبر شاشة)، فهناك مصارف

تتفاوت خدماتها الإلكترونية من خدمة إطلاع فقط إلى خدمات عمليات دفع وتحصيل وطلب شيكات. وربما يدلّ هذا على حرص المصارف على التقدّم تدريجياً في خدماتها الإلكترونية لتجهيز الأنظمة وتعزيز الجهاز البشري التقني المسؤول عن أمان هذه الخدمات.

فيما يتعلق بالتعليمات الرقابية التي يتم فرضها على عمليات تعهيد أمن نظم المعلومات والأنظمة الإلكترونية للمصارف إلى جهة ثالثة (Third Party)، فإنّ تعميم لجنة الرقابة على المصارف الصادر عام 2011 والمتعلّق بأمان أنظمة تقنيات المعلومات لدى المصارف والمؤسسات المالية ومؤسسات الوساطة المالية، يتضمّن في المادّة الثالثة منه "قواعد الإلزام الخارجي لمزودي خدمات وأنشطة المصارف والمؤسسات المالية ومؤسسات الوساطة المالية" وتشمل التعليمات التالية:

- يجب أن يرتكز قرار الإسناد على دراسات مبيّنة توضح مبررات الخيار المتّخذ على أن يتمّ توثيق هذه الدراسات تسهيلاً لأعمال المراجعة والتدقيق.
- يجب أن يراعي اختيار الشركة الملتزمة معايير الكفاءة والخبرة والملاءة والنزاهة وأن يتمّ وفق دفتر شروط واضح وشامل.
- على المصرف أو المؤسسة مراقبة سلامة أداء الشركة الملتزمة وتقييمها دورياً واتخاذ الإجراءات المناسبة لتصحيح أي خلل في تنفيذ عقد الإسناد عند الحاجة، بما فيه اللجوء إلى إنهائه طوعاً.
- وضع أسس واضحة لاختيار الشركة مزودة الخدمات وفق المعايير التالية:

أ) اختيار الشركات المرشّحة لالتزام الخدمة وفق دفتر شروط واضح وشامل (Request For Proposal).
ب) دراسة وضعية الشركة مزودة الخدمة إدارياً وتقنياً، وخبرتها في تقديم الخدمة المطلوبة.
ج) تضمين دفتر الشروط، ولاحقاً العقود التي تتبعها، البنود التي تضمن التزام الشركات الملتزمة بتقديم الخدمة وفق متطلبات تعاميم ومذكرات مصرف لبنان ولجنة الرقابة على المصارف وهيئة التحقيق الخاصة.

- اتخاذ التدابير المناسبة لضمان استمرارية الخدمة في حال توقّف تقديمها من قِبَل الشركة مزودة الخدمة وذلك وفقاً لاتفاقية محددة لإنهاء عقد الإسناد (Escrow Agreement upon source programs and Exit Strategies)، وبالتالي وضع خطط متابعة العمل التي تُمكّن من استعادة تسيير الخدمة داخلياً بشكل طبيعي وميسّر.

إضافة لما سبق، هناك توجيهات رقابية تلزم المصارف بتضمين استراتيجيات المخاطر المُقرة من قبل مجالس إدارات البنوك إطاراً يتعلق بالمخاطر الإلكترونية ومخاطر نظم المعلومات والهجمات الإلكترونية (Cyber-attacks)، بحيث يتم التحقق منها من خلال عمليات الرقابة المصرفية في هذا الشأن. كما يتم إلزام المصارف بتعيين مسؤول عن أمن المعلومات [Chief Information Security Officer (CISO)].

2. الضوابط والتعليمات الخاصة بتنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الإنترنت

في هذا الاطار، يسمح للعملاء بإنشاء أو فتح حساب مصرفي من خلال موقع البنك على شبكة الإنترنت، بحيث يُمكن للعميل الجديد تعبئة مستندات فتح الحساب عبر الوسائل الإلكترونية، إلّا أنّ التشغيل الفعلي لحساباته وعملياته لا يتمّ إلّا بعد أن يتقدّم العميل بشخصه إلى أحد فروع المصرف المعني للتوقيع الخطّي على المستندات ومنها مستندات (Agreement/Terms and Conditions) واستمارات "أعرف عميلك" (KYC). بعد أخذ تواقيع العميل، يتمّ إدراجه على لائحة العملاء ومنحه اسم مستعمل وكلمة سرّ أو رمز إضافي لمرّة واحدة (Token) لتحميل البرامج الإلكترونية على هاتفه المحمول أو الولوج مباشرةً على الموقع الإلكتروني للمصرف، ومن ثمّ يقوم بفتح الحساب عبر التطبيق الإلكتروني والقيام بالعمليات تِبعاً لضوابط أمان تقنية متعدّدة. إضافة إلى ذلك، فإنّ القوانين اللبنانية المنظّمة للتعامل الإلكتروني بالمستندات الإلكترونية مُنتظر إقرارها في أقرب تاريخ من قِبَل السلطة التشريعية (مجلس النوّاب) للسماح بالتوقيع الالكتروني (e-Signature). يُمكن بعد إقرارها الاستناد إلى مسوغ قانوني لتعريف العميل عن بُعد وفتح الحسابات المصرفية بالوسائل الإلكترونية دون الحضور إلى المصرف للتوقيع الخطّي. ويكون أيضاً للقضاء أرضية قوانين واضحة للفصل في القضايا.

فيما يلي عرض للضوابط والتعليمات (الشروط والأحكام) التي يطبقها البنك في لبنان على العميل الراغب في الاستفادة من الخدمات المصرفية من خلال شبكة الإنترنت:

- أن يكون عمره فوق 18 عاماً.
- أن يستوفي كل متطلبات ومستندات "أعرف عميلك" (KYC).
- أن يكون الحساب المصرفي فردي وليس مشترك (في بعض المصارف).
- أن يطّلع على آلية الخدمات التي يطلبها وعلى شروط وأحكام تنفيذها وأن يُوقّع على فهمه لها.
- أن يطّلع على إرشادات المصرف فيما يتعلّق بمخاطر العمليات الإلكترونية (كعدم إفشاء كلمات السرّ وضرورة الحفاظ على خصوصية بطاقاته وأهمية التيقّظ في الردّ على البريد الإلكتروني والتنبّه لطلبات ترِدُ على الخدمة عبر تطبيقات الإنترنت.
- ضرورة إبلاغ المصرف عن كل عملية مشبوهة أو حدوث أشياء غير معهودة تظهر في تطبيق الخدمة وذلك خلال أقصر وقت مبكر من لحظة اكتشافه لأي التباسات.

بخصوص الضوابط والأساليب التي يعتمد عليها البنك في التحقق من هوية وصلاحية العميل الراغب في الاستفادة من الخدمات المصرفية (أو الراغب في تنفيذ أنشطة مصرفية) من خلال شبكة الإ نترنت، لا زالت القوانين التي ترعى الاتفاقات بين الأفراد والمؤسسات في لبنان تستوجب التوقيع الخطي من الجانبين، وهذا الأمر يُحتّم على العميل الحضور شخصياً إلى المصرف للتوقيع على مستندات بياناته الشخصية واتفاقية (Terms & Conditions) قبل المباشرة بفتح الحسابات المصرفية. أمّا الضوابط التقنية فهي كثيرة تستند على مبدأ (Multi Authentication Process)، إضافةً إلى آلية الاتصال المباشر بالعميل إذا تطلّب الأمر (Call Back).

بالنسبة للحسابات الخاصة بالأشخاص الاعتبارية، فإنه يتم التحقق من هوية وصلاحية المخولين بالاستفادة من الخدمات المصرفية من خلال شبكة الإنترنت، عن طريق أحد الحلول التالية:

الحلّ الأول: هو المُعتمد في تعريف إلكتروني مستقلّ لكل شخص يتشارك في الحساب بحيث تسري نفس الضوابط المعهودة في الحسابات الفردية (شخص واحد صاحب الحساب).

الحلّ الثاني: هو تطبيق مختصّ بالشركات حيث تُعتمد هيكلية تعريف تُمنح لكل مستخدم مخوّل التعامل في حسابات الشركة (الاعتبارية) اسم مستخدم وكلمة سرّ خاصّة به (Specific credentials for every use)، مشابهة لهيكلية موظفي المصرف المخوّلين التعامل مع حسابات العملاء.

كما تتّخذ المصارف الضوابط التالية للتحقّق من هوية العميل عند قيامه بعمليات إلكترونية عبر الإنترنت:

- حصر خدمة العمليات الإلكترونية عبر الإنترنت (HTML) أو من جهاز هاتف محمول محدّد (Web or (Apps).
- اعتماد عملية توثيق متعددة والتحقق من هوية العميل بما يشمل (Multi Factors Authentication) وتعريف المستخدم من خلال كلمة سّر لكل اسم مستخدم، ورمز إضافي سرّي متحرّك لمرّة واحدة (OTP) يتلقّاه على جهاز الخلوي عبر خدمة الرسائل القصيرة (SMS).
- اعتماد سلّة خدمات محدّدة السقوف وظروف استعمالاتها إذا أمكن.

3. الضوابط والتعليمات الخاصة بتنظيم وسائل إثبات الهوية عبر الإنترنت

تعتمد عليها البنوك على عدد من الوسائل في التحقق من هوية العميل المستفيد من الخدمات المصرفية من خلال الإنترنت، اعتماد Multi Factor Authentication لتعريف المستخدم، وربط الخدمة المصرفية بجهاز هاتف محدّد بحيث لا يُمكن استعمال الخدمة على جهاز غير مسجّل للخدمة. إضافة الى تشفير المعلومات المتبادلة بين المصرف والعميل لمنع استغلالها من طرف ثالث، وتوثيق كافة معطيات وظروف العمليات التي يُجريها العميل Date stamp) user credentials, IP addresses, operations completeness status, OTP effectiveness) كما تقوم البنوك بدراسة شاملة لمخاطر تكنولوجيا المعلومات ومنها مخاطر العمليات عبر شبكة الإنترنت، بدءاً بهيكلية تقنية تحمي دقة المعلومات خلال كافة مساراتها (Integrity Check) منذ نشأتها لدى العميل (VPN Tunnel)، واعتماد آلية تشفير أمينة (High level of Encryption). إضافةً إلى إجراء اختبارات محاولات الدخول المتخصّصة (Intrusion Penetration Test). إضافة الى اعتماد هيكلية برامج لمكافحة البرامج الخبيثة وبرامج التجسس (Antivirus, antimalware, Systems Patch Management). وكذا اعتماد برامج ذكية لرسم الخط المعهود لاستعمالات الخدمة من قِبَل العميل (System Self Learning Customers Behavior)، بحيث يُطوّر نظام الخدمة ذاته للتعرّف على عادات العميل وتطويعها في التغيّرات بعد التأكد من رغبة العميل بذلك.

بخصوص الآلية التي تعتمد عليها البنوك في التحقق من تصديق العميل إلكترونياً من خلال الإنترنت، هناك عدد من الوسائل:

- رسالة إلى هاتفه المحمول (SMS) لإبلاغه بالعملية المنفذة.
- رسالة إلى هاتفه المحمول (SMS as OTP) طلباً لتأكيد العملية قبل تثبيتها.
- الاتصال هاتفياً بالعميل في حال تجاوزت قيمة العملية سقفاً معيّناً، وخاصّةً في العمليات التجارية حيث يكون الاتصال منهجياً بالاستنادً إلى دراسة تقييمية لمخاطر العمليات التجارية (الشركات).
- بريد إلكتروني للعميل بكل عملية تتمّ عبر الوسائل الإلكترونية.

بالنسبة للآلية التي تعتمد عليها البنوك في لبنان بهدف التحكم في عدد مرات المحاولات الفاشلة للدخول إلى الحساب من خلال الإنترنت، فإنه يتمّ تجميد الخدمة للعميل بعد ثلاث محاولات فاشلة له للدخول إلى الخدمة (أو للمنتحل تعريفه) مع إبلاغه بهذا الأمر على هاتفه المحمول بواسطة رسالة قصيرة أو من خلال الاتصال الهاتفي المباشر معه، وإبلاغه أنّ عليه مراجعة المصرف لاستيضاح الأمر وإعادة تشغيل الخدمة.

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

أشار رد السلطات الرقابية في لبنان على الاستبيان، أنّ المواصفات الدنيا لكلمات السرّ والمُعتمدة في المعايير المتعارف عليها عالمياً، يتمثل أهمّها فيما يلي:

- أن تكون معقدّة صعبة الاستنتاج (Complex).
- ألا تقلّ عن ثماني خانات مختلطة بين الأرقم والأحرف.
- أن تتضمّن أحرف (CAPS).

- أن يُفرض تغييرها فور استلامها للمرّة الأولى، ومن ثمّ دورياً تحدّد مدّتها بالاستناد إلى دراسة تقييمية لمخاطرها (من شهر إلى ثلاث أشهر).
- ألا تتكرّر بشكل دوري في فترة نطاقها لا يقل عن إثنى عشر شهراً ولا يزيد عن سنتين.
- إضافةً إلى تزويد العميل بإرشادات حول الحفاظ على سرّيتها، وعدم إفشاءها لأيّ كان وخاصّة للطلبات المشبوهة التي تنتحل صفة المصرف (phishing).

كما يتم اعتماد كلمات السر التي تستخدم لمرة واحدة في آليات التعريف (Multi Authentication) وأيضاً عند إجراء أي عملية مصرفية (دفع، تحويل أموال، تعديل في معطيات خدمة العميل أو خياراته). يتم تزويد العميل بهذه الكلمات من خلال نظام مستقلّ عن النظام الذي تتمّ عليه العمليات لتفادي مخاطر (One Single Point of Failure)، عبر (Token Device) أو برنامج. كما يجب أن تكون مدّة صلاحية هذه الكلمات قصيرة جدّاً تتناسب ومخاطر العمليات المصرفية المباشرة عبر الوسائل الإلكترونية (من دقيقة إلى عدّة دقائق).

5. **الضوابط والتعليمات الرقابية الخاصة بعمليات تحويل الأموال من خلال خدمات الإنترنت**

لا تتم عمليات تحويل الأموال من حسابات العملاء إلى حسابات أطراف أخرى (في مصارف أخرى) بصورة فورية بل إنّ متطلبات قرار مصرف لبنان الأساسي المتعلّق بالعمليات المالية والمصرفية بالوسائل الإلكترونية

الصادر في عام 2000، تنص على أنه يجب أن يتمّ على ثلاث مراحل كما يلي:

المرحلة الأولى: قيام العميل بطلب التحويل من خلال خدمة التحويل الإلكترونية المعتمدة لدى المصرف.

المرحلة الثانية: تحويل العملية في مصرف العميل إلى دوائر (Back Office) لتدقيق طلب التحويل (هوية العميل، المبلغ المحوّل، مستند لشرعية التحويل بين العميل والمستفيد، الوجهة الاقتصادية) ومن ثمّ إرساله إلى مصرف المستفيد عبر شبكة (Swift) المعهودة.

المرحلة الثالثة: تلقّي مصرف المستفيد عملية التحويل عبر شبكة (Swift) وإنجاز العملية.

6. الضوابط والتعليمات الرقابية الخاصة بسرية وسلامة المعلومات

تتمثل الضوابط والتعليمات الخاصة بسرية وسلامة المعلومات الخاصة بالإنترنت البنكي في الضوابط التالية:

- طبيعة ومواصفات الهيكلية المعتمدة للمعلومات (As per the database design).
- الإدارة المخوّلة وضع أسس لحفظ والتعامل بحوكمة المعلومات (Data Governance).
- نظام الصلاحيات الممنوحة للمستعملين المخوّلين بالاطلاع والتعامل بهد المعلومات (rights to data).
- إجراءات تقنية كتشفير مناسب للمعلومات (Encryption) أو حجبها عن غير المعني بها (Masking).

- نظام قيود (Logging) يساعد على التدقيق بعمليات الاطلاع ومعالجة المعلومات بصورة مناسبة لحساسيّتها (Data Sensitivity).

7. الضوابط والتعليمات الرقابية الخاصة بتأمين التطبيقات الإلكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الإنترنت

تشمل التعليمات الرقابية ضرورة التحقق من أمان أنظمة المعلومات (IT Security) والتطبيقات الإلكترونية المستخدمة وإخضاعها لكافة السياسات والإجراءات المعتمدة في هذا الشأن، وخاصّةً تعميم لجنة الرقابة على المصارف الصادر بعام 2000 والمتعلّق بأمان أنظمة تكنولوجيا المعلومات وكذا تعميم لجنة الرقابة على المصارف الصادر عام 2011 والخاص بجودة أنظمة وبرامج المعلوماتية – تقارير جودة الأنظمة المعلوماتية وقواعد قياسها. من جهة أخرى، يجب أن تخضع كل خدمة أو تطبيق مصرفي من خلال الوسائل الإلكترونية لدراسة جدوى، تجهيز البنية التحتية الأمنية (Secure Infrastructure)، وتزويد مصرف لبنان ولجنة الرقابة على المصارف بملف حول كلّ خدمة جديدة بالوسائل الإلكترونية قبل شهر على الاقل قبل إطلاقه يتضمّن مستندات مشروع الخدمة (ماهية الخدمة، الخدمات التي تتضمّنها، البنية التحتية، اختبارات التشغيل واختبارات الضغط واختبارات القبول التي خضعت لها).

8. تقييم السلطات الرقابية للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني والوضع الراهن

بلغ عدد حالات الإبلاغ التي تلقتها السلطة الرقابية والمتعلقة بانتهاكات لأمن الفضاء الإلكتروني في القطاع المصرفي خلال عام 2017 حوالي عشرة

حالات جدّية عدا محاولات (DDOS)، وخلال النصف الأول من عام 2018 ثلاث حالات جدّية عدا محاولات (DDOS). علماً انّ حالات إبلاغ السلطات الرقابية يحدّدها تعميم لجنة الرقابة على المصارف الصادر خلال عام 2011 الخاص بحالات الإبلاغ عن حوادث إرباك الأنظمة المعلوماتية والتشغيلية الرئيسة الناتجة عن عوامل داخلية او خارجية. فيما يلي عرض لأبرز حالات انتهاك الخاصة بأمن الفضاء الإلكتروني التي تعرض لها القطاع المصرفي في لبنان خلال عامي 2017 و2018، مرتبة حسب أهميتها:

جدول رقم (3)

أبرز حالات انتهاك الخاصة بأمن الفضاء الإلكتروني التي تعرض لها القطاع المصرفي اللبناني

خلال عامي 2017 و2018

نوع الهجمات	يتم تقييم أهمية حدوث كل حالة كما يلي: 1 (ترمز الى تكرار الحدوث) 2 (متوسطة الحدوث) 3 (نادرة الحدوث)
• برمجيات خبيثة (Malware)	**2**
• هجوم إلكتروني سطحي (اختراق سطحي لموقع المصرف على الإنترنت يتسبب في إيقاف عمل الموقع، أو تغيير الصفحة الرئيسية).	**3**

نوع الهجمات	يتم تقييم أهمية حدوث كل حالة كما يلي: 1 (ترمز الى تكرار الحدوث) 2 (متوسطة الحدوث) 3 (نادرة الحدوث)
• هجوم إلكتروني يتسبب في وقف نظام آلي عن العمل (نظام مدفوعات، نظام شراء إلكتروني، من خلال إرسال طلبات وهمية ضخمة في الثانية الواحدة).	**3**
• اختراقات/ سرقة بيانات العملاء أو الحسابات المصرفية.	**3**

المصدر: مصرف لبنان (2018) من خلال "استبيان الجوانب المتعلقة بأمن الفضاء الإلكتروني (Cyber Security) في إطار المخاطر التشغيلية: تجارب رقابية عربية".

كما تفرض السلطة الرقابية على المصارف القيام باختبارات الضغط (Stress Testing) لتحديد حجم الآثار المترتبة على نجاح أية عمليات قرصنة تتعرض لها الأنظمة الإلكترونية، وذلك بصفة دورية سنوية. وتلزم السلطة الرقابية المصارف بالإبلاغ عن تعرضها لأية عمليات قرصنة إلكترونية (Cyber-event reporting) في غضون يوم أو يومين من التعرض. وذلك لكافة حالات الخروقات الخاصة بأمن الفضاء الإلكتروني، والتي يترتب عليها خسائر ملموسة للعملاء، والتي تؤثر سلباً على عمليات المصرف.

9. التعاون والتنسيق مع السلطات الرقابية الأخرى عبر الحدود والشركاء في صناعة تقنية المعلومات فيما يتعلق بالمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

تقوم لجنة الرقابة على المصارف باتصالات دورية مع سلطات رقابية لمناقشة أمور أمن الفضاء الإلكتروني ذلك من خلال زيارات متبادلة ولقاءات في مؤتمرات دولية بهذا الشأن، كما تقوم اللجنة بتنظيم ندوات كما سيتمّ خلال شهر أيلول مع سلطات رقابية تابعة للدول الفرنكوفونية. كما تقوم جمعية المصارف في لبنان بالتعاون مع شركات تقنيات المعلومات بعقد لقاءات ومؤتمرات ودورات تكاد تكون شهرية حول المخاطر التشغيلية المترتّبة على القطاع المصرفي والمالي، شملت في النصف الأول من سنة 2018 المخاطر السيبرانية (Cyber Security).

10. بناء القدرات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

يتمّ تعزيز القدرات البشرية لدى لجنة الرقابة من خلال إخضاع الكوادر المسؤولة لديها عن تنظيم ومراقبة أمن الفضاء الإلكتروني لدورات داخلية وخارجية متخصّصة بمتطلبات أمن العمليات الإلكترونية وحضور مؤتمرات ومعارض لشركات تقنيات المعلومات.

11. التحديات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

أهم التحديات التي القطاع المصرفي اللبناني في هذا الشأن تتمثل فيما يلي:

- رفع إدارة أمن الفضاء الإلكتروني إلى أعلى المراجع في إدارات المصارف (IT Governance).

- ورشة تحديث الأنظمة والبنية التحتية (Infrastructure)
- ارتفاع كلفة موازنات أنظمة الحماية المطلوب استمرار تأمينها مع تجدّد تقنيات خرق الأنظمة على اختلاف أنواعها.
- تأمين الخبرات وتعزيز القدرات الداخلية المسؤولة عن أمان تقنيات المعلومات.

واجهت لجنة الرقابة على المصارف في لبنان هذه التحديات من خلال الوسائل التالية:

- إصدار التعاميم التنظيمية والتطبيقية في هذا الشأن.
- تقوم الفرق الميدانية لدى مصرف لبنان بمهام تقييم مدى التزام المصارف بالتعاميم والتوجيهات ذات الصلة، ومن ثمّ يتمّ إرسال كتاب بملاحظات اللجنة على أمن الفضاء الإلكتروني لدى هذه المصارف للقيام بالمعالجات المطلوبة وفق جدول زمني محدّد.
- تشاركّ لجنة الرقابة جمعية المصارف في إعداد دورات شبه فصلية للمصارف تتناول مخاطر تقنيات المعلومات وفق برنامج تدريبي محدّد. وكان لمخاطر العمليات المصرفية عبر الوسائل الإلكترونية الحصّة الكبيرة خلال سنة 2017 و2018.

12. التجارب الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

إنّ أمن الفضاء الإلكتروني يبقى جزءاً من أمن الخدمات الإلكترونية عامةً في المصارف، فكلاهما يستندان على هيكلية المصرف الإدارية واللوجستية والتشغيلية والبشرية والتشريعية بكل ما يتطلّب الأمر من تنظيم لهذه الهيكلية بشكل مناسب خالٍ من الضعف والثغرات، وهي الدعامة الداخلية التي توفّر

للإجراءات التقنية المتخصّصة بتصفيح مداخل المصرف تجاه المخاطر السيبرانية (Cyber Threats) متطلبات الضبط المناسب والفعالية. كما لا شكّ أنّ متطلبات أمن الفضاء الإلكتروني تحتمّ على المصارف وضع استراتيجية تحصين الأمن التي تشمل تخصيص إدارة للأمن المطلوب وجهاز بشري متخصّص بوضع الخطط المناسبة للمخاطر وسياسات وإجراءات الحماية وتحديثها باستمرار.

من أهم الدروس المستفادة في هذا الصدد:

- لا يستقيم وضع القطاع المصرفي ويتحصّن في هذا المجال بدون تشريعات مناسبة تصدر عن السلطات المصرفية الرقابية في هذا الشأن.
- في حين يبقى أمن أنظمة المعلومات التشغيلية والتطبيقية داخل المصارف شأناً داخلياً لديها، فإنّ أمن الفضاء الإلكتروني يتميّز بمتطلبات الشراكة بين جميع المصارف في تحمّل المسؤولية وإرساء آليات الحماية وسبل التصدّي وآليات الإبلاغ وتبادل التجارب فيما بينها. وهذا الأمر يحتّم إنشاء إدارة وطنية أو قطاعية تتولّى وضع معايير الحماية وتنسيق التعاون بين كافة الأطراف والتنبيه حول مخاطر محققة أو محتملة وتزويدها لكافة المصارف حصراً لنطاق انتشارها.

أمّا نجاح الخطط والإجراءات المُتخذة لحماية الفضاء الإلكتروني فتكمن في استكمال التدابير الضامنة التالية:

- إخضاع هذه الخطط والإجراءات لمقاييس جودة التخطيط وجودة التنفيذ (Quality Control & Quality Assurance).

- إخضاع هذه الخطط والإجراءات لاختبارات دورية مستفيضة ومنها اختبارات الضغط بشكل يحاكي الظروف الفعلية إلى أقصى حدٍّ ممكن.

مصر

1. الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

تتضمن التعليمات الرقابية الخاصة بإطار المخاطر التشغيلية (Operational Risks) جزءً متعلقاً بمخاطر نظم المعلومات وأمن الفضاء الإلكتروني في القطاع المصرفي، وتمثل القواعد المنظمة لتقديم الخدمات المصرفية عبر الانترنت، والهاتف المحمول. وتتضمن أيضاً عمليات الرقابة اختبارات توضح مدى قدرة المصارف على مواجهة مخاطر أمن الفضاء الإلكتروني. كما صدر عن البنك المركزي المصري تعليمات وقواعد تنظم تقديم الخدمات المصرفية عبر الإنترنت.

فيما يخص التعليمات الرقابية التي يتم فرضها على عمليات تعهيد أمن نظم المعلومات والأنظمة الإلكترونية للمصرف إلى جهة ثالثة، فإنه يجب إعداد آليه شاملة ومستمرة لإجراء الأبحاث النافية للجهالة (Due Diligence)، والرقابة على عمليات التعهيد، وعلاقات البنك بأطراف خارجية أخرى يتم الاعتماد عليهم لتقديم خدمة الانترنت البنكي، مع تركيز مجلس الإدارة والإدارة العليا على النقاط التالية على سبيل المثال لا الحصر:

- الإلمام الكامل بالمخاطر المترتبة على إبرام أي ترتيبات خاصة بالإسناد أو الشراكة فيما يتعلق بنظم أو تطبيقات خدمات الانترنت البنكي بالإضافة إلى توفير الموارد اللازمة للإشراف على هذه الترتيبات.

- إجراء الأبحاث النافية للجهالة اللازمة فيما يتعلق بالكفاءة والبنية التحتية للنظام والقدرة المالية للشريك أو الطرف الخارجي مُقدم الخدمة وذلك قبل إبرام أي اتفاقيات خاصة بالإسناد أو الشراكة.
- تحديد المسؤوليات التعاقدية لكافة الأطراف الخاصة باتفاقيات الاسناد أو الشراكة بشكل واضح. على سبيل المثال، يتم تحديد مسؤوليات توفير المعلومات إلى مقدم الخدمة وتلقيها منه بشكل واضح.
- تتضمن تعاقدات خدمات الإسناد اتفاقية لعدم الإفصاح عن المعلومات السرية لأطراف خارجية، واتفاقية مستوى الخدمة التي تشمل على سبيل المثال لا الحصر: تحديد الأدوار والمسؤوليات، والوقت المطلوب لتنفيذ الخدمة، وإجراءات وبيانات التصعيد، والعقوبات في حال عدم الالتزام، هذا بالإضافة إلى البنود التي تحفظ حق البنك في التدقيق على موردي الخدمات أو الاعتماد على تقارير التدقيق المعتمدة (الصادرة عن جهات تدقيق معتمدة).
- خضوع كافة النظم والعمليات الخاصة بخدمات الانترنت البنكي التي تتم من خلال عملية الإسناد لنظام إدارة المخاطر وسياسات الخصوصية وأمن المعلومات التي تتفق مع المعايير الخاصة بالبنك.
- إجراء التدقيق الداخلي و/أو الخارجي بصفة دورية على العمليات التي تتم عن طريق الإسناد، وينبغي ألا يقل نطاق تغطية أعمال التدقيق عن مثيلتها التي يتم تطبيقها على المستوى الداخلي في البنك.
- توفير كافة تقارير التدقيق والتقييم لمفتشي قطاع الرقابة والإشراف بالبنك المركزي المصري.
- وضع خطط طوارئ مناسبة لخدمات الانترنت البنكي التي تتم عن طريق الإسناد.

- أن تتسم إجراءات فسخ / انهاء التعاقد بالفاعلية، كما يجب أن تضمن هذه الإجراءات الحفاظ على استمرارية العمل وسلامة البيانات وكذلك نقلها والتخلص منها.
- في حالة إسناد خدمات الانترنت البنكي لجهات خارج جمهورية مصر العربية، يجب على البنوك اتخاذ التدابير اللازمة للامتثال للقوانين والتشريعات المصرية واختصاص المحاكم المصرية بما قد ينشأ من منازعات.

تجدر الإشارة إلى أنه سيتم إصدار قواعد تفصيلية مُنظمة تحكم أنشطة الإسناد وذلك على نحو منفصل، على أن تشمل الضوابط الرقابية التفصيلية إضافة إلى الأهداف الرقابية وكذلك قائمة بالنظم والخدمات المسموح بإسنادها والاستعانة بمصادر خارجية لتنفيذها. ولحين إصدار هذه القواعد، يجب على البنك عدم إبرام أي اتفاقيات تتعلق بإسناد خدمات الإنترنت البنكي أو تطبيقاتها دون الحصول على موافقة مسبقة من البنك المركزي المصري. ذلك بالإضافة الى التعليمات الخاصة بالرقابة الداخلية في البنوك الصادرة في عام 2014.

كما أن هناك توجيهات رقابية تُلزم المصارف بتضمين استراتيجيات المخاطر المُقرة من قبل مجالس إدارات البنوك إطاراً يتعلق بالمخاطر الإلكترونية ومخاطر نظم المعلومات والهجمات الإلكترونية (Cyber-attacks)، يتم التحقق من وجود تلك الاستراتيجيات من خلال عمليات الرقابة المصرفية، بحيث تكون متضمنة مستوى المخاطر المتعلقة بأمن الفضاء الإلكتروني وإجراءات موازية لدعم مستويات أمن الفضاء الإلكتروني (cyber resilience) بما يشمل وجود سياسة واضحة لحوكمة إدارة مخاطر أمن

الفضاء الإلكتروني. كذا تلزم السلطات الرقابية البنوك بتعيين مسؤول عن أمن المعلومات [Chief Information Security Officer (CISO)].

2. الضوابط والتعليمات الخاصة بتنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الإنترنت

لا يسمح للعملاء بإنشاء أو فتح حساب مصرفي من خلال موقع البنك على شبكة الانترنت، ذلك لأنه وفقاً للتعليمات الصادرة عن البنك المركزي فان البنوك تلتزم بعدم السماح للعملاء الجدد (ممن لا يمتلكون حساب مصرفي وليس حساب خدمات الانترنت البنكي) بفتح حساب مصرفي باستخدام أي من قنوات تقديم الخدمات الالكترونية. ويجب أن تطبق البنوك قواعد التعرف على هوية العملاء بالبنوك الصادرة عن وحدة مكافحة غسل الأموال وتمويل الإرهاب الصادرة بعام 2011 على هؤلاء العملاء الجدد.

أما بالنسبة للعملاء الراغبين في الاستفادة من الخدمات المصرفية من خلال شبكة الانترنت، تحصل البنوك على توقيع يدوي من العميل الذي يرغب في الاشتراك بخدمات الانترنت البنكي على نموذج (نماذج) طلب الخدمة أو العقد (العقود) التي تحتوي على البيانات الأساسية للعميل كحد أدنى (مثال: البريد الالكتروني، رقم الهاتف المحمول، والأرضي، عنوان المراسلات، إلخ..)، بالإضافة إلى الشروط والاحكام التي تحدد الحقوق والالتزامات بين البنوك والعملاء بشكل واضح. فوفقاً لعقد تقديم الخدمة فانه يجب على البنوك ان تحدد بدقة كافة الحقوق والالتزامات بينها وبين عملائها ضمن عقد تقديم خدمات الانترنت البنكي، كما يجب استيفاء العقد للمتطلبات التالية:

- تتم صياغة العقد بصورة واضحة ومحددة بحيث يسهل فهمه بالنسبة لأي عميل مع تجنب استخدام الكلمات والعبارات التي تحمل أكثر من معنى.
- توضيح التزامات كل من البنك والعميل في حالة الإخلال بأي من شروط العقد.
- يحتوي العقد على بنود محددة واضحة والتي من الممكن أن تتضمن ما يلي كحد أدنى:
- التأكيد على أوقات توفير الخدمة طبقا لتقييم البنك لهدف وقت الاسترجاع (RTO) الوارد في خطة استمرارية الأعمال، وينبغي إخطار العملاء في حالة انقطاع الخدمة لعمل صيانة محددة مسبقاً.
- توضيح مستوى خصوصية بيانات العملاء ومدى اتاحتها للغير داخل البنك أو خارج البنك بما يتوافق مع التعليمات الرقابية الصادرة عن البنك المركزي المصري أو القوانين المنظمة لذلك.
- توضيح الآلية والخطوات المتبعة والوقت المتوقع للبت في شكاوى أو نزاعات العملاء.
- توضيح بشكل مفصل للخطوات الواجب على العميل اتباعها لتفعيل الخدمة في حالة الاشتراك لأول مرة أو في حالة وقف الخدمة أو إعادة تشغيلها.
- التأكيد على التزام العميل بقراءة التحذيرات والاخطارات التنبيهية مثل التنبيهات الأمنية أو تنبيهات محاولات الاحتيال والهندسة الاجتماعية (Social Engineering)، والتأكيد على أن قبول العميل من خلال الانترنت البنكي لأي تغيير في الشروط والاحكام الذي سيظهر من خلال النظام إلكترونياً يعتبر التزاماً قانونياً.

- التأكيد بوضوح على أن القوانين المصرية ذات الصلة ولوائحها التنفيذية والتعليمات والقواعد الرقابية هي التي تحكم الخدمات التي يقوم البنك بتقديمها للعملاء عبر شبكة الانترنت.
- في حالة اعتماد البنك على التوقيع الإلكتروني كوسيلة مصادقة ووجود اتفاق مع العميل كتابة على استخدام هذه الوسيلة، فإن خدمة الإنترنت البنكي في هذه الحالة تخضع لأحكام القانون رقم (5) لسنة 2004 ولائحته التنفيذية والقرارات المنفذة له.

بهدف التحقق من هوية وصلاحية العميل الراغب في الاستفادة من الخدمات المصرفية، تلتزم البنوك باستخدام أساليب يمكن الاعتماد عليها للتحقق من هوية وصلاحيات العملاء الراغبين في الاشتراك في خدمات الإنترنت البنكي، وكذلك التحقق من هوية وصلاحيات العملاء المشتركين بالخدمة الراغبين في تنفيذ أنشطة مصرفية عبر خدمات الإنترنت البنكي.

فيما يخص التحقق من هوية وصلاحية المخولين بالاستفادة من الخدمات المصرفية، تلتزم البنوك بتطبيق كافة الإجراءات والضوابط الرقابية التي تمكنها من تحديد هوية القائمين بأي معاملات إلكترونية مرتبطة بالحسابات المصرفية، ذلك في الحالات التي يصرح فيها لأكثر من مستخدم بالتعامل على هذا الحساب. كما تلتزم البنوك بالحصول على كافة المستندات القانونية اللازمة لإثبات تفويض الصلاحيات للمستخدمين بإجراء معاملات على حسابات الأشخاص الاعتبارية. إضافة الى ذلك تلتزم البنوك بالحصول على كافة المستندات القانونية اللازمة لإثبات تفويض الصلاحيات للمستخدمين بإجراء معاملات على حسابات الأشخاص الاعتبارية.

تلتزم أيضا البنوك بإجراء عمليات التدقيق اللازمة للتأكد من هوية العميل عند طلبه اجراء تعديل في بيانات حساب خدمات الانترنت البنكي الخاص به، أو تعديل أي بيانات يستخدمها العميل لمتابعة أنشطة حساباته المصرفية. يطبق ذلك على عمليات إعادة تفعيل الحساب وإعادة اصدار كلمة سر جديدة لعميل خدمات الانترنت البنكي وتغيير بيانات الاتصال الخاصة بالعميل مثل عنوان البريد الالكتروني، ورقم الهاتف المحمول والأرضي، وعنوان المراسلات.

3. الضوابط والتعليمات الخاصة بتنظيم وسائل إثبات الهوية عبر الإنترنت

تلتزم البنوك باستخدام وسائل فعالة يمكن الاعتماد عليها للتحقق من هوية العملاء المستخدمين لخدمات الانترنت البنكي، وعادة ما تكون عملية التصديق أكثر فعالية عند الجمع بين اثنين من العناصر التالية:

- أحد الأشياء المعروفة للعميل (مثال اسم المستخدم وكلمة السر).
- أحد الأشياء التي بحوزة العميل (مثال التوقيع الرقمي، أو كلمات السر المستخدمة لمرة واحدة التي تصدر باستخدام أجهزة رموز الأمان).
- أحد السمات المميزة والخاصة بالعميل (مثال الصفقات البيومترية).

يجب على البنوك إعادة التصديق باستخدام وسيلتين معاً (مثال: التوقيع الرقمي، أو كلمات السر المستخدمة لمرة واحدة التي تصدر باستخدام أجهزة رموز الأمان مع عدم السماح بمنح كلمات السر المستخدمة بشكل آلي ومباشر عبر الرسائل النصية القصيرة أو البريد الالكتروني للعملاء من الأفراد والأشخاص الاعتبارية، الخ) عند تنفيذ الأنشطة ذات المخاطر المرتفعة (مثل تحويل الأموال لأطراف خارجية، تسجيل مستفيدين جدد، تغيير بيانات الاتصال بالعميل، الخ)، ويجب ان تعمل وسيلة التصديق المستخدمة بالتزامن مع الضوابط الأخرى المطبقة على تعزيز الابعاد التالية:

- عدم الإنكار.

- سلامة وتكامل البيانات.
- سرية البيانات.
- صحة الهوية.

يجب على البنوك تحديد وسائل التصديق التي ستستخدمها لخدمات الإنترنت البنكي وذلك بناء على تحليل المخاطر المرتبطة بالنظام، مع الأخذ في الاعتبار تقييم نوعية المعاملات المصرفية التي تقدم عبر الإنترنت البنكي.
تحتاج البنوك إلى التقييم الدقيق لتحديد ما إذا كانت الوسيلة المستخدمة للتصديق مناسبة من الناحية الأمنية حتى إذا كان الحاسب الشخصي بالعميل عرضه للتهديدات، مثال: عن طريق برامج خبيثة مثل حصان طروادة وبرامج التجسس عن طريق تسجيل الضغط على أوجه المفاتيح.

يجب على البنوك استخدام التكنولوجيا المناسبة لإنشاء كلمات السر إضافة إلى تطبيق الوسائل اللازمة للحفاظ على سرية كلمات السر في حال تسليمها للعميل.

يجب أيضاً على البنوك تطبيق الوسائل المناسبة التي تُمكن العملاء من التحقق من هوية ومصداقية المواقع الإلكترونية الخاصة بهذه البنوك وذلك بخلاف معايير التصديق الخاصة بهوية العملاء، ذلك عن طريق تثبيت شهادات التصديق الرقمية (Digital Certificates) والمفاتيح المرتبطة بها من الجهات المعروفة والموثوق بها على خوادم نظام الإنترنت البنكي، كما يوصى باستخدام شهادات التصديق التي تتضمن تحقق/ تأكيد إضافي.

إضافة إلى ذلك يجب على البنوك إنشاء آلية للتحقق من التصديق على النحو التالي:

- إخطار العميل بمجرد دخوله على النظام بالمحاولات السابقة الناجحة و/أو الفاشلة الخاصة باسم المستخدم الخاص بالعميل وذلك فور دخول العميل على النظام.
- منع دخول المستخدم على خدمات الإنترنت البنكي بعد عدد محدد من المحاولات الفاشلة – لا يتعدى خمس محاولات – ويجب على البنك إعداد إجراءات واضحة لإعادة تفعيل حساب المستخدم الذي تم إيقافه.
- منع المستخدم من استخدام أكثر من نافذة للنظام بشكل متزامن.
- عدم إعطاء أي معلومات بعد المحاولات الفاشلة للدخول على النظام إلى الشخص الذي قام بتلك المحاولات مثل الإفصاح عن عدم وجود اسم هذا المستخدم أو إن كلمة السر غير صحيحة.
- القيام بالرقابة بصورة منتظمة لمحاولات الدخول الناجحة و/أو الفاشلة لخدمات الإنترنت البنكي، وعند اكتشاف أي تجاوز جسيم يجب التحقيق فيه وتحديد التهديدات المحتملة واتخاذ التدابير اللازمة.

فيما يتعلق بتقييم الوسائل التي تعتمد عليها البنوك في التحقق من هوية العميل بحيث تكون مناسبة من الناحية الأمنية وغير عُرضه للقرصنة أو للتهديد عن طريق البرامج الخبيثة وبرامج التجسس، فقد أصدر البنك المركزي التعليمات التالية:

- يجب على البنوك دورياً تقييم الوضع الأمني لكافة الأنظمة (التطبيقات، الشبكات، أجهزة التأمين، خوادم نظام أسماء النطاقات، وخوادم البريد الالكتروني، الخ) المتعلقة بأعمال الإنترنت البنكي، ذلك في المركز الرئيس للمعلومات والمركز الاحتياطي الذي يستخدم في حالات الكوارث.

- يجب على البنوك إجراء تقييم دوري لنقاط الضعف كل ثلاثة أشهر على الأقل أو عند حدوث تغيير جوهري في البيئة التشغيلية لنظام خدمات الإنترنت البنكي لاكتشاف نقاط الضعف في بيئة تقنيات المعلومات، وتقييمها، ويمكن أن يتولى هذا التقييم مستشار أو مقدم خدمة خارجي، أو إدارة أمن المعلومات بالبنك، ذلك بحيث يجب أن يحتوي نطاق تقييم نقاط الضعف على اختبار الثغرات الشائعة في الشبكة (مثل الثغرات التي تُمكن المخترق من حقن قواعد البيانات (SQL Injection) وثغرات البرمجة عبر المواقع Cross-Site (Scripting). كما يجب على البنك إعداد خطة لمعالجة المشاكل التي تظهر في تقييم نقاط الضعف، ثم التحقق من صحة هذه المعالجة عن طريق إعداد الاختبار لإثبات إنه قد تم التعامل مع هذه المشاكل بالكامل.
- يجب على البنك القيام باختبارات الاختراق وذلك لعمل تقييم مفصل ومُعمق للوضع الأمني للنظام من خلال محاكاة للهجمات الفعلية على النظام على أن يتم ذلك على الأقل مرة واحدة سنوياً، أو قبل البدء في تقييم أي خدمات حيوية جديدة، على أن تتم مراعاة إنه يجب أن يتولى إجراء اختبار الاختراق أحد مقدمي الخدمة الخارجين المستقلين حيث يجب عليه أولاً التوقيع على اتفاقية السرية وعدم الإفصاح قبل مزاولة العمل. ويجب أيضاً أن يكون لدى البنوك تقرير مبدئي عن اختبار الاختراق وخطة المعالجة التي تم إصدارها والموقعة من مقدم الخدمة الخارجي. إضافة إلى ذلك، يجب على البنوك التحقق من صحة معالجة الملاحظات الناتجة عن اختبار الاختراق سواء كان على الأنظمة الرئيسة أو الأنظمة البديلة المستخدمة لمواجهة الكوارث.

كما تتمثل الآلية التي تعتمد عليها البنوك في التحقق من تصديق العميل الكترونياً من خلال الإنترنت، في إخطار العميل بمجرد دخوله على النظام بالمحاولات السابقة الناجحة و/أو الفاشلة الخاصة باسم المستخدم الخاص بالعميل وذلك فور دخول العميل على النظام. ويتم التحكم في عدد مرات المحاولات الفاشلة للدخول إلى الحساب من خلال الانترنت من خلال منع دخول المستخدم إلى خدمات الإنترنت البنكي بعد عدد محدد من المحاولات الفاشلة (لا يتعدى خمس محاولات) ويجب على البنك إعداد اجراءات واضحة لإعادة تفعيل حساب المستخدم الذي تم إيقافه.

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

أشارت التعليمات والتدابير الرقابية الصادرة عن البنك المركزي المصري والخاصة بإدارة كلمة السر (Password) ومواصفاتها، بإنه يجب على البنوك مراعاة التدابير الرقابية التالية عند التعامل مع كلمة السر الخاصة بالعملاء:

- تطبيق الرقابة المزدوجة و/أو الفصل بين المهام لعملية إنشاء كلمات السر وتسليمها للعملاء وعملية تفعيل حسابات خدمات الإنترنت البنكي.
- تعزيز تأمين عملية انشاء كلمة السر لضمان عدم تعرضها للكشف.
- التأكد من أن كلمات السر لا يتم معالجتها أو إرسالها أو تخزينها كنص واضح.
- وجوب توجيه مستخدمي ومديري أنظمة الإنترنت البنكي لتغيير كلمة السر الصادرة فور الدخول إلى النظام لأول مرة.
- تطبيق قواعد انتهاء الصلاحية لكلمة السر على أساس مدة صلاحية محددة مسبقة من قبل البنك.

- الحفاظ على تاريخ كلمات السر المستخدمة والتأكد من عدم اعادة استخدامها مرة أخرى خلال عدة مرات أو مدة زمنية يحددها البنك.
- فرض استخدام كلمات سر معقدة (مثال: تتكون من ثمانية أحرف وتتضمن حروف وأرقام ورموز خاصة).
- يجب تشفير كلمة السر باستخدام آلية تشفير قوية أو أن يكون طول مفتاح التشفير مناسب (لا يقل عن 1024 بايت).
- استخدام التكنولوجيا المناسبة لإنشاء كلمة السر واعتماد التقنيات المناسبة للحفاظ على تأمينها اثناء التسليم للعميل إما باليد أو إلكترونياً.
- التأكد من أن آلية تذكر كلمة السر لا يمكن استخدامها (أي لا يتم السماح بتخزين كلمة السر في صورة كود تطبيق خاص بالموقع او في ملفات تعريف الارتباط بكلمة السر).

أما بالنسبة للتعليمات والمواصفات الخاصة بكلمة السر التي تستخدم لمرة واحدة والصادرة باستخدام أجهزة رموز الأمان (OTP)، فقد حددتها السلطات الرقابية على الوجه التالي:

- الحد الأدنى لمواصفات كلمة السر لمرة واحدة:
  - يجب ألا تكون كلمة السر أقل من 6 رموز.
  - يجب ألا تزيد الوقت الزمني لصلاحية استخدام كلمة السر عن 90 ثانية.
  - التأكد من أن نظام الحلول الحسابية Algorithm لإنشاء كلمة السر يوفر العشوائية الكافية من القيم الرمزية.
- يجب أن يتم حماية رموز الأمان برقم سري طبقاً لما يلي:
  - يجب ألا يقل الرقم السري لجهاز رموز الأمان عن 4 أرقام.

- لا ينبغي السماح بالأرقام السهلة كرقم سري PIN مثال: 1111 أو 1234.
- يجب أن يكون هناك حد أقصى للمحاولات غير الناجحة لإدخال الرقم السري – لا تتجاوز خمس محاولات – قبل إيقاف جهاز رموز الأمان.
- يجب على البنوك إعداد إجراءات واضحة لإعداد الأرقام السرية الأولية وإعادة تفعيل أجهزة رموز الأمان الموقوفة.
- يجب توجيه العميل لتغيير الرقم السري عند أول استخدام وذلك في حالة إصدارة عن طريق البنك.

5. الضوابط والتعليمات الرقابية الخاصة بعمليات تحويل الأموال من خلال خدمات الانترنت

تتمثل الضوابط والتعليمات الصادرة عن البنك المركزي المصري في هذا الشأن فيما يلي:

- يجب على البنوك التي تقدم خدمة تحويل الأموال من حسابات عملائها إلى حسابات أطراف أخرى من خلال خدمات الإنترنت البنكي وضع الضوابط المناسبة التي تساعد على تقليل المخاطر المصاحبة لتلك الخدمة لتصل الى مستوى مقبول ومعتمد من البنك.
- يجوز للبنوك استخدام وسيلة تصديق أحادية للتصديق على عمليات تحويل الأموال بين الحسابات التابعة لنفس العميل، التي تتم داخل نفس البنك بجمهورية مصر العربية، أو سداد التزامات العميل

الخاصة ببطاقات الائتمان أو القروض أو إنشاء شهادة إيداع أو حساب وديعة لأجل داخل نفس البنك بجمهورية مصر العربية.

- يجب على البنوك تطبيق مبدأ الرقابة المزدوجة على الأقل (المُعد / المُدقق والمصرح) على تحويلات أموال الأشخاص الاعتبارية لمستفيدين آخرين – إلا في حالة طلب الشركة أو الشخص الاعتباري غير ذلك كتابياً مع ضرورة استخدام كل من المُعد / المدقق والمصرح لوسائل إثبات الهوية (التصديق).
- يجب على البنوك وضع حد أقصى يومي أو حدود للمعاملات التي تتم من خلال خدمات الانترنت البنكي لتحويل الأموال من حسابات عملائها لمستفيدين أخرين على أن تخضع لدراسة المخاطر من قبل البنك، ويجب ألا تتعارض تلك الحدود مع أي حدود أخرى يحددها البنك المركزي المصري.
- يحظر معالجة بعض الوظائف / الخدمات باستخدام نظام التنفيذ الآلي المباشر للعمليات، حيث يجب تنفيذها بعد أن يتحقق موظفي المكتب الخلفي بالبنك Back Office من صحة الطلب أو المعاملة، وفيما يلي الخدمات المحظور تنفيذها آلياً:
  - تحويل الأموال لمستفيدين خارج جمهورية مصر العربية (بالتوافق مع أي لوائح أو تعليمات صادرة عن البنك المركزي المصري بخصوص تحويل الأموال بالعملة الاجنبية).
  - الطلبات المتعلقة بالعمليات الائتمانية (القروض، التسهيلات الائتمانية، طلبات بطاقات الائتمان، الخ)، حيث يمكن تقديمها

عبر الإنترنت ولكن يجب على البنوك الحصول على توقيع من العميل قبل تنفيذ العملية أو الطلب.

- يجب على البنوك إخطار عملائها من مستخدمي خدمة الإنترنت البنكي بأية معاملات مالية وأنشطة ذات مخاطر مرتفعة تتم على حساباتهم إلا في حالة طلب العميل غير ذلك – ذلك من خلال وسيلة مميكنة بديلة (مثل الرسائل النصية القصيرة او رسائل البريد الإلكتروني).
- يتم التعامل مع خدمة سداد الفواتير عبر خدمات الإنترنت البنكي خصماً على حساب العميل على أنها عملية تحويل أموال لمستفيدين أخرين، حتى وإن تم تحويلها عن طريق المكتب الخلفي Back Office.
- يتعين على البنوك الوفاء بالتزاماتها الخاصة بتحويلات الأموال وفقاً لما ورد بالجزء التاسع الخاص بالقواعد الخاصة بتحويل الأموال وذلك ضمن قواعد التعرف على هوية العميل بالبنوك الصادرة عن وحدة مكافحة غسيل الاموال وتمويل الارهاب لسنة 2011.

6. الضوابط والتعليمات الرقابية الخاصة بسرية وسلامة المعلومات

أصدر البنك المركزي المصري الضوابط والتعليمات التالية والخاصة بسرية وسلامة المعلومات:

- يتضمن تقديم خدمات الإنترنت البنكي تداول بيانات سرية (مثل كلمات السر الخاصة بخدمات الإنترنت البنكي والمعاملات المالية) عبر شبكة الإنترنت والشبكة الداخلية للبنك. لذلك يجب على البنوك

استخدام الأساليب المناسبة للحفاظ على سرية وسلامة المعلومات المتداولة عبر الشبكات الداخلية والخارجية للبنك.

- يتم استخدام تكنولوجيا التشفير لحماية سرية وسلامة المعلومات التي تتسم بالحساسية. حيث يجب على البنوك اختيار تكنولوجيا التشفير التي تتناسب مع حساسية وأهمية المعلومات وكذا درجة الحماية المطلوبة، وفي هذا السياق يوصى دائما بتبني البنوك لتكنولوجيا التشفير التي تستخدم طرق التشفير المتعارف عليها دولياً، حيث تخضع نقاط القوة في هذه الطرق لاختبارات شاملة. وينبغي أن تطبق البنوك الممارسات السليمة لإدارة مفاتيح التشفير اللازمة لحماية هذه المفاتيح.
- يجب على البنوك أيضا تنفيذ ضوابط أخرى بخلاف أساليب التشفير، ذلك للحفاظ على سرية وسلامة المعلومات التي يتم تداولها عبر نظم خدمات الإنترنت البنكي ويتضمن هذا على سبيل المثال:
  - الضوابط وأعمال التدقيق المدرجة بتطبيقات الإنترنت البنكي للتأكد من سلامة تسوية أرصدة العملاء بعد تنفيذ المعاملات بالإضافة إلى التأكد من سلامة البيانات التي يتم نقلها بين الأنظمة المختلفة.
  - مراقبة المعاملات غير المعتادة بما في ذلك المعاملات محل الاشتباه الخاصة بخدمات الانترنت البنكي أو السجلات التي يشتبه التلاعب فيها.
- ينبغي على البنك تطبيق سياسة الفصل بين المهام، وذلك للتأكد من عدم إمكانية قيام أي موظف داخل البنك بأي عمل غير مصرح له

وإخفائه، ويتضمن هذا على سبيل المثال لا الحصر، إدارة حساب المستخدم وتنفيذ المعاملات كما يلي:

- عدم السماح لموظف واحد فقط بالقيام بإنشاء حساب مستخدم لخدمات الإنترنت البنكي والتصريح بالموافقة عليه وإلغائه دون مشاركة موظفي الإدارات الأخرى بالبنك للتحقق من سلامة تصرفات هذا الموظف.
- يجب على البنك تصميم الإجراءات الخاصة بتعاملات الإنترنت البنكي بما يضمن عدم انفراد أحد الأشخاص بإنشاء التعاملات والموافقة عليها وتنفيذها على النظام مما قد يدعم عملية احتيال او إخفاء تفاصيل خاصة بتلك المعاملات.

7. الضوابط والتعليمات الرقابية الخاصة بتأمين التطبيقات الإلكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الانترنت

تشير التعليمات الصادرة من السلطات الرقابية في هذا الشأن، إنه يجب على البنوك التأكد من توفير مستوى مناسب من تأمين التطبيقات الخاصة بخدمات الانترنت البنكي مع أخذ الممارسات السليمة التالية بعين الاعتبار:

- يجب على البنوك عند اختيار أدوات تطوير النظام أو لغات البرمجة من أجل تطوير التطبيقات الخاصة بخدمات الإنترنت البنكي أن تُقيم الخصائص الأمنية التي يُمكن أن توفرها الأدوات أو اللغات المختلفة لضمان إمكانية تنفيذ الحماية الفعالة للتطبيقات.
- يجب إجراء عملية تحقق شاملة وفعالة حول صحة المُدخلات (بما في ذلك البيانات المُدخلة من قبل المستخدم والاستعلام من خلال

قواعد البيانات التي قد يقوم المستخدم بطلب تنفيذها) وذلك من خلال خوادم الشبكة، ويمنع هذا نظام الإنترنت البنكي من معالجة المعطيات غير الصحيحة التي يتم إدخالها بطريقة متعمدة، الأمر الذي قد يؤدي إلى الوصول غير المصرح به إلى البيانات، أو تنفيذ الأوامر الواردة في هذه المعطيات، أو حدوث هجمات تؤدي إلى تجاوز سعة الذاكرة.

- يجب أن تعمل أنظمة خدمات الإنترنت البنكي بأقل الصلاحيات الممكنة الخاصة بإدارة النظام، كذلك يجب منع استخدام كلمات السر المعروفة أو كلمات السر الموحدة التي تعد مع نشأة النظام.
- يجب ألا تكشف رسائل الأخطاء التي تصدر من النظام لعملاء خدمات الإنترنت البنكي عن معلومات دقيقة خاصة بالنظام. ويجب تسجيل الأخطاء بشكل مناسب، كما يجب التأكد من عدم احتواء النص المصدري للغة توصيف النصوص المترابطة HTML في خادم الشبكة الخاص بالنظام Production Web Server على أي من المعلومات الدقيقة الخاصة بالنظام مثل أي إشارات أو مرجعيات متعلقة بخصائص تصميم كود البرامج / التطبيقات Web Application Code.
- يجب إنهاء نافذة المعاملة عبر الإنترنت تلقائيا Session Termination بعد فترة محددة من الوقت في حال عدم وجود أي نشاط على النظام، لإلا إذا تم إعادة تصديق بيانات العميل مرة أخرى، الأمر الذي يمنع أي مخترق من الإبقاء على أي نافذة مفتوحة على الإنترنت إلى أجل غير محدد.

- يجب منع برامج التصفح الخاصة بالعميل من حفظ أو عرض اسم المستخدم أو كلمات السر السابق إدخالها من العملاء المستخدمين لخدمات إلانترنت البنكي وكذلك صفحات الويب الخاصة بتلك الخدمات التي سبق الدخول عليها.
- يجب على البنوك اتخاذ إلاجراءات اللازمة لعلاج أي نقاط ضعف بنظام الإنترنت البنكي يتم اكتشافها، وذلك استناداً إلى الاجراءات الامنية المتبعة في البنك.
- يجب حماية المسارات المخفية الخاصة بالموقع الإلكتروني والتي تحتوي على أي صفحات إدارية أو معلومات سرية، وذلك عن طريق تطبيق نظام تصديق فعال وآليات معيارية للتحكم في الدخول على كافة النظم الخاصة بخدمات الإنترنت البنكي.
- يجب مسح كافة الملفات الإحتياطية والمشتركة من خوادم شبكة الاصدار أو هيكل مسارات الملفات لتجنب وصول المستخدمين غير المصرح لهم بذلك.
- القيام بمراجعة أمنية دورية لهيكل مسارات الملفات وصلاحيات النفاذ إلى الملفات، وذلك لضمان أن الملفات السرية يتم حمايتها بشكل ملائم، ولا يتم عرضها من خلال تطبيقات الويب.
- يجب على البنوك عمل الترتيبات الأمنية المناسبة لبعض الخدمات التي تتضمن اتصالات مع الشبكات العامة (كخدمات البريد الإلكتروني للتواصل مع عملاء خدمة الإنترنت البنكي، ونظام أسماء النطاقات DNS لترجمة أسماء المواقع إلى عناوين على الشبكة والعكس) لتجنب الهجمات على أنظمة خدمات الانترنت البنكي.

- يمكن للبنك – بجانب استخدام بروتوكول طبقة المنافذ الأمنة SSL – أن يقوم بتأمين عملية تشفير شاملة على مستوى (طبقة) التطبيقات للبيانات المرسلة عبر الإنترنت، حتى لا يتم كسف الأرقام السرية وكلمات السر الخاصة بالعميل في أي مرحلة وسيطة لتداول البيانات بين المتصفح وخادم الاستضافة Host حتى يتم التحقق من أرقام التعريف الشخصية وكلمات السر.
- يجب على البنوك القيام بالاختبارات اللازمة للتأكد من عدم إمكانية تجاوز عملية التصديق او إغفالها للدخول إلى النظام.
- نظراً لسهولة الوصول إلى قواعد البيانات ذات الحماية الضعيفة من خلال الشبكات الداخلية والخارجية، لذا يجب التشديد على توافر الآتي:
  - إجراءات صارمة بشأن تحديد الهوية والصلاحيات للدخول على الأنظمة وقواعد البيانات.
  - تصميم آمن وسليم لعميات النظام System Processes.
  - مسارات تدقيق ملائمة Audit Trails.

8. تقييم السلطات الرقابية للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني والوضع الراهن

تفرض السلطة الرقابية على المصارف القيام باختبارات الضغط (Stress Testing) وذلك بصفة دورية سنوية لتحديد حجم الآثار المترتبة على نجاح أية عمليات قرصنة تتعرض لها الأنظمة الإلكترونية. كما يلزم البنك المركزي المصري البنوك بالإبلاغ عن تعرضها لأية عمليات قرصنة إلكترونية (Cyber-event reporting)، وذلك في غضون يوم أو يومين من التعرض

لعملية القرصنة. حيث يتولى مسؤول الإلتزام بالبنك مسؤولية التأكد من إبلاغ البنك المركزي المصري بصورة صحيحة وفي الوقت المناسب، بكافة الحالات التالية:

- أي هجمات احتيال لتسريب أو إفشاء هوية العميل أو وثائق اعتماد الشخصية (كالاحتيال Phishing، وملفات التجسس (حصان طروادة Trojans)، والبرمجيات الخبيثة Malware).
- الدخول غير المصرح به إلى أنظمة تكنولوجيا المعلومات بالبنك لتسريب بيانات العميل المتعلقة بخدمات الإنترنت البنكي.
- أي عملية تخريبية للبيانات المتعلقة بأنظمة خدمات الانترنت البنكي والتي لا يمكن استرجاعها.
- الإيقاف التام المتعمد أو العارض لخدمات الانترنت البنكي لفترة تزيد عن الفترة المحددة كهدف لوقت الاسترجاع RTO المحدد من قبل البنك.
- أي حالة من حالات الاحتيال الداخلي ذات الصلة بخدمات الانترنت البنكي.

9. التعاون والتنسيق مع السلطات الرقابية الأخرى عبر الحدود والشركاء في صناعة تقنية المعلومات فيما يتعلق بالمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

يتم التعاون والتنسيق مع الجهات الرقابية الأخرى المحلية فيما يتعلق بدعم أمن الفضاء الإلكتروني، حيث يتم التعاون بين المركز القومي لطوارئ الإنترنت ومركز الاستجابة لطوارئ الإنترنت للقطاع المصرفي.

10.بناء القدرات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

في هذا الإطار تم عمل مبادرة تدريبية لعدد مائة متخصص في مجال تأمين المعلومات للحصول على الشهادات العالمية في هذا المجال للقطاع المصرفي وذلك في خلال عامين – تتضمن المسارات العالمية لتأمين المعلومات.

11.التحديات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

تتمثل أهم التحديات التي واجهت السلطات الرقابية في هذا المجال، في عدم وجود تكامل أو مركز للاستجابة لطوارئ الحاسب الآلي الخاص بالقطاع المصرفي، إضافة إلى ندرة خبراء تأمين المعلومات المتخصصين في القطاع المصرفي. تم التعامل مع هذه التحديات من خلال إنشاء مركز الاستجابة لطوارئ الحاسب الآلى للقطاع المصرفي، كما تم عمل مبادرة تدريب مائة متخصص في مجال تأمين المعلومات.

المغرب

1. الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

تتضمن التعليمات الرقابية الخاصة بإطار المخاطر التشغيلية (Operational Risks) جزءً متعلقاً بمخاطر نظم المعلومات وأمن الفضاء الإلكتروني في القطاع المصرفي، مثل التعليمات الخاصة بالمراقبة الداخلية لمؤسسات الائتمان، ولجنة الفحص وتدبير المخاطر. إضافة الى التعليمات الخاصة بشروط وكيفية إعداد وتقديم المخطط المسمى "مخطط تسوية الأزمات الداخلية" من طرف مؤسسات الائتمان، وتلك المتعلقة بمنظومة تدبير مخاطر التشغيل وبمخطط استمرارية النشاط داخل مؤسسات الائتمان، وكذا التعليمات

التي تحدد القواعد الدنيا الواجب على مؤسسات الائتمان مراعاتها لإجراء اختبارات اختراق أنظمة المعلومات.

كما تقوم السلطات الرقابية المغربية، بصفة دورية سنوية، بتضمين عمليات الرقابة على أساس المخاطر (ongoing risk-based supervisory activities) لاختبارات توضح مدى قدرة المصارف على مواجهة مخاطر أمن الفضاء الإلكتروني (تجارب محاكاة لهجمات افتراضية). إضافة الى ذلك أصدرت السلطات الرقابية تعليمات خلال عام 2017 متعلقة بواجب اليقظة من طرف مؤسسات الائتمان عند تقديم الخدمات المصرفية من خلال الانترنت والتي تشمل عملية فتح الحساب وحماية الدفع ببطاقة الائتمان عبر الانترنت من خلال تطبيق(3D secure).

فيما يخص التعليمات الرقابية التي يتم فرضها على عمليات تعهيد أمن نظم المعلومات والأنظمة الإلكترونية للمصرف إلى جهة ثالثة (Third Party)، نصت التعليمات الصادرة في هذا الشأن خلال عام 2014 (والمتعلق بالمراقبة الداخلية لمؤسسات الائتمان) على الشروط والضوابط الواجب احترامها عند إسناد أنشطة مؤسسات الائتمان لجهة خارجية بما في ذلك أمن نظم المعلومات والأنظمة الإلكترونية حيث يجب:

- وضع سياسة مقننة لتقييم ومراقبة المخاطر المرتبطة بالتعاقد مع متعهدين خارجيين والعلاقات معهم.
- تدبير الأنشطة المسندة إلى متعهدين خارجيين في إطار عقود مكتوبة تحدد بوضوح جميع الجوانب المادية لاتفاقية الإسناد الخارجي للأنشطة، لاسيما الحقوق والواجبات لكل الأطراف.

- التأكد من كون جميع اتفاقيات الإسناد الخارجي للأنشطة لا تُقلص من قدرة المؤسسة على الوفاء بالتزاماتها تجاه عملائها وتجاه بنك المغرب.
- تقييم مدى توفر المتعهد الخارجي على مخططات استعجالية تتناسب مع متطلباتها الذاتية فيما يخص استمرارية النشاط. ويجب أن يرتكز هذا التقييم على دراسة ملائمة لهذه المخططات وأن يأخذ بعين الاعتبار وتيرة الاختبارات المطبقة وطرقها بالإضافة إلى النتائج المترتبة عنها بالنسبة للمخططات الاستعجالية للمؤسسة.
- ضرورة إخبار المؤسسة من طرف المتعهد الخارجي بشأن أي حدث قد يكون له أثر كبير على قدرته على ممارسة المهام المسندة إليه بطريقة فعالة ومطابقة للقانون المعمول به وللمتطلبات التنظيمية.
- اتخاذ التدابير الملائمة لإلزام متعهد الخدمات بحماية المعلومات السرية للمؤسسة ولعملائها من إفشائها إلى الأشخاص غير المرخص لهم.

تجدر الإشارة الى أن هناك توجيهات رقابية تلزم المصارف بتضمين استراتيجيات المخاطر المُقرة من قبل مجالس إدارات البنوك إطاراً يتعلق بالمخاطر الإلكترونية ومخاطر نظم المعلومات والهجمات الإلكترونية، ويتم من خلال عمليات الرقابة المصرفية التحقق من وجود تلك الاستراتيجيات بحيث تتضمن مستوى المخاطر المتعلقة بأمن الفضاء الإلكتروني والإجراءات موازية لدعم مستويات أمن الفضاء الإلكتروني (cyber resilience) بما يشمل وجود سياسة واضحة لحوكمة إدارة مخاطر أمن الفضاء الإلكتروني.

كما تلزم التعليمات الرقابية المصارف بتعيين مسؤول عن أمن المعلومات Chief Information Security Officer (CISO).

2. الضوابط والتعليمات الخاصة بتنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الانترنت

قام بنك المغرب بتنظيم طلبات فتح الحسابات بإصدار تعليمات خلال عام 2017 تنص على مراعاة الشروط التالية في حالة فتح الحساب عن بعد (عن طريق الانترنت مثلا):

- الحصول على وثيقة ثبوتية إضافية تمكن من تأكيد هوية العميل (مثل بطاقة الإقامة وجواز السفر).
- اشتراط أن تتم العملية الأولى المقيدة بدائنية الحساب الجديد انطلاقا من حساب مفتوح مسبقا من طرف صاحب الطلب بدفاتر مؤسسة بنكية موجودة ببلد يحترم معايير مجموعة العمل المالي FATF.
- تطبيق إجراءات اليقظة المُكثفة على الحساب طالما لم يحضر العميل بنفسه إلى الوكالة المعنية.

كما تطبق جميع الشروط والأحكام الواردة بتلك التعليمات المذكورة على جميع العملاء الراغبين في الاستفادة من الخدمات المصرفية بصفة عامة على الخدمات المصرفية عبر الإنترنت. هذا، ويعمل حالياً بنك المغرب بالتشاور مع المصارف على تحديد الآليات المعتمدة على التكنولوجيات الحديثة لتسهيل عملية التحقق من هوية العميل عند عملية فتح الحساب بما في ذلك عقد اللقاء معه.

فيما يتعلق بالضوابط والأساليب التي يعتمد عليها البنك في التحقق من هوية وصلاحية العميل الراغب في الاستفادة من الخدمات المصرفية (أو الراغب في تنفيذ أنشطة مصرفية) من خلال شبكة الانترنت، فإنه يجب مراعاة إستيفاء العميل لجميع الشروط المتضمنة ضمن التعليمات سالفة الذكر في مجال تحديد والتحقق من هويته وذلك عند فتح الحساب. أما بخصوص انجاز العمليات يضع المصرف رهن إشارة العميل تطبيقاً خاصاً يمكن الولوج اليه اعتماداً على رمز دخول خاص بالعميل (login) وكلمة سر (Password). كما طلب بنك المغرب في هذا الصدد من المصارف الاعتماد على تقنية 3D Secure لتوثيق العمليات المنجزة عبر الإنترنت عند استعمال بطاقة الأداء.

في إطار التحقق من هوية وصلاحية المخولين بالاستفادة من الخدمات المصرفية، تطبق البنوك نفس الضوابط والاساليب سواء كانت عبر الوكالات البنكية او من خلال شبكة الانترنت، حيث يتم تطبيق الإجراءات التالية:

- قبل فتح أي حساب، تقوم مؤسسات الائتمان بإجراء لقاءات مع مقدمي طلب فتح الحساب وعند الاقتضاء، مع وكلائهم، وذلك بهدف:
  - التأكد من هويتهم وجمع كافة المعلومات والوثائق المفيدة ذات الصلة بأنشطة طالبي فتح الحسابات ومناخ عملهم خاصة بالنسبة للأشخاص المعنويين.
  - فهم موضوع علاقة الأعمال المعتزم إقامتها وطبيعتها والحصول، عندما يلزم، على الوثائق الخاصة بهذا الجانب.
  - يتم إعداد استمارة باسم كل عميل ذي شخصية ذاتية ووكيله، استنادا إلى البيانات الواردة في وثائق التعريف الرسمية. يتعين الحصول على نفس المعلومات، المشار إليها في التعليمات

المذكورة، من الأشخاص الذين قد يطالبون بتشغيل حساب أحد العملاء بموجب توكيل.

- فلترة (screening) بيانات العملاء ووكلائهم ومنشئي العمليات والمستفيدين منها بالنظر إلى قوائم الهيئات الدولية المؤهلة المتعلقة بتجميد الممتلكات.
- تتبع العمليات غير الاعتيادية التي يتم توطينها في حاسابات العملاء بغض النظر عن الشخص الدي تم القيام بها (العملاء او وكلائهم).

بالنسبة للعملاء ذوي الشخصية المعنوية، إضافة الى الإجراءات المذكورة سالفاً فإنه يتم إعداد استمارة باسم كل عميل يدون فيها، حسب الطبيعة القانونية لهؤلاء الأشخاص، مجموع أو بعض بيانات التعريف، استنادا إلى البيانات الواردة في وثائق التعريف الرسمية. كما يجب أن تجمع المؤسسات عناصر التعريف المُشار إليها بالنسبة للمستفيدين الفعليين والأشخاص الذاتيين المخول لهم تشغيل حساب الأشخاص المعنويين.

فيما يتعلق بالضوابط والأساليب التي يلتزم البنك بتطبيقها للتحقق من هوية العميل الراغب في إجراء أحد التعديلات الخاصة ببيانات حساب خدمات الانترنت البنكي او البيانات الخاصة بالعميل، تحدد المصارف قائمة البيانات المسموح تعديلها عبر الانترنت، حيث إن تغيير البيانات المتعلقة بالهوية والنشاط المهني مثلاً يكون مشروطاً بتقديم الدلائل الضرورية لذلك. وبخصوص باقي البيانات، يقوم المصرف بإخبار العميل عن طريق البريد الإلكتروني أو من خلال رسالة قصيرة عن التعديل المطلوب مع ضرورة إدخال رمز لتوثيق العملية.

3. الضوابط والتعليمات الخاصة بتنظيم وسائل اثبات الهوية عبر الانترنت

بخصوص فتح الحساب، يجب مراعاة استيفاء العميل لجميع الشروط المضمنة بالتعميم الصادر عام 2017 في مجال تحديد والتحقق من هويته تبعا لتوصيات مجموعة العمل المالي FATF. فيما يتعلق بإنجاز العمليات، يضع المصرف رهن إشارة العميل تطبيقا خاصا يمكن الولوج اليه اعتمادا على رمز دخول خاص بالعميل (login) وكلمة السر (Password). كما طلب بنك المغرب في هذا الصدد من المصارف الاعتماد على تقنية 3D Secure لتوثيق العمليات المنجزة عبر الأنترنيت عند استعمال بطاقة الأداء. إضافة الى ذلك فانه طبقا لمقتضيات تعليمات بنك المغرب التي تحدد القواعد الدنيا، الواجب على مؤسسات الائتمان مراعاتها لإجراء اختبارات اختراق أنظمة المعلومات، التي توجب إخضاع أنظمة المعلومات المنفتحة على الخارج لاختبارات الاختراق على الاقل مرة واحدة في العام.

كما تتمثل الآلية التي تعتمد عليها البنوك في التحقق من تصديق العميل الكترونياً من خلال الانترنت، في ان يتم إبلاغ العميل من خلال الوسائل المختارة مثل الرسائل الإلكترونية والرسائل النصية القصيرة. وتقوم المصارف بتحديد عدد مرات المحاولات الفاشلة، هذا العدد الذي يختلف من مصرف الى آخر، لا يزيد عن ثلاث محاولات في أغلب الأحيان، وعند تجاوز العدد المسموح به، يتم التعطيل المؤقت للحساب البنكي. وفي بعض الحالات، يتطلب إعادة تشغيل الحساب تدخل الفرق الفنية للمصرف.

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

تحدد الجهات الرقابية التعليمات والتدابير الرقابية الخاصة بإدارة كلمة السر (Password) و (OTP)ومواصفاتهما، كما يدعو بنك المغرب المصارف إلى الاعتماد على أفضل الممارسات في هذا المجال.

5. الضوابط والتعليمات الرقابية الخاصة بعمليات تحويل الأموال من خلال خدمات الانترنت

تنص التعليمات الرقابية لبنك المغرب الصادرة عام 2017 المتعلقة بواجب اليقظة على المعلومات التي يجب أن ترافق التحويلات الالكترونية للأموال سواء عبر الحدود أو داخل الدولة.

6. الضوابط والتعليمات الرقابية الخاصة بسرية وسلامة المعلومات

في هذا الصدد، تحدد التعاميم سالفة الذكر الضوابط والتعليمات الخاصة بسرية وسلامة المعلومات، بحيث يجب أن تستفيد هذه المعلومات من نظام التشفير (data encryptions) ويمنع تخزينها خارج الدولة. من جانب آخر، تحدد التعليمات الخاصة بحماية المعلومات الشخصية شروط وضوابط معالجة المعطيات ذات الطابع الشخصي التي تفرض على المصارف في هذا الشأن.

7. الضوابط والتعليمات الرقابية الخاصة بتأمين التطبيقات الإلكترونية المستخدمة في تقديم الخدمات والمعاملات البنكية من خلال شبكة الانترنت

تحدد التعاميم الصادرة عن السلطات الاشرافية الضوابط والتعليمات فيما يخص أدوات تطوير النظم التي تلزم المصارف باحترام المعايير المعتمدة في هذا المجال وإخضاع الأنظمة المطورة لعملية الفحص الداخلي بصفة منتظمة ودورية. وطبقاً لمقتضيات تعليمات بنك المغرب، التي تُحدد القواعد الدنيا

الواجب على مؤسسات الائتمان مراعاتها لإجراء اختبارات اختراق أنظمة المعلومات، يجب إخضاع أنظمة المعلومات المنفتحة على الخارج لاختبارات الاختراق على الأقل مرة واحدة سنوياً.

8. تقييم السلطات الرقابية للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني والوضع الراهن

بلغ عدد حالات الإبلاغ التي تلقتها السلطة الرقابية التي تتعلق بانتهاكات لأمن الفضاء الإلكتروني في القطاع المصرفي حالتين خلال عام 2017 موزعة بواقع حالة برمجيات خبيثة وحالة هجوم إلكتروني سطحي، في حين لا توجد حالات مشابهة خلال عام النصف الأول من عام 2018.

تجدر الإشارة إلى أن السلطات الرقابية بالمغرب تُلزم المصارف بالقيام باختبارات الضغط (Stress Testing) لتحديد حجم الآثار المترتبة على نجاح أية عمليات قرصنة تتعرض لها الأنظمة الإلكترونية، وذلك بصفة دورية سنوية. كما تُلزم تلك التعليمات المصارف بالإبلاغ عن تعرضها لأية عمليات قرصنة إلكترونية وذلك في غضون يوم أو يومين من التعرض لعملية القرصنة الالكترونية.

9. التعاون والتنسيق مع السلطات الرقابية الأخرى عبر الحدود والشركاء في صناعة تقنية المعلومات فيما يتعلق بالمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإلكتروني

أصبحت مذكرات التفاهم والتعاون الموقعة مع الجهات الرقابية الأخرى تغطي كذلك موضوع تبادل الخبرات والمعلومات في مجال أمن نظم المعلومات. ويتم تدارس المخاطر المرتبطة بهذا الموضوع مع المراقبين الاخرين في إطار الاجتماعات الدورية التي يتم عقدها. هذا، ويتم تنظيم ورشة عمل سنوياً

بمشاركة بنك المغرب والمصارف وكذا الفاعلين في مجال أنظمة المعلومات وسلامتها.

10. بناء القدرات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

في هذا السياق تعمل السلطة الرقابية المسؤولة عن القطاع المصرفي على تعزيز القدرات البشرية لديها في مجال أمن الفضاء الإلكتروني، حيث بذلت الجهود التالية:

- أنشـــأ بنك المغرب وحدة مختصـــة في رصـــد مخاطر تكنولوجيا المعلومات.
- إصـــدار التعليمات بتحديد الحد الأدنى لمتطلبات أمن المعلومات المصرفية. بحيث تستند على أفضل الممارسات الصادرة من الجهات الرقابية والجهات الدولية ذات العلاقة مثل لجنة بازل.
- وضـــع إطار اشـــرافي على المصـــارف يتم التأكد من خلاله بالتزام المصارف بمتطلبات الحد الادنى لأمن المعلومات.
- تكوين لجان وفرق العمل المختصـــة بين المصـــارف وتحت إشـــراف المصـرف المركزي، لتبادل التجارب، ورسم إطار مشترك ومعالجة القضايا والتحديات الشائعة المتعلقة بأمن المعلومات.
- توسيع نطاق التعاون مع المؤسسات الحكومية الوطنية العاملة في هذا المجال (المديرية العامة لســـلامة نظم المعلومات ، وكالة التنمية الرقمية، ...).
- بنك المغرب في صـــدد برمجة بعثة مســـاعدة فنية مع صـــندوق النقد الدولي.

- الاشـــتراك في ورش العمل التي ينظمها صـــندوق النقد الدولي والمؤسسات الوطنية والدولية الأخرى.

11. التحديات الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

في ظل تطورات العمل المصرفي وتنامي استخدام أدوات مصرفية إلكترونية جديدة ساعدت على تطورها، التقدم التكنولوجي، فقد بات موضوع سلامة وأمن الصيرفة الالكترونية ذا أهمية عالية. يتمثل التحدي الرئيس في إنشاء إطار ملائم للتحول الرقمي للبنوك وانجاز مشاريع الانفتاح على الخارج والتكنولوجيات الجديدة من خلال الحفاظ على أمن أنظمة المعلومات.

كما تعاملت السلطات الرقابية مع هذه التحديات، إضافة الى الإجراءات سالف الإشارة اليها تم اتخاذ الإجراءات التالية:

- زيادة وتيرة المهام التفتيشية.
- إعداد خارطة طريق لسلامة أنظمة معلومات القطاع المالي بالتعاون مع الجهات الرقابية الأخرى.
- تعزيز عملية بناء القدرات في مجال أمن نظم المعلومات للمصارف.

12. التجارب الرقابية في مجال أمن نظم المعلومات والفضاء الإلكتروني

في هذا الإطار، فيما يلي عرض للتجربة المغربية في مجال أمن نظم المعلومات والفضاء الإلكتروني:

إن أمن وسلامة المعلومات المصرفية يعتبر أمراً ذات أهمية عالية للمصارف المركزية المسؤولة عن الاستقرار المالي. ويعد التهديد الإلكتروني من أبرز التحديات التي تواجه النظام المالي مما يستوجب سن تشريعات نظامية ورقابية وحث المصارف على تأمين نظم معلوماتها. وفي هذا الصدد ووفقاً لما

ينصه المخطـط الاستـراتيجي لبنك المغرب (2016-2018)، اتخذت مديرية الاشراف البنكي عدة إجراءات أهمها:

- وضع إطار إشرافي على المصارف تتبعه، حيث تم إصدار تعليمات رقابية في هذا الصدد بالتنسيق مع القطاع المصرفي تحدد القواعد الدنيا الواجب على مؤسسات الائتمان مراعاتها من أجل إجراء اختبارات اختراق نظم المعلومات. فأصبح من الواجب على هذه المؤسسات القيام بهذه الاختبارات بصفة منتظمة سواء من داخل او خارج شبكاتها المعلوماتية وعرض نتائجها على لجنة الفحص أو لجنة المخاطر ثم إرسال تقرير سنوي إلى بنك المغرب ترصد فيه خريطتها للمخاطر المعلوماتية والبرنامج المتبع من أجل تحقيق اختبارات الاختراق وكذا النتائج المترتبة عنها إضافة إلى التدابير المتخذة لتصحيح الثغرات المحتملة. وتمكن هذه الاجراءات بنك المغرب من التأكد من السياسة المتبعة من طرف مؤسسات الائتمان لضمان أمن نظمها وكذلك الوسائل المتاحة لديها.
- التنسيق مع القطاع المصرفي طبقا للمرسوم رقم 2-15-172، والذي فوضت بموجبه لبنك المغرب مهمة الإشراف على الأنشطة المتعلقة بأمن النظم المعلوماتية للمصارف التي تم تعيينها كبنيات ذات أهمية حيوية. وقد تم عقد عدة لقاءات مع الإدارة العامة لأمن نظم المعلومات التابعة للإدارة المركزية للدفاع الوطني تهم سبل تشجيع التعاون وتبادل المعلومات بين الطرفين في هذا المجال وكذا ضمان تطبيق المصارف لمقتضيات التعليمة الوطنية لأمن نظم المعلومات الصادرة عن هذه الإدارة.

- وطبقاً لنفس المرسوم، قام بنك المغرب بوضع لائحة لبنيات القطاع المصرفي ذات أهمية حيوية وبموجب تعليمات الإدارة العامة لأمن نظم المعلومات يتحتم على المؤسسات المصرفية حصر أنظمها المعلوماتية الحساسة واتخاد جميع التدابير لحمايتها.
- تكوين لجنة وفرقة عمل مختصة بين بنك المغرب والمصارف وذلك تحت إشراف مديرية الرقابة البنكية لتبادل الأفكار ورسم إطار مشترك ومعالجة القضايا التي تهم أمن نظم المعلومات.
- تفعيل الآلية التي وضعتها المديرية العامة لأمن نظم المعلومات لمشاركة التجارب حول حوادث الأمن المعلوماتي.

من جهة أخرى، وفي ظل هذه التهديدات الالكترونية المتزايدة، يتوفر لدى بنك المغرب نظام حماية يتوافق مع المعايير العالمية ولديه كفاءات مُتخصصة تضمن حسن سيره. ومن أجل تعزيز فعاليته يعمل بنك المغرب على نوعية موظفيه بضرورة اتخاد الحذر وكل تدابير السلامة المعلوماتية عند استعمال الأنظمة التي توجد تحت تصرفه مثل تجنب فتح او اعادة ارسال اي رسالة إلكترونية يشتبه في مصدرها. وقد وضعت مصلحة متخصصة تعمل على استقبال ومعالجة اي معلومة تهم أمن نظم البنك المركزي.

ثالثاً: الخلاصة

الاستعراض السابق لتجارب الدول العربية فيما يخص الجوانب المتعلقة بأمن الفضاء الالكترونيCyber Security في إطار المخاطر التشغيلية، أوضح ان التجارب الرقابية العربية في هذا المجال ليست ببعيدة عن الممارسات الدولية الأخرى في الشأن. فمعظم التعليمات الرقابية الصادرة من معظم السلطات الرقابية في الدول العربية (الخاصة بإطار المخاطر التشغيلية) تتسم بتضمنها

جزءً متعلقاً بمخاطر نظم المعلومات وأمن الفضاء الإلكتروني في القطاع المصرفي يحدد المعايير اللازم توافرها لضمان أمن الفضاء الإلكتروني. كما أن معظم المصارف المركزية العربية تُضمن عمليات الرقابة على أساس المخاطر اختبارات توضح مدى قدرة البنوك على مواجهة تلك المخاطر المتعلقة بأمن الفضاء الإلكتروني (المخاطر الإلكترونية ومخاطر نظم المعلومات والهجمات الإلكترونية Cyber attacks).

إضافة لذلك تسمح بعض الدول العربية للعملاء إنشاء أو فتح حساب مصرفي من خلال موقع البنك على شبكة الانترنت، وذلك في ضوء عدد من الضوابط والتعليمات بالنسبة للمصرف والعميل. بينما، وفقاً للتعليمات الصادرة عن السلطات الرقابية في بعض البلدان العربية فان المصارف تلتزم بعدم السماح للعملاء الجدد بفتح حساب مصرفي باستخدام موقع البنك على شبكة الانترنت، وتقوم تلك الدول بتطبيق قواعد التعرف على هوية العملاء والخاصة بمكافحة غسل الأموال وتمويل الإرهاب الصادرة من السلطات الرقابية في هذا الشأن. تعتمد معظم المصارف في الدول العربية على استخدام مبدأ الدخول المزدوج (Tow Factors Authentication) في التحقق من هوية العميل المستفيد من الخدمات المصرفية من خلال الإنترنت، وتقوم المصارف المركزية بالدول العربية بعملية التقييم الفني والأمني للخدمات المصرفية المقدمة من البنوك عبر الانترنت، خاصة فيما يتعلق بالسرية والخصوصية والتحقق من الهوية وذلك قبل تقديم الخدمة للعميل. توضح التعليمات والتعاميم الرقابية في معظم الدول العربية، انه 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.

تنص التعليمات الصادرة عن معظم الأجهزة العربية للرقابة على المصارف على أنه يجب على كل بنك مراعاة التدابير الرقابية عند التعامل مع كلمة السر الخاصة بالعملاء، بحيث يتم تطبيق الرقابة المزدوجة وان يتم الفصل بين عملية انشاء كلمات السر وتسليمها للعملاء وعملية تفعيل حسابات خدمات الانترنت البنكي، وتعزيز تأمين عملية انشاء كلمة السر لضمان عدم تعرضها للكشف. كما قامت غالبية الدول العربية بتحديد الحد الأدنى المطلوب في المواصفات الخاصة بكلمة السر لمرة واحدة (OTP)، و لرموز الأمان(PIN). اما بالنسبة لخدمة تحويل الأموال، فقد ألزمت السلطات الرقابية البنوك بوضع الضوابط المناسبة التي تساعد على خفض مستوى المخاطر المصاحبة لتلك الخدمة لتصل الى مستوى مقبول ومعتمد من البنك.

إن وصول البنوك العربية لهذا المستوى من حيث تطبيق المعايير والممارسات الدولية لم يكن بمحض الصدفة، ولكنه جاء نتاج الجهود المبذلة من تلك الدول والمتابعة الدؤوبة لكل ما هو جديد في مجال امن نظم المعلومات الالكترونية. إضافة الى الاستعانة بالخبرات الدولية والعربية، وكذا العمل على خلق الكوادر المدربة من خلال اتاحة الفرصة للتدريب وحضور المؤتمرات بالخارج والداخل. كما تقوم معظم الدول العربية بالتعاون مع المؤسسات والجهات الدولية المتخصصة في الشأن.

للحصول على مطبوعات صندوق النقد العربي

يرجى الاتصال بالعنوان التالي:

صندوق النقد العربي

ص.ب. 2818

أبوظبي - الإمارات العربية المتحدة

هاتف رقم: 6215000 (9712+)

فاكس رقم: 6326454 (9712+)

البريد الإلكتروني: centralmail@amfad.org.ae

موقع الصندوق على الإنترنت: http://www.amf.org.ae

http://www.amf.org.ae

صندوق النقد العربي
ARAB MONETARY FUND

مجلس محافظي المصارف المركزية ومؤسسات النقد العربية
Council of Arab Central Banks and Monetary Authorities Governors