مؤسسة النقد العربي السعودي

قواعد الخدمات المصرفية الإلكترونية

إدارة التقنيـة البنكيـة

أبريل 2010م

جدول المحتويات

1- مقدمة:

1-1 تعريف المصرفية الإلكترونية:

يقصد بعبارة "المصرفية الإلكترونية" الخدمات المصرفية التي تقدمها عن بعد مصارف مصرحة، أو ممثلوها عبر أجهزة تعمل تحت رقابة وإدارة مباشرة من المصرف أو بموجب اتفاقية إسناد هذه المهمة لجهة أخرى. والمصرفية الإلكترونية، بعبارة أخرى، هي مصطلح عام لعملية يمكن بواسطتها للعميل القيام بعمليات مصرفية إلكترونياً بدون زيارة الفرع ويشمل هذا المصطلح الأنظمة التي تمكن عملاء المصارف، سواء أفراد أو شركات، من الوصول إلى حساباتهم أو تنفيذ عملياتهم أو الحصول على معلومات تتعلق بمنتجات وخدمات مالية عبر شبكة عامة أو خاصة، بما في ذلك شبكة الإنترنت.

ويقصد بالخدمة المصرفية عن بعد:

- خدمة مصرفية خاصة قام العميل بالتسجيل بها وإعتمدها بشكل صريح.
- خدمة مقدمة باستخدام أجهزة لا تخضع لرقابة مقدم الخدمة.
- خدمة تحتاج إلى توثيق العميل.

ويقصد بالمصرفية الإلكترونية عبر الحدود، تقديم منتجات أو خدمات لعمليات مصرفية عبر الإنترنت من قبل مصرف في دولة ما إلى عميل مصرح له في دول أخرى. ويشمل هذا التعريف الحالات التي يقدم فيها مصرف أجنبي منتجات أو خدمات إلكترونية لمقيمين في بلد أجنبي من (1) موقع في البلد الأم للمصرف، أو(2) مؤسسة في بلد أجنبي آخر تكون خاضعة لأنظمته.

يمكن غالباً استخدام كل مصطلح من المصطلحات التالية مكان الآخر لوصف الصور المتنوعة للمصرفية الإلكترونية: المصرفية باستخدام جهاز الحاسوب الشخصي، والمصرفية عبر الإنترنت، ، والمصرفية عبر الاتصال بالانترنت، والمصرفية المباشرة (virtual)، والمصرفية من المنزل، والمصرفية الإلكترونية عن بعد.

الخدمات المستثناة

تشمل عادة المصرفية الالكترونية أيضاً الهاتف المصرفي واستخدام أجهزة الصرف الآلي إلا أنهما غير مشمولين بتعريف المصرفية الإلكترونية المذكور آنفاً لغرض هذه القواعد.

علاوة على ذلك، إن المراسلات الشخصية كرسائل البريد الالكتروني (الموقعة رقمياً أو خلاف ذلك) التي يتلقاها مقدم الخدمة من عميل ما خارج سياق الخدمة المصرفية عن بعد غير مشمولة أيضاً في هذا التعريف.

هناك مصطلحات أخرى مختلفة ذات صلة معرفة في قائمة المفردات في ملحق 1 من هذه القواعد.

1-2 تطور المصرفية الالكترونية

إن لتطورات وابتكارات التقنية تأثيراً كبيراً على النشاط المصرفي. وتواجه المصارف تحدي التكيف والابتكار والتعامل مع الفرص التي تقدمها التطورات التقنية. وقد استفادت المصارف وعملاؤها إلى حد كبير من نمو المصرفية الإلكترونية. فقد أتاحت المصرفية الإلكترونية للمصارف التوسع في تقديم الخدمات إلى من يتعذر عليهم الوصول إليها، وتقليص تكاليف العمليات، وتحسين الفاعلية، وتقديم خدمات مصرفية مباشرة. وعلى الجانب الآخر، استفاد العملاء من الخدمات المصرفية الفعالة بتكاليف أقل نسبياً مع إتاحة خيار الاختيار من القنوات البديلة لتقديم الخدمات. كما سهلت المصرفية الإلكترونية الانتقال السريع للأموال محلياً وعبر الحدود.

لقد فرضت هذه البيئة المالية المتغيرة تحديات جديدة على المصارف وصانعي السياسات/الجهات الرقابية. وقد زادت الآن المصارف من اعتمادها على التقنية للمنافسة في بيئة عمل تنافسية بشكل متزايد وبالتالي يجب عليها إدارة أمن تقنية المعلومات والمخاطر الأخرى المتعلقة بها. وتواجه البنوك المركزية والسلطات الرقابية تحديات جديدة في الرقابة المصرفية وكذلك في تصميم وتنفيذ السياسة النقدية. ويتطلب النطاق المتنامي للمصرفية الإلكترونية ودرجة التعقيد المتزايدة للمنتجات والخدمات المصرفية استمرار تكيف الإطار التنظيمي وإشرافاً رقابياً فعالاً.

1-3 قواعد المصرفية الإلكترونية

لكي تتمكن المصارف من حماية معلومات عملائها، وتقليص حالات الاحتيال، وإدارة المخاطر المتعلقة بالمصرفية الإلكترونية، وأيضاً تقليص عدد الشكاوى من مستخدمي المصرفية الإلكترونية، قررت مؤسسة النقد العربي السعودي إصدار "قواعد جديدة للمصرفية إلكترونية". وسوف تحل هذه القواعد محل "إرشادات أمن المصرفية عبر الإنترنت" الصادرة عام 2001م.

وتعتمد القواعد الجديدة للمصرفية الإلكترونية على المخاطر وتحدد الطريقة التنظيمية الاحترازية التي تعتمدها مؤسسة النقد للرقابة على خدمات المصرفية الإلكترونية. وتقدم هذه القواعد التوجيه للمصارف بشأن إدارة المخاطر في المصرفية الإلكترونية وتؤكد على:

- المسئولية المشتركة لمجلس الإدارة والإدارة العليا.
- حماية العميل وتثقيفه.
- خصوصية العميل.
- الحد الأدنى للمعايير الأمنية تماشياً مع أفضل المعايير الدولية.
- الإدارة الملائمة للحوادث ورفع تقارير للمؤسسة.
- الإدارة الملائمة لإتاحة الاستخدام (Availability).
- بناء القدرات والتخطيط من أجل استمرارية العمل.

ويتوقع أن تراجع المصارف وأن تعدل، إن كان ذلك ضرورياً، سياساتها وعملياتها الخاصة بإدارة المخاطر لتكون أنشطتها المصرفية الإلكترونية متوافقة مع هذه القواعد.

1-4 هدف القواعد

الهدف الرئيس من قواعد المصرفية الإلكترونية تقديم التوجيه للمصارف فيما يتعلق بتنفيذ الضوابط الأمنية في منتجاتها وخدماتها المصرفية الإلكترونية والإدارة الفعالة للمخاطر المرتبطة بها. ولا تهدف القواعد إلى تثبيط المصارف عن الابتكار والإبداع في المصرفية الإلكترونية شريطة أن تظل ضمن الإطار التنظيمي وأن تضمن التيسير على العملاء.

1-5 نطاق التطبيق

يتم تطبيق "قواعد المصرفية الإلكترونية" على جميع أشكال المصرفية الإلكترونية كما هي محددة في قسم 1-1 من هذه القواعد. مع ملاحظة أن هذه القواعد لا تشمل خدمات المصرفية الإلكترونية التي تقدمها أجهزة الصرف الآلي، ونقاط البيع، والهاتف المصرفي.

و على جميع المصارف المرخصة والمصرحة من المؤسسة بتقديم خدمات مصرفية إلكترونية، سواء محلياً أو خارجياً من خلال فروعها/ مؤسسات تابعة لها، الإلتزام بهذه القواعد.

يخضع تقديم الخدمات المصرفية الإلكترونية عبر الحدود إلى الترخيص الضروري والالتزام بقوانين وأنظمة/لوائح البلدان الأم والمضيفة. ولا يُسمح للمصارف الأجنبية غير المرخصة من المؤسسة للعمل في المملكة بمزاولة أنشطة المصرفية الإلكترونية عبر الحدود في السوق السعودية.

1-6 تاريخ سريان تطبيق القواعد

تدخل هذه القواعد حيز التنفيذ فوراً. ويجب على جميع المصارف اتخاذ الإجراءات الضرورية لضمان الالتزام بهذه ا لقواعد.

2- الاشراف على الخدمات المصرفية الإلكترونية

2-1 طريقة الاشراف

يتمثل أسلوب المؤسسة الرقابي في وضع إطار تنظيمي إحترازي لنمو الخدمات المصرفية الإلكترونية في المملكة العربية السعودية والمحافظة عليه. ويتوقع من المصارف تطبيق ضوابط لإدارة المخاطر تنسجم مع المخاطر المرتبطة بأنواع ومستوى تعقيد وحجم العمليات المنفذة وبقنوات الخدمة الإلكترونية المقدمة. ويجب عليها إتخاذ إجراءات صارمه لإدارة المخاطر ومقاييس أمنية لتقنية المعلومات تتلاءم مع إستراتيجية أعمالها المصرفية الإلكترونية والمستوى المعتمد لتحمل المخاطر. ويجب أن تكون ضوابط إدارة المخاطر الموضوعة للخدمات المصرفية الإلكترونية مطابقة ومتوافقة مع الأنظمة الشاملة لإدارة المخاطر. ويتوقع أيضاً من المصارف إستحداث إجراءات مفصله ومدروسة لضمان حل سريع للقضايا المتعلقة بالنواحي الأمنية.

ولضمان الإلتزام بأفضل المعايير الدولية، صادقت المؤسسة على المبادئ والتوصيات المتعلقة بالخدمات المصرفية الإلكترونية الوارده في ورقة لجنة بازل للإشراف المصرفي بعنوان "مبادئ إدارة المخاطر للخدمات المصرفية الإلكترونية".

(httb:/www.bis.org/publ/bcbs98.htm)

ونظراً للطبيعة الديناميكية للخدمات المصرفية الإلكترونية والوسائل التقنية ذات العلاقة، تدرك المؤسسة أن القضايا التي يتعين علاجها قد تتفاوت من آن لأخر ومن بنكٍ لآخر. ولهذا السبب، تميز هذه القواعد بين الحد الأدنى من المتطلبات وبين الضوابط الإضافية الموصى بها.

2-2 المنتجات الجديدة للخدمات المصرفية الإلكترونية

يتعين على المصارف الحصول مسبقاً على موافقة المؤسسة قبل إطلاق أي منتج مصرفي إلكتروني جديد أو تعديل المنتج القائم بشكلٍ كبير و/أو إطلاق منتج جديد بنفس الإسم. ولهذا الغرض، يتعين عليها تقديم طلب للمؤسسة مصحوباً بالمعلومات ذات الصلة، بما فيها أبرز سمات المنتج والسوق المستهدفة والأنظمة والضوابط ذات العلاقة، وتأكيداً مفاده أن المنتج المقترح يلتزم بكافة الأنظمة والقواعد/اللوائح ذات الصلة. ويجوز للمؤسسة منح موافقتها أو الإمتناع عن ذلك، أو منحها وفقاً للشروط التي قد تراها مناسبة.

2-3 المتطلبات القانونية والتنظيمية

بالإضافة إلى هذه القواعد، يُطلب من المصارف ضمان الإلتزام بالأنظمة والمتطلبات التنظيمية الأخرى ذات العلاقة. وعند إسناد مهمة القيام بممارسة عمليات ونشاطات متعلقة بالمصرفية الإلكترونية لجهة أخرى، يجب على المصارف إتباع "قواعد المؤسسة المتعلقة بإسناد المهام لجهات أخرى" حسب تعديلها من وقتٍ لآخر.

وتشمل الأنظمة والتوجيهات الأخرى ذات العلاقة، من ضمن أمور أخرى، ما يلي:

- نظام مراقبة البنوك.
- نظام مكافحة غسل الأموال.
- قواعد مكافحة غسل الأموال وتمويل الإرهاب.
- دليل مكافحة الإختلاس والإحتيال المالي وتعليمات الرقابة.
- دليل الإلتزام بالأنظمة للبنوك العاملة في المملكة العربية السعودية.
- اللوائح والقواعد التشغيلية لنظام سريع.
- القواعد والتوجيهات والتعاميم الأخرى ذات الصلة الصادرة عن المؤسسة.

وتقوم المؤسسة بتحديث إطارها التنظيمي باستمرار ليتواكب مع المعايير الدولية والظروف المتغيرة للسوق. ويتوقع من المصارف متابعة هذه التغيرات وضمان الإلتزام بأحدث المتطلبات التنظيمية.

2-4 آلية التنفيذ

أ) المراجعة الداخليه

يجب على المصارف تحديد برنامج مناسب لتدقيق الإلتزام بالأنظمة لضمان سير تنفيذ الأعمال المصرفية الإلكترونية طبقاً لهذه القواعد وسياسة وإستراتيجية المصرف. ويجب أن يشمل نطاق هذه المراجعة، من بين مسائل أخرى، تقييم الضوابط الداخلية ذات الصلة، بما في ذلك فصل المهام، والضوابط المزدوجة، وضوابط أمن المعلومات، والمطابقة.

كما يجب على المصارف تحديد عملية إجراء مراجعة الإلتزام بالأنظمة فيما يخص أعمالها المصرفية الإلكترونية. ويجب أن تشمل عملية المراجعة تقييم قابلية التعرض للتجاوزات والإختراق الأخلاقي لجميع الشبكات والأنظمة والبرامج التطبيقية المرتبطة بالخدمات المصرفية الإلكترونية. وعلاوة على ذلك، يجب عليها تحديد مستوى مشاركة إدارة التدقيق والمراجعة في حالة حدوث عملية إحتيال تتعلق بالخدمات المصرفية الإلكترونية. كما يجب أن تشمل إجراءات المراجعة مراجعة تقديم/إنشاء حساب مستخدم جديد، والتغييرات اللاحقة في حساب المستخدم، وعقود الخدمات المصرفية الإلكترونية وتثقيف العملاء حول التوثيق.

ب) المراجعة الإشرافية

تراجع المؤسسة كفاءة المقاييس الأمنية لتقنية المعلومات وإجراءات إدارة المخاطر التي تعتمدها المصارف للقيام بالأعمال المصرفية الإلكترونية. ويتم ذلك كجزء من عملية المراجعة الإشرافية. وبالإضافة إلى ذلك، يتم التحقق من الإلتزام بهذه القواعد خلال الزيارة التفتيشية المكتبية للمصرف.

2-5 متطلبات الإبلاغ

يتعين على المصارف متابعة وإبلاغ المؤسسة عن أي حادثة أمنية يصنفها مالك المؤسسة المالية على أنها من المخاطر ذات الدرجة العليا أو المتوسطة والخطوات التي اتخذتها لمعالجة الحادثة في الوقت المناسب،

وكذلك الخطوات التي اتخذها المصرف لتجنب وقوع حادثة مشابهة في المستقبل. ويوضح الملحق3 (الإبلاغ عن الحوادث) المرفق بهذه القواعد التفاصيل المتعين إبلاغها والجدول الزمني للإبلاغ. ويجب رفع هذه التقارير لمدير إدارة التقنية البنكية لدى المؤسسة وذلك عن طريق البريد الإلكتروني.

3- حماية وتثقيف العملاء

3-1 حقوق والتزامات المصارف والعملاء

يُتوقع من المصارف مراجعة عقود العملاء فيما يتعلق بحقوق والتزامات كل شريك متعاقد. كما يجب على المصارف إنشاء عقود تكون:

- سهلة الفهم، مكتوبة بلغة واضحة ودقيقة (باللغتين العربية والإنجليزية) يمكن لأي عميل أن يفهمها. ويجب تجنب الكلمات والعبارات الغامضة، التي قد تحمل معنىً مزدوجاً.

- مستندة على أحكام وشروط واضحة بحيث:

  - تضمن توفر الخدمة على مدار الساعة (24 X 7 X 365). وفي حالة وجود مدة توقف مقرر لغرض الصيانة، يجب إشعار العملاء بذلك مسبقاً قبل وقت كافٍ.
  - تنص على إتفاقية مستوى الخدمة (SLA) بين المصرف وبين العميل مع برنامج تعويضي في حالة تعذر تقديم الخدمة المصرفية الإلكترونية بسبب أخطاء المصرف أو تعطل الأنظمة.
  - تشرح للعملاء وتثقفهم حول كيفية إستخدام آلية محكمة للتوثيق (مثلاً كلمة سر محكمة).
  - تستخدم نظاماً آمناً للإرسال عند التخاطب مع العملاء.
  - تنص بوضوح على مستوى خصوصية العميل ومدى الكشف عن معلوماته/معلوماتها داخلياً ضمن نطاق المصرف.
  - تحظر على المصرف كشف معلومات العملاء للغير.
  - تشرح عملية معالجة شكاوى أو إعتراضات العملاء ضمن إطار زمني معقول للتقدم بشكوى أو إعتراض.

- تشرح بوضوح عملية تفعيل وإيقاف حركة الحساب المصرفي الإلكتروني لحماية العملاء عندما تكون حساباتهم غير نشطه لفترة زمنية طويلة.
- تشرح بوضوح خطورة إستخدام العملاء لشبكات/ أجهزة حاسب آلي عامة أو شبكات دولية عندما يكونون في الخارج.
- تشرح بوضوح باللغتين العربية والإنجليزية مستوى الأمان الذي يتعهد المصرف بتحقيقه لحماية موجودات العملاء وبالتالي معلوماتهم.
- تزود العملاء بطريقة عن كيفية تمكّنهم من تجميد حساباتهم الخاصة بشكلٍ أتوماتيكي (مثلاً، إجراء خمس محاولات متتابعة للدخول باستخدام كلمة مرور خاطئة). ويحظر على المصرف تجميد حسابات العملاء أو الخدمة بدون تحديد أسباب موضوعية وبدون إشعار مسبق للعميل بذلك.

• مستندة على بيانات واضحة حول إلتزامات المصرف والعميل في حالة عدم الوفاء بالإلتزامات الخاصة بكل منهما.

3-2 أمن العملاء وتثقيفهم

يجب على المصارف أن تضع وتنفذ برامج توعوية/ تثقيفية مناسبة حول منتجاتها وخدماتها المصرفية الإلكترونية لضمان التعرف على هوية العميل وتوثيقه تماماً قبل الدخول إلى وتنفيذ عمليات مصرفية عن طريق الإنترنت. ولهذا الغرض، تستطيع المصارف إستخدام قنوات متعددة مثل المواقع الإلكترونية على الشبكة، أو الرسائل المطبوعة على كشوفات العميل أو المنشورات الترويجية أو الإتصال المباشر بالموظفين من خلال مراكز الاتصال الهاتفية وفي الفروع.

ويجب أن يغطي الإشعار الأمني، على الأقل، المسائل الآتية:

• أساليب توعوية وتحذيرية من إحتمال حدوث محاولات للإحتيال عن طريق الإنترنت، تشمل:

- هجمات على المواقع، وإستخدام هوية المصرف على موقع زائف.
- يجب تحذير العملاء من الدخول لموارد المصرف عبر الإنترنت من خلال مواقع أو بوابات إليكترونية أو عناوين بريد إليكترونيه أخرى.

- يجب إشعار العملاء بأن لايثقوا بأي مصدرعبر الإنترنت لمجرد أنه يحمل هوية المصرف.

- الاستخدام السري لإسم المستخدم وكلمة المرور.

- يجب على العملاء عدم إشراك الآخرين بإطلاعهم على كلمات المرور الخاصة بهم.
- لا يفترض أن يفصح العملاء عن إسم المستخدم االشخصي أو كلمة المرور الخاصة بهم لأيٍ من موظفي المصرف تحت أي ظرفٍ كان.
- ضرورة تغيير كلمة السر بشكلٍ دوري.

- الإنتقاء الحذر لكلمة السر لتجنب تخمينها.

- إسداء المشورة للعملاء حول كيفية إنتقاء أو إيجاد كلمات مرور أو أرقام هوية شخصية محكمة بإتقان بحيث لا يمكن تخمينها أو التنبؤ بها بسهولة.

- تخزين كلمات المرور بشكل مناسب.

- إعتماد توثيق يحتوي عاملين توثيقيين وفقاً على تعميم المؤسسة رقم **40690** الصادر في السادس من أغسطس **2009**م.

- عدم إفشاء المعلومات الشخصية لأشخاص غير مخولين أو لمواقع إليكترونية/ عناوين بريد إليكتروني مشكوك فيها.

- التذكير بعدم الدخول إلى الخدمات المصرفية الإلكترونية من خلال حاسبات إليكترونية عامة أو مشتركة.

- إسداء المشورة للعملاء حول كيفية تحديد هوية موظف المصرف الواجب التعامل معه في حالة وجود مطالبات "لموظف ما".

- توجيه النصح باستخدام أحدث الإصدارات للجدار الناري الشخصي لحماية نظام الحاسب، والبرامج المضادة للفيروسات.

3-3 إلتزامات المصرف

تتحمل المصارف المسؤولية عن أمان وسلامة الخدمات والأنظمة التي توفر لعملائها. وتشمل إلتزاماتها بهذا الخصوص ما يلي:

- المسؤولية والأضرار المحتملة على العملاء بسبب عدم دقة أو عدم إكتمال المعلومات حول المنتجات والخدمات والأسعار التي تقدمها على الموقع الإليكتروني؛

- إحتمال الدخول والتهديد بالدخول لمعلومات العملاء أو المصرف إذا لم يكن الموقع الإليكتروني معزولاً بشكلٍ مناسب عن الشبكة الداخلية للمصرف؛

- المسؤولية المحتملة عن نشر الفيروسات والبرامج الخبيثة لحواسيب إليكترونية تتخاطب مع الموقع الإليكتروني للمصرف؛

- عمليات التوثيق اللازمة للتحقق مبدئياً من هوية العملاء الجدد. ويجب على المصارف التأكد من أن هوية العميل تم التحقق منها وثبتت صحتها قبل بدء الإرتباط بأي نوع من العلاقة. وتُعد هذه الخطوة الإجرائية هامة بشكلٍ خاص مع العملاء الجدد الذين توجد مواقعهم خارج المنطقة التي يقع فيها مقر المصرف؛

- عمليات التوثيق لتحديد هوية العملاء الموجودين الذين يصلون للخدمات المصرفية الإلكترونية لأي إستخدام للخيارات المصرفية الإليكترونية على مختلف المستويات: الاتصال بشبكة الحاسوب لبدء التشغيل، تنفيذ عملية، وإعطاء أوامر، ووضع تأكيدات، وإيقاف التشغيل؛

- الخسائر الناجمة عن الإحتيال في حالة إخفاق المصرف في التحقق من هوية الأشخاص أو المؤسسات التجارية المتقدمة بطلب الحصول على حسابات جديدة أو خدمة ائتمانية عبر الإنترنت. ويجب على المصارف معرفة عملائها وتحديد طرق لمعرفة الهوية بشكل صريح؛

- حماية عملاء المصرف من محاولة الإحتيال عبر الإنترنت (هجمات المواقع ورسائل البريد الإلكتروني الزائفة وتزوير العناوين حيث يطلب إفشاء معلومات شخصية سرية) وذلك بإستخدام عملية أو خدمة إحترافية موثوقة لدرء خطر هذه الانتهاكات وكشفها ومجابهتها؛

- إتخاذ إجراء حماية ضد البيانات الخاطئة غير المشروعة للمصرف أو أي إستخدام غير مشروع لهوية المصرف عبر الإنترنت بصرف النظر عن الغرض؛
- توعية عملاء المصرف بعدم الإنقياد لأي جهة تدعي أنها المصرف بإعطائها معلوماتهم الشخصية.
- توعية عملاء المصرف بعدم الوثوق بأي موقع إليكتروني لمجرد أنه يحمل شعار المصرف؛
- الإنتهاكات المحتملة للأنظمة واللوائح الخاصة بخصوصية العملاء ومكافحة غسل الأموال ومكافحة الإرهاب، أو لمحتوى أو توقيت أو تقديم بيانات الإفصاح المطلوبة من العملاء؛
- الفشل في تنفيذ مدفوعات طرف ثالث حسب التوجيه أو في غضون الأطر الزمنية المحددة، ونقص توفر الخدمات عبر الإنترنت أو الدخول غير المصرح به لمعلومات العملاء السرية خلال الإرسال أو التخزين؛
- تأمين خدمة للعملاء سهلة الإستعمال عن طريق وضع إجراءات مناسبة لإجابة مطالباتهم خلال (3) أيام عمل.

إلا أن المصارف لايمكن أن تتحمل المسؤولية تجاه إخفاق العملاء في حماية معلوماتهم الشخصية مثل إفشاء التفاصيل السرية (مثلاً، رقم المستخدم أو كلمة المرور).

4- مخاطر المصرفية الإلكترونية

4-1 أنواع الخدمات

أ) المواقع الإلكترونية للحصول على المعلومات فقط

تعّرف المواقع الإلكترونية للحصول على المعلومات فقط بأنها تلك المواقع التي تتيح الدخول لغرض الحصول على معلومات عن التسويق بشكل عام ومعلومات أخرى متاحة للجمهور، أو لإرسال رسائل بريدية إليكترونية غير حساسة. ويجب على المصارف ضمان تحذير العملاء من المخاطر المحتملة المرتبطة بالرسائل البريدية الإليكترونية غير المشفرة المرسلة عبر تلك وسيلة كهذه.

ب) المواقع الإليكترونية لنقل المعلومات

تعد المواقع الإليكترونية لنقل المعلومات تفاعلية من حيث أنها تمكّن من إرسال الرسائل أو الوثائق أو الملفات الحساسة فيما بين مجموعة من المستخدمين، مثل موقع إليكتروني لمصرف يتيح للعميل تقديم طلب الحصول على قرض أو حساب إيداع عن طريق الإنترنت. وبما أن المخاطر الأمنية المتعلقة بالاتصال والأنظمة تشمل خصوصية وسرية البيانات وسلامة البيانات والتوثيق وعدم الإنكار وتصميم نظام الدخول، لذا من الضروري وضع بعض الطرق للتخفيف من حدة المخاطر.

جـ) المواقع الإليكترونية لإتمام تنفيذ العمليات:

تمثل المواقع الإليكترونية لإتمام تنفيذ العمليات أعلى درجة للطاقة التشغيلية، كما أنها تنطوي على مستويات مرتفعة من المخاطر المحتملة. فهذه الأنظمة توفر الإمكانات اللازمة للتقدم بطلب للحصول على المعلومات فقط وأنظمة تحويل المعلومات إليكترونياً، بالإضافة إلى الحصول على الخدمات المصرفية لتنفيذ العمليات عبر الإنترنت. وتوفر هذه الإمكانات عن طريق الإرتباط التفاعلي بين أجهزة العملاء وبين الأنظمة الداخلية للمصرف. كما أن العديد من الأنظمة تشتمل على مزيج من هذه الإمكانات.

4-2 لمحة مختصره للمخاطر

تصنف هذه القواعد الخدمات والمنتجات المصرفية الإلكترونية طبقاً لمستوى الأمن المطلوب لأداء الخدمة، وطبقاً للشرط التعاقدي المرتبط بهذه الخدمة كما يلي:

أ- معلومات عامة (مثل النشرات والإعلانات الدعائية ... الخ)

تمثل هذه المجموعة أدنى المخاطر. وتتعلق بتقديم البيانات التي لا علاقة بها بأي حساب أو فرد. ولا يتوجب على المصرف فيما يتعلق بالأوصاف وأسعار الصرف وأسعار الفائدة وتفاصيل الاتصال إلا مجرد أن تكون المعلومات سليمة.

ب- معلومات تتعلق بالعملاء (مثل الكشوفات)

تمثل هذه المجموعة المعلومات المتعلقة بالعملاء أو حساباتهم. وتشمل الأمثلة لذلك كشوفات وأرصدة الحسابات. وضمن هذه المجموعة، لا يسمح بأي عمليات تتضمن تحويل الأموال أو تغيير البيانات، بحيث تنحصر المخاطرة في إنكشاف بعض البيانات السرية.

جـ- تعليمات تفويضية مسبقة للعملاء (موقعة مرة واحدة)

تتعلق هذه المجموعة بالعمليات المالية الأقل خطورة، وهى تلك العمليات التي سبق التفويض بها باستخدام قنوات (مصرفية غير إليكترونية) أخرى. وعلى نحو نمطي، لاتتيح هذه العمليات للعميل إلا مجرد تعديل المبلغ المقرر دفعه أو التاريخ الذي يتم فيه تنفيذ العملية.

د- عمليات يُنشئها العميل (عمليات فردية)

تتعلق هذه المجموعة بتقديم العمليات التي يمكن للعميل خلالها تحديد المستفيد والمبلغ والتاريخ دون ترتيب مسبق أو تفويض إضافي لاحق. وتتمحور هذه الوثيقة بشكل رئيس على هذه المجموعة. ويجوز للمصارف أن تقرر تقسيم هذه المجموعة بناء على مبلغ العملية أو مؤشرات أخرى تتعلق بالعملية.

هـ- تسجيل وتعيين العميل (إشارة بدء الإتصال)

تمثل هذه المجموعة أعلى أحجام المخاطرة. حيث يشكل تسجيل وتعيين العميل الأساس الذي تقوم عليه كافة الجوانب الأمنية، ولذلك يجب التعامل معها بأقصى درجات العناية. وتشمل هذه المجموعة القدرة على تعديل إسم العميل أو عنوانه أو بيانات التوثيق.

4-3 مخاطر مصاحبة

أوجدت المصرفية الإلكترونية تحديات جديدة لإدارة المخاطر بالنسبة للمصارف. وبالطبع، قد تتأثر جميع المخاطر المرتبطة بالخدمات والمنتجات المصرفية التقليدية والمنتجات بتطبيق المصرفية الإلكترونية. وعلاوة على ذلك، هناك سبع فئات من المخاطر ذات الصلة بشكل خاص بالمصرفية الالكترونية. والمخاطر المصاحبة هي مخاطر إستراتيجية وتشغيلية/عمليات ومخاطر تقنية ومخاطر أعمال ومخاطر احتيال عبر الانترنت ومخاطر سمعة ومخاطر قانونية.

أ- **مخاطر إستراتيجية:** المخاطر الإستراتيجية هي الآثار الحالية والمنظورة على المتحصلات ورأس المال الناشئة عن قرارات عمل غير ملائمة وتطبيق خاطئ للقرارات وقصور أو عدم الاستجابة للتغيرات الحاصلة في الصناعة المصرفية. ويجب أن تتوافق الخدمة المصرفية الالكترونية مع إستراتيجية المصرف المالية الكلية، وهذا هو الأمثل. ويجب أن تركز عملية التخطيط واتخاذ القرارات على كيفية

تلبية حاجات العمل وتعزيز المصرفية الالكترونية بدلاً من التركيز على المنتج كهدف عمل مستقل. ويجب أن تحدد الرؤية الإستراتيجية كيفية تصميم المصرفية الالكترونية وعملية تطبيقها ومتابعتها.

ب- **مخاطر تشغيلية/عمليات:** تنشأ المخاطر التشغيلية/العمليات من الاحتيال، وأخطاء المعالجة، وتوقف النظام، وعدم القدرة على تقديم المنتجات والخدمات، والمحافظة على الوضع التنافسي، وإدارة المعلومات. ولتقديم الخدمات المصرفية الالكترونية قد تعتمد المصارف على عملية إسناد مهام لشركات برمجيات خارجية. وتتطلب المصارف أنظمة ملائمة لإدارة المعلومات والسعة المناسبة لخدمة عملائها. وإنه من الضروري بالنسبة للمصارف تخطيط حالات الطوارئ واستئناف العمل لضمان قدرتها على تقديم المنتجات والخدمات في الأحوال والظروف غير المواتية.

ت- **مخاطر تقنية:** هي المخاطر التي تتعلق بأي نتيجة غير مواتية، أو ضرر، أو خسائر ما، أو توقف العمل، أو التجاوز، أو مخالفة للنظام، أو خلل أو تعطل النظام، ناجم عن استخدام أو اعتماد أجهزة كمبيوتر، والبرمجيات، والأجهزة الالكترونية، وشبكات الانترنت بالإضافة إلى أنظمة الاتصالات. وإن مثل هذه المخاطر قد ترتبط أيضاً بتوقف النظام، وأخطاء المعالجة، وخلل في البرمجيات، وأخطاء التشغيل، وتعطل النظام، وعدم ملاءمة السعة، وضعف في المراقبة، وقصور في الحماية، والهجمات بقصد إلحاق الضرر، وحوادث الاختراق، وأعمال الاحتيال، والقدرة غير الملائمة على التعافي. ويجب على المصارف مراقبة كل عنصر وعملية تتعلق بأنظمتها المصرفية الالكترونية. ويمثل كل عنصر نقطة للمراقبة تؤخذ بعين الاعتبار. ويسري هذا أيضاً على العناصر المحتملة التي يجب تقييمها بطريقة مناسبة قبل تطبيقها في بيئة المصرفية الالكترونية. ويتأثر مستوى مخاطر العمليات بهيكل بيئة المعالجة للمنشأة ويشمل ذلك أنواع الخدمات المقدمة ومستوى تعقيد العمليات وتقنية الدعم.

ث- **مخاطر العمل:** في بعض الظروف، ونظراً لطبيعة مستخدم المصرفية الالكترونية الأكثر معرفة والأكثر تركيزاً على التكاليف والأسعار، ترتفع مخاطر المصرفية التقليدية مثل مخاطر الائتمان، ومخاطر سعر الفائدة، ومخاطر السيولة، ومخاطر أسعار الصرف الأجنبي.

ج- **مخاطر الاحتيال عبر الانترنت:** مع وجود التجارة/التداول عبر الانترنت، يجب أخذ مخاطر الاحتيال المباشرة عبر الانترنت بعين الاعتبار. فالتخطيط غير القانوني للتحايل مثل هجمات المواقع المزورة ورسائل البريد الالكتروني وتزوير العناوين التي تتطلب إفشاء معلومات شخصية سرية، وسرقة بيانات الهوية، وتصريحات الشركات الخاطئة تعرض المصرف لمخاطر عالية له ولعملائه. ويجب على

المصرف اتخاذ الإجراءات المناسبة لمنع حدوث خسائر نتيجة التعرض للاحتيال عبر الانترنت والقيام بالإجراء المناسب لحماية عملائه عالمياً حينما يحدث ذلك.

ح- **مخاطر السمعة:** تنشأ مخاطر السمعة نتيجة لرأي الجمهور السلبي. ويمكن أن تتضرر سمعة المصرف بواسطة الخدمات المصرفية الالكترونية التي تنفذ بشكل سيئ والتي تتسبب بطريقة أو بأخرى في نفور العملاء. ومن المهم أن يفهم العملاء ما يمكن أن يتوقعوه بشكل معقول من المنتج أو الخدمة، وما هي المخاطر والفوائد الخاصة التي تترتب عليهم عند استخدامهم لهذه المنتجات أو الخدمات. ويمكن أن يساعد مستوى تثقيف العميل والاستجابة الرسمية للحادث العرضي وإجراءات الإدارة على تقليل مخاطر السمعة للمصرف. ويطلب من المصارف التواصل بطريقة شفافة وواضحة والوفاء بالتزاماتها بهذا الخصوص. وعلى مجلس الإدارة، أو الإدارة العليا الاتفاق على إستراتجية التواصل ومضمونها.

خ- **مخاطر قانونية:** هي مخاطر تتعلق بالمكاسب أو رأس المال وتنشأ من الانتهاكات أو عدم الالتزام بالقوانين والأنظمة واللوائح والمعايير الأخلاقية. وتزيد الحاجة لضمان التوافق بين الإعلانات الورقية والالكترونية والإفصاحات والإشعارات من احتمال حدوث مخالفات قانونية. وتساعد عملية المتابعة المنتظمة لمواقع المصرف الالكترونية على ضمان الالتزام بالقوانين والأنظمة واللوائح السارية.

إن مجلس الإدارة والإدارة العليا مسؤولان عن إدارة المخاطر المذكورة أعلاه، ويجب عليهما ضمان أن إدارة مخاطر المصرفية الإلكترونية جزء لا يتجزأ من إدارة مخاطر المصرف بشكل عام. ونتيجة لذلك، يجب تعزيز وتنفيذ السياسات وإجراءات إدارة المخاطر والضوابط الداخلية والمراجعه الداخلية للحسابات ذات الصلة وفق ما يتطلبه نظام إدارة مخاطر المؤسسة المالية بشكل يناسب خدمات المصرفية الالكترونية. وعلاوة على ذلك، يجب على المجلس أو لجنته المختارة ضمان أن أنظمة وضوابط إدارة مخاطر المصرف يتم تعديلها وتحسينها حسب ما هو ضروري لكي تواجه المشاكل المصاحبة للمصرفية الالكترونية.

4-4 طرق إدارة المخاطر

إن الطبيعة المفتوحة والمعقدة للبنية التحتية لتقنية المعلومات خصوصاً المستخدمة بواسطة الانترنت (مثال: مخاطر مصاحبة لاستخدام الانترنت، مخاطر ذات صلة بالشركاء في سلسلة تقديم الخدمات مثل مزودي الاتصالات، بائعي ومقدمي الأنظمة، ومقدمي المنتجات والخدمات) هي الأسباب الرئيسة التي توجب على المصارف إنشاء إطار عمل سليم لإدارة المخاطر.

يجب تغطية جميع الأعمال ذات الصلة ومجالات التشغيل والدعم التي لديها مسؤوليات لإدارة مخاطر التقنية على الخطوط أو المستويات الوظيفية.

إن مجلس الإدارة وجميع مستويات الإدارة مسؤولون وخاضعون للمساءلة عن إدارة ومراقبة المخاطر التقنية (الفعلية والمستقبلية).

بما أنه يتعين على الإدارة العليا الإشراف على جميع مهام إدارة المخاطر؛ لذلك يجب عليها وضع عمليات لإدارة المخاطر.

وهذه المسؤولية تتطلب أن تقوم المصارف بعملية تحديد وتقييم المخاطر من خلال فحص مجموعة من المخاطر ذات الصلة وتحليل اثر المخاطر المختلفة على أنظمة وعمليات أعمالها.

يجب تقويم وتحديد الأولوية للمخاطر التي تعتبر جسيمة بالنسبة للمنشأة بشكل عميق؛ لكي يتسنى إعداد إستراتيجية للتعامل مع هذه المخاطر والتخفيف من حدتها.

4-4-1 تحديد المخاطر

إن المخاطر النموذجية المصاحبة لخدمات المصرفية الالكترونية ليست في الحقيقة جديدة، ولكن الطرق المختلفة التي تنشأ من خلالها بعض المخاطر وحجمها وآثارها المحتملة تتخذ أبعاداً جديدة. ومن ناحية أخرى، فإن المخاطر الأمنية مثل تلك التي تتجلى في عمليات الهجوم لقطع الخدمة عن المستخدمين، ليس لها سابقة أو مقابل في الطريقة التقليدية لتنفيذ الأعمال، قد تسبب انقطاعاً حاداً في عمليات المصرف مما يؤدي لخسائر فادحة لجميع الأطراف المتضررة.

يجب أن تغطي عملية تحديد المخاطر تعيين جميع أنواع التهديدات ونقاط الضعف والانكشاف الكامنة في هيكل المصرفية الالكترونية وجميع المكونات مثل الشبكات الداخلية والخارجية، والأجهزة، والبرامج، والتطبيقات البرمجية، والعمليات، والعناصر البشرية وخصوصاً أثر سوء التصرف البشري. وعلاوة على ذلك، يجب أن تغطي عملية تحديد المخاطر بيئة المصرفية الالكترونية المباشرة بالإضافة إلى أنظمة الدعم والمهام والاعتماد الفردي المتبادل من أجل الحصول على تقرير ملائم لحجم المخاطر.

يجب تقييم وحل المخاطر ذات الصلة بعملية إطلاق منتجات أو خدمات جديدة أو إجراء تعديلات أساسية للمنتجات والخدمات الموجودة خلال مراحل عملية وضع التصورات والتطوير. ويجب أن تكون هناك إجراءات التحكم بالمخاطر وإجراءات أمنية قبل أو خلال مرحلة التطبيق.

يجب على الإدارة تحديد وتصنيف وتقييم المخاطر ذات الصلة بعمليات المصرف على النحو التالي:

أ- اعتماد صيغة لتصنيف المخاطر.

ب- تحديد خطة تشمل السياسات والممارسات والإجراءات لمعالجة هذه المخاطر والتحكم بها.

ت- تنفيذ الخطة.

ث- متابعة المخاطر ومدى فعالية الخطة على أساس مستمر.

ج- تحديد عمليات لعمل اختبارات منتظمة وتحديث الخطة لمراعاة التغييرات التي تحدث في التقنية والتطورات القانونية وبيئة العمل (وتشمل التهديدات الخارجية والداخلية لأمن المعلومات).

4-4-2 تحليل المخاطر وتحديد حجمها

إن هذه المرحلة عبارة عن تحليل وفهم وتحديد حجم الأثر المحتمل وتبعات المخاطر التي تم تحديدها على العمل والعمليات بشكل عام: تحديد الأولوية للمخاطر، والقيام بتحليل تكلفة المنفعة واتخاذ قرارات لتخفيف حدة المخاطر.

4-4-3 معالجة المخاطر

يجب على الإدارة تقييم حجم الأضرار والخسائر التي قد يتحملها المصرف عند وقوع مخاطر معينة ذات صلة. ويجب على المصارف استيعاب أي خسائر ذات صلة قد تحدث من دون تعريض سلامتها المالية واستقرارها للخطر.

يجب موازنة تكاليف التحكم بالمخاطر والتخفيف من حدتها مقابل الفوائد التي يمكن تحقيقها. ويجب أن تتخذ الإدارة قرارا يتعلق بالموارد التي تخصص لمهمة المراقبة والانخفاض المتوقع للحوادث، على سبيل المثال: انخفاض احتمالية حدوث المخاطر.

إنه من المهم التأكد من فعالية الضوابط الداخلية بما في ذلك فصل المهام، والرقابه الثنائية والمطابقة. إن ضوابط أمن المعلومات، بشكل خاص، أصبحت أكثر أهمية حيث تتطلب وجود إجراءات إضافية، وأدوات، وخبرات، واختبار. ويجب على المؤسسات تحديد مستوى الضوابط الأمنية المناسبة بناءاً على تقييمها للخدمة التي تقدمها ، وعلى حساسية المعلومات بالنسبة للعميل والمؤسسة، وعلى مستوى تحمل المخاطر القائم للمؤسسة.

يجب على المصارف ألا تقدم أي منتج أو خدمة المصرفية الالكترونية عندما لا يمكن تنفيذ الضوابط الضرورية وإجراءات الأمن بشكل ملائم.

4-4-4 متابعة المخاطر ومراجعتها

لمواجهة التغير المستمر الحاصل في بيئة المصرفية الالكترونية يجب على الإدارة إنشاء إطار عمل لمتابعة المخاطر والالتزام على أساس مستمر للتأكد من أداء وفعالية إجراءات إدارة المخاطر.

وفي أي وقت تتغير فيه مؤشرات المخاطر، يجب تحديث إجراءات المخاطر وتعزيزها وفقاً لذلك. ويجب القيام باختبارات روتينية ومراجعة نظامية لكفاءة وفعالية إجراءات إدارة المخاطر والضوابط المصاحبة والإجراءات الأمنية السارية.

وينصح كثيراً بأن يقوم المصرف بإجراء برنامج تقييم شامل للمخاطر بواسطة طرف ثالث سنوياً.

4-4-5 ملخص

إن أثر المصرفية الالكترونية على إدارة المخاطر معقد ومتغير. ويجب على الإدارة إعادة تقييم وتحديث طرق مراقبة المخاطر وتخفيفها لتأخذ بعين الاعتبار الظروف المختلفة والتغيرات في حجم مخاطرها في بيئة الانترنت.

5- مبادئ إدارة المخاطر:

تصادق مؤسسة النقد العربي السعودي على "مبادئ إدارة المخاطر المصرفية الالكترونية" (http://www.bis.org/pub/bcbs98.htm) الصادرة عن لجنة بازل للرقابة المصرفية (BCBS). ويجب على المصارف أن تأخذ بعين الاعتبار متطلبات هذه المبادئ عند وضع سياساتها وإجراءاتها للمصرفية الالكترونية.

إن المبادئ الموضحة أدناه تعتمد بشكل رئيس على مبادئ لجنة بازل للرقابة المصرفية، وتتضمن بعض الإسهابات الهادفة وتحدد المتطلبات الدنيا التي يتعين على المصارف الالتزام بها.

5-1 مبادئ 3-1: إشراف المجلس والإدارة:

مبدأ 1:

يجب على مجلس الإدارة والإدارة العليا إنشاء إدارة إشراف فعالة تشرف على المخاطر المصاحبة لنشاطات المصرفية الالكترونية، ويشمل ذلك إحداث عملية مساءلة محددة وسياسات وضوابط لإدارة هذه المخاطر.

يجب على كل من الإدارة العليا للمصرف ومجلس الإدارة وضع تعليمات واضحة وتقديم الدعم الإداري الضروري للمبادرات الأمنية للمصرفية الالكترونية.

وهذا يشمل:

- تعزيز الأمان والأمن السليم داخل المنشأة من خلال الالتزام المناسب وتخصيص الموارد الكافية.
- اعتماد جميع السياسات والإجراءات ذات الصلة بإدارة مخاطر المصرفية الالكترونية.
- مراجعة ومتابعة المعلومات التي تتعلق بالحوادث الأمنية.
- إنشاء وحدة منفصلة داخل إدارة "إدارة المخاطر" مخصصة لإدارة مخاطر المصرفية الالكترونية، وترتبط مباشرة بكبير مسئولي المخاطر/ مدير إدارة المخاطر.
- تطوير خطة اتصالات داخلية وخارجية من أجل رفع مستوى ثقافة الأمن للمصرفية الالكترونية.
- امتلاك القدرة على الوقاية والاستجابة للاحتيال عبر الانترنت وعمليات الإساءة إلى هوية الشركات.
- التشجيع على وجود برنامج شامل لتوعية وتثقيف العملاء.

المبدأ 2:

على مجلس الإدارة والإدارة العليا أن يراجعا ويعتمدا الجوانب الرئيسة لعملية الرقابة الأمنية للمصرف.

وتعتبر الإدارة العليا مسؤولةً عن مطابقة الضوابط الأمنية مع الاحتياجات الكلية للمؤسسة. ولذلك، على الإدارة العليا أن تراجع وتعتمد بشكل منتظم سياسات أمنية و إجراءات ومبادرات جديدة تشمل ما يلي:

- سياسة أمن معلومات.
- مبادرات رئيسة لتحسين أمن المعلومات.
- كفاءة عمليات الرقابة الأمنية.
- مصداقية واتساق الأنظمة المصرفية الإلكترونية قيد الاستخدام.
- برامج توعية وتثقيف العميل.
- منهجية الاستجابة ضد الاحتيال الإلكتروني وحالات إساءة استخدام العلامة التجارية.
- التغيرات الهامة في التقنية وإطلاق الخدمات والمنتجات الجديدة.
- تقييم كفاءة عمليات الرقابة الأمنية المطبقة لأنشطة الخدمات المصرفية الإلكترونية.
- عملية إدارة الحدث وخطة التواصل للموظفين والعملاء ومؤسسة النقد.

المبدأ 3:

على مجلس الإدارة والإدارة العليا وضع دراسات تحليلية شاملة ومستمرة وإجراءات للإشراف على إدارة علاقات إسناد مهام لأطراف خارجية يقوم بها المصرف وكذلك البرامج الأخرى التابعة لطرف ثالث لدعم الخدمات المصرفية الإلكترونية.

وإذا كان المصرف يعتمد على مقدمي خدمات طرف ثالث لتقديم الخدمات المصرفية الإلكترونية، فعلى الإدارة أن تستوعب بشكل عام برنامج أمن المعلومات الخاص بمقدم الخدمات لكي تقيم قدرة الأنظمة الأمنية على حماية بيانات المصرف وعملائه بشكل فاعل. وتبقى المصارف مسؤولةً عن نقاط ضعف أنظمتها، وينطبق هذا بشكل خاص على الحلول المقدمة من جهاتٍ خارجية.

ترتبط المخاطر التالية بالخدمات المقدمة من أطراف خارجية (قائمة غير شاملة وليست ذات أولوية) ويجب تحليلها قبل ارتباط المصرف بعقد من هذا القبيل:

- فقدان السيطرة
- العوائق الكبرى للخروج
- التعرض لمخاطر لمقدمي الحلول وتشمل:
  - المتانة المالية
  - فقدان الالتزام بعملية إسناد خدمات لجهات خارجية
  - البطء في التنفيذ

- عدم توفر المزايا المطلوبة
- نقص الاستجابة
- رداءة جودة الخدمات اليومية

- أن يصبح ضحية رسوم "الاستخدام المفرط"
- صعوبات في حساب الوفورات
- تكاليف التحويل
- الاهتمام المطلوب من الإدارة العليا
- قيود التوريد
- احتمال التقييد بتقنية ذات عيوب
- الاهتمام بالمرونة بعيدة الأمد وتلبية التغيرات في متطلبات تغير الأعمال في الوقت المناسب
- المخاوف المتعلقة بمزايا التكلفة المستمرة للإسناد الخارجي
- الإضرار بصورة الشركة
- مطالبات مسؤولية محتملة
- عدم الوضوح في الملكية والتبليغ والرقابة
- مخاوف بخصوص قبول الصناعية المصرفية
- عدم كفاية جودة الخدمات التقنية

5-2 المبادئ 4-10: الضوابط الأمنية:

المبدأ 4:

يجب على المصارف تبنى إجراءات مناسبة للتأكد من صحة هوية وتخويل العملاء الذين تقدم الخدمات لهم على الانترنت.

ومن أجل خدمات مصرفية آمنة وسليمة، فمن المهم التأكد من شرعية أي عملية أو طلب دخول إلى النظام. ولذلك على المصرف أن يستخدم طرقاً موثوقة للتأكد من صحة هويات وتفويض العملاء الجدد والحاليين. وفي هذا الشأن، فقد تم تقديم بعض الطرق إلى المصارف في تعميم منفصل (رقم 40690 وتاريخ 6-8-2009).

وعلى المصارف أثناء تواصلهم بالعملاء ألا يبدوا انطباعاً بأن الخدمات المصرفية الإلكترونية آمنة بالكامل، ويجب عليهم توعيتهم بمخاطر المصرفية على الانترنت.

المبدأ 5:

على المصارف أن تستخدم طرقاً لتوثيق العمليات التي تعزز عدم الإنكار وتنشئ المساءلة عن العمليات المصرفية الإلكترونية.

تشمل طريقة عدم الإنكار التقنية إنشاء دليل للمنشأ أو تقديم المعلومات الإلكترونية لحماية:

- المرسل من الإنكار الزائف بواسطة المتلقي بأنه تم استلام البيانات.
- المتلقي من الإنكار الزائف بواسطة المرسل بأنه تم إرسال البيانات.

وعلى المصارف أن تطبق الطرق التي تشمل تسجيلاً آمناً وموثوقاً وختماً زمنيا.

المبدأ 6:

على المصارف التأكد من وجود إجراءات مناسبة لتعزيز الفصل الملائم في أنظمة الخدمات المصرفية الإلكترونية وقواعد البيانات والبرامج التطبيقية.

ويعد فصل المهام مهماً للخدمات المصرفية الإلكترونية الآمنة والسليمة. ومن هذا المنطلق، يطلب من المصارف أن تضع إجراءات رقابية داخلية مصممةً لتقليل مخاطر الاحتيال في الأنظمة والعمليات التشغيلية، ولضمان أن العمليات والأجهزة مصرحة ومسجلة ومحمية بشكل مناسب فعليها:

- وضع وتوثيق إجراءاتٍ لتحديد المهام التي يجب فصلها.
- مراقبة الإجراءات لضمان الالتزام بقواعد الفصل.
- يجب تحديد ثلاث فئات من المهام:
  - التفويض: مسؤولية تكليف شخص/أشخاص بمهمة.
  - الحفظ: مسؤولية تخويل شخص بتخزين البيانات.
  - حفظ السجلات ومطابقتها: مسؤولية تخويل شخص بحفظ السجلات ومطابقتها.

المبدأ 7:

على المصارف أن تضمن وجود ضوابط توثيق مناسبة وامتيازات دخول ملائمة لأنظمة الخدمات المصرفية الإلكترونية وقواعد البيانات والبرامج التطبيقية.

يمكن أن يؤدي الدخول بدون امتياز خاص إلى أنظمة الخدمة المصرفية الإلكترونية (قواعد البيانات/برامج تطبيقية) إلى حوادث ذات تأثيرات عالية. ومن هذا المنطلق، يجب أن يكون لدى المصارف ضوابط دخول ملائمة، وتشمل التالي:

- لا تمنح امتيازات الدخول إلا للأشخاص الذين بحاجة للدخول إلى نظام محدد.
- لا يسمح للمدققين (المراجعين) إلا بتأدية المهام التي يفوض المستخدمون العاديون والمدققون بأدائها فقط، وليست الخاصة بالمشغلين.
- يجب أن يكون لدى المصرف إجراء موثق ومعتمد بصورةٍ جيدة يصف عملية التصديق (التوثيق). ويجب أن تتم عملية إعادة التصديق على أساسٍ منتظم، وأن تقوم الجهات الإدارية بالتحقق من حاجة الفرد للاحتفاظ بالامتيازات.
- في الحالات التي لا يتمكن فيها المدراء من تنفيذ مهامهم، ويتوجب تحويل سلطتهم إلى أشخاصٍ آخرين، فيجب أن يوفر إجراء الطوارئ سجلات كافية وإعطاء إشعار إلى الإدارة العليا عن عملية الاستبدال. ويجب أن تكون الإدارة قادرة على أن تبطل أو تسيطر على عملية الاستبدال.
- يجب التبليغ عن جميع أنشطة الأشخاص ذوي الامتيازات في سجلات التدقيق.
- يجب مراجعة جميع القيود والسجلات ووقائع النظام والإشعارات بشكل دوري، ويجب التحقيق بشكل كامل في أي عملية إساءة استخدام.

المبدأ 8:

على المصارف أن تضمن وجود إجراءات مناسبة لحماية سلامة البيانات لعمليات وسجلات ومعلومات الخدمات المصرفية الإلكترونية.

تعتبر سلامة بيانات العمليات والسجلات والمعلومات جوهرية للخدمات المصرفية الإلكترونية الآمنة والسليمة. وقد يعرض عدم المحافظة على سلامة البيانات المصارفَ لخسائر مالية وكذلك مخاطر سمعة وقانونية. وفيما يخص االتعرض للمخاطر العالية، فعلى المصارف أن تخطط وتدخل أساليب تنظيمية وإجرائية وتقنية مناسبة تضمن سلامة بيانات العمليات والبيانات المالية والمحافظة عليها:

- يجب أن تكون هناك آليات لاكتشاف الاختلافات (المشاكل) وأن تضمن تخطيط الإجراءات التصحيحية واتخاذها بشكل جيد.
- يجب على البيانات المالية أن:
  - تعكس القيم الحقيقة موضوع العملية
  - يتم نشرها في وقتها
  - يتم تخزينها بشكل آمن
  - تكون جاهزة للاستعادة لغرض الاستفسار أو التبليغ
  - تكون محمية ضد التغيير غير المناسب

المبدأ 9:

على المصارف أن تضمن وجود مسارات تدقيق Audit Trails واضحة لجميع عمليات الخدمات المصرفية الإلكترونية.

إن تقديم الخدمات المالية على الانترنت يزيد من صعوبة تطبيق وتنفيذ الضوابط الداخلية. لذلك، فعلى المصارف أن تحرص أن يكون نظام الضوابط الداخلية متوائماً مع خدمات ومنتجات المصرفية الإلكترونية وأن يتم المحافظة على مسارات تدقيق واضحة.

علاوةً على ذلك، يجب أن تكون الضوابط الداخلية قابلة للتدقيق المستقل بواسطة مؤسسات خارجية.

يشترط بمسارات التدقيق:

- أن توفر أدلة كافية لإثبات تدفق العمليات، من البداية حتى النهاية، وأي أداء رقابي/إجرائي مصاحب لها.
- أن تكون كافية لتلبية متطلبات لوائح المحاكم التي قد تستخدم بموجبها.

يتوجب استخدام الإجراءات الفنية مثل الترميز والتوقيعات الرقمية ورموز رسائل التوثيق لحماية سلامة سجلات مسارات التدقيق. علاوةً على ذلك، يجب الاحتفاظ بنسخة إلكترونية لدليل التلاعب لمسارات التدقيق.

المبدأ 10:

على المصارف أن تتخذ إجراءات مناسبة للحفاظ على سرية المعومات الرئيسة الخاصة بالخدمات المصرفية الإلكترونية. ويجب أن تتناسب تلك الإجراءات المتخذة مع درجة حساسية المعلومات المرسلة و/أو المخزنة في قواعد البيانات.

تمثل بداية الخدمات المصرفية الإلكترونية مزيداً من التحديات الأمنية للمصارف حيث أنها تزيد تعرض المعلومات المرسلة على الشبكة العامة أو المخزنة في قواعد البيانات للدخول إليها من قبل أطراف غير مخولة أو مرغوبة، أو تستخدم في غير الطرق التي يقصدها العميل موفر المعلومات. بالإضافة إلى ذلك، إن الاستخدام المتزايد لمقدمي الخدمات قد يكشف بيانات جوهرية خاصة بالمصارف لأطرافٍ أخرى.

ومن هذا المنطلق، يجب أن تظل البيانات الرئيسة خاصة بالمصرف، لأن أي سوء استخدام سيعرض المصرف لمخاطر قانونية ومخاطر سمعة ذات أثر بالغ.

يجب أن تتناسب حماية السرية مع أثر مخاطر االتعرض غير المخول:

- يجب المحافظة على السرية باستخدام ضوابط الدخول والترميز.
- يجب أن تعتمد تقنيات التشفير على لوغاريتمات معترف بها لا غبار على قوتها واستخدامها.
- يجب أن يعتمد تصريح الدخول على مبدأ "الحاجة للمعرفة" فقط.

5-3 المبادئ 11-14: إدارة المخاطر القانونية ومخاطر السمعة:

المبدأ 11:

على المصارف أن تضمن توفير معلومات كافية على مواقعها الإلكترونية قبل الشروع في عمليات مصرفية إلكترونية لتمكين العملاء المحتملين من الوصول إلى استنتاج مطلعٍ عن هوية المصرف ووضعه التنظيمي.

تطلب مؤسسة النقد من جميع المصارف حماية العملاء ضد المواقع الإلكترونية الاحتيالية:

- يجب تطبيق مجموعة من إجراءات توثيق الهوية للأشخاص لتجنب الحصول على بيانات توثيق الهوية الخاصة بالعميل ومعلوماته المالية.
- يجب تطبيق ضوابط لحماية السجلات الهامة والمعلومات من الفقدان والتخريب والتزوير.

يجب على المصارف توعية العميل بمخاطر المواقع الإلكترونية الاحتيالية، وهي مهمة في عملية تثقيف العميل. وبهذا الخصوص، ينصح باستخدام شهادات SSL ومحدد مواقع منتظم URL ورابط معروف إلى المصرف (أي في مطبوعات المصرف المنشورة).

المبدأ 12:

على المصارف أن تتخذ إجراءات ملائمة لضمان الالتزام بمتطلبات خصوصية العميل السارية في البلدان التي يقدم لها المصرف المنتجات والخدمات المصرفية الإلكترونية.

على المصارف ضمان أن توفير الخدمات لأية دولة يأخذ بالاعتبار أي ضمانات إضافية ضرورية لحماية خصوصية العميل (والمصرف) في تلك الدولة، وقد لا تكون أنظمة خصوصية البيانات متشابهة في جميع أنحاء العالم، ولكن الأنظمة التي يخضع لها عمل المصرف وعملاؤه تتطلب حماية متساوية. وقد يفرض التشريع الخارجي ضوابط ليست مطلوبة في التشريع المحلي.

على المصارف الراغبة في الدخول في أنشطة الخدمات المصرفية الإلكترونية عبر الحدود أن تفهم التحديات والمخاطر المرتبطة بمثل تلك الأعمال وأن تتخذ إجراءات كافية لإدارة تلك المخاطر بكفاءة.

المبدأ 13:

يجب أن تكون لدى المصارف قدرة فاعلة، واستمرارية أعمال و إجراءات تخطيط للطوارئ فاعلة للمساعدة في ضمان توفر أنظمة وخدمات المصرفية الإلكترونية.

ويتوقع من المصارف أن تضع خططاً للمحافظة على عمليات الأعمال أو استعادتها في سلم زمني مناسب في أعقاب توقف أو تعطل عمليات الأعمال الخطره.

ويجب أن تكون جميع خطط الطوارئ جزءاً من إطار ثابت للاستمرارية الأعمال.

يجب في كل عملية أن:

- تحدد الأولويات للاختبار والصيانة.
- تحدد بوضوح ظروف تفعيلها، وكذلك الأشخاص المسؤولين عن تنفيذ كل عنصر من الخطة.
- تحدد المسؤوليات وإجراءات الطوارئ وتوافق عليها.
- تتضمن الاختبارات النظامية وتحديثات الخطة.

علاوةً على ذلك، على المصارف أن تضع خطة ملائمة لمعالجة الكوارث ، تشمل على الأقل ما يلي:

- بنية تحتية مسانِدة خارج الموقع.
- إجراء تعافي من الكوارث موثق ومجرب.
- اختبارات منتظمة لضمان أن تكون معالجة الكوارث ضمن الحد الأقصى لوقت الانقطاع المسموح به (يحدده المصرف).

تطلب مؤسسة النقد العربي السعودي من المصارف أن تضع خططاً للقدرات (قابلة للقياس) لضمان مواكبة نمو الخدمات المصرفية الإلكترونية مستقبلاً. وعلى المصارف أن تضع تخطيط قدرات ملائم لدعم نمو العمليات بأوقات استجابة معقولة. ويكون التخطيط مركزاً على مستوى القدرات المراد توفيره في كل مرحلة من مراحل الإنتاج أو توفير الخدمة. ويعالج تخطيط القدرات مسألة التحميل/حجم الأعمال غير المتوقعة بسبب نمو الأعمال الإلكترونية لتوفير بنية ونظام منافسين بتكلفة اقتصادية.

يجب أن تشمل خطة بناء القدرات على المدى البعيد والمتوسط والقريب على ما يلي:

- قدرة التخزين المتوقعة الخاصة بالنظام وحجم البيانات المسترجعة والمنشأة والمخزنة خلال دورة ما.
- عدد العمليات الجارية والتنافسية التقديرية المحتملة.
- الأداء المطلوب والاستجابة المطلوبة من كلٍ من النظام والشبكة، أي الأداء من النهاية إلى الأخرى.
- مستوى المرونة المطلوبة ودورة الاستخدام التي تم التخطيط لها– الذروة والدنيا والوسطى.
- أثر إجراءات الأمن مثل ترميز وفك ترميز جميع البيانات.
- الحاجة إلى عمليات مستمرة (365x7x24) وإمكانية إيقاف النظام للصيانة وأعمال إصلاح أخرى.
- الفائض الذي يتعين إنشاؤه في البنية التحتية لتخطيط النظام.

يجب تحديد علامة بداية لاستخدام موارد النظام في وقت تخطيط القدرات.

المبدأ 14:

يجب على المصارف وضع خطط الاستجابة المناسبة لإدارة واحتواء والحد من المشاكل الناجمة عن أحداث غير متوقعة، بما في ذلك الهجمات الداخلية والخارجية، التي قد تعيق توفير الأنظمة والخدمات المصرفية الإلكترونية.

وترى مؤسسة النقد العربي السعودي أن الإدارة الملائمة للحوادث مهمة للمصرفية الإلكترونية الآمنة والسليمة في المملكة العربية السعودية.

يجب على المصارف تشجيع الإبلاغ عن الحوادث من جميع الأطراف وخاصة من العملاء. ويجب عليها استحداث قسم خاص في مواقعها على الانترنت لهذا الغرض.

وتنصح المصارف بقوة بوضع خطط الاستجابة للحوادث، بما في ذلك كحد أدنى:

• آلية للكشف عن الحوادث في أسرع وقت عند حصولها، وتقييم خطورتها، والسيطرة على المخاطر المرتبطة بأي خلل في الخدمة (وخاصة التركيز على مخاطر السمعة).

• أن يكون لديها القدرة على حماية عملائها على الانترنت من الاحتيال عبر الإنترنت.

• أن يكون لديها القدرة على حماية هويتهم عبر الإنترنت من الاستخدام غير المشروع.

• أن يكون لديها القدرة على منع وكشف والرد على محاولات الاحتيال عبر الإنترنت وإساءة استخدام العلامة التجارية.

• إجراءات موثقة ومختبرة تضمن ردود فعل سريعة لاكتشاف الحوادث والحد من احتمال تكرارها.
• خطة اتصالات لضمان إبلاغ جميع الأطراف الخارجية ذات الصلة، بما في ذلك عملاء البنك، والأطراف الأخرى المشتركة ووسائل الإعلام، في الوقت المناسب وبطريقة مناسبة بخصوص الأعطال الخطيرة في المصرفية الإلكترونية وتطورات استئناف الأعمال دون إحداث أي ذعر في أذهان الجمهور.

• وضع خطة تدريبية للموظفين لضمان تدريبهم بشكل كاف على تحليل أنظمة الكشف عن الحوادث والاستجابة لها، وتفسير أهمية النتائج ذات الصلة.

بالإضافة إلى ذلك، يجب وضع إجراءات وتحديد مسؤوليات إدارة الحوادث لضمان الاستجابة السريعة والفعالة وفي الوقت المناسب للحوادث الأمنية. وعلاوة على ذلك، يشجع تبادل المعلومات وتبادل الخبرات بين المصارف والأطراف الأخرى. كما تشجع مشاركة المصارف في مبادرة الاستجابة للحوادث التي تديرها اللجنة المصرفية لأمن المعلومات.

الملحق 1

المصطلحات

الإدارة العليا

يقصد بالإدارة العليا أي شخص يشغل منصب مدير عام فما فوق.

التوثيق

خاصية من خصائص برنامج أمن الانترنت الذي يعمل على التحقق من هوية الشخص أو نوع العملية.

عرض النطاق الترددي

كمية البيانات التي يمكن أن ترسل في فترة محددة من الزمن. بالنسبة للأجهزة التمثيلية، يحدد النطاق الترددي حسب الدورة في الثانية، أو الهرتز. وبالنسبة للأجهزة الرقمية، عادة ما يتم تحديد النطاق الترددي حسب البت في الثانية أو للبايت في الثانية الواحدة.

البت في الثانية (bit)

الوحدات التي يتم بموجبها قياس سرعة إرسال البيانات عندما تنتقل البتات (bits) عبر وسائل الاتصالات.

النطاق العريض

أحد وسائط إرسال البيانات يتم من خلال وسيلة واحدة (عادة سلك) يتم فيه نقل عدة قنوات عبر وسيلة واحدة. وعلى سبيل المثال، يستخدم كيبل التلفزيون إرسال النطاق العريض.

المتصفح

برنامج يستخدم للوصول إلى وعرض وثائق من الشبكة العنكبوتية وغيرها من موارد الانترنت. وتشمل المتصفحات المشهورة نتسكيب وانترنت اكسبلورر.

سجل المتصفح (cookie)

حزمة من المعلومات التي يتم إرسالها بواسطة خادم المتشعب (HTTP) إلى متصفح العميل ثم يقوم المتصفح بإعادة إرسالها في كل مرة يتصل العميل بالخادم. وعادة ما يتم استخدامها لتحديد وتعقب مستخدم مسجل في موقع على شبكة الانترنت دون الحاجة إلى تسجيل الدخول في كل مرة يقوم بفتح هذا الموقع.

اسم النطاق

هو الجزء من أسم الانترنت الذي يحدد موقع حاسبوك في العالم، يكتب على شكل سلسلة من الأسماء المفصولة بنقاط.

التشفير

ترميز البيانات التي تمر عبر الإنترنت لحمايتهما من الإطلاع عليها من قبل أشخاص غير مخولين.

FB's

تعني البنوك الأجنبية

جدار الحماية (Firewall)

مقياس أمني على شبكة الإنترنت لحماية المعلومات، أو منع الوصول إلى، أو ضمان عدم قدرة المستخدمين على القيام بأي ضرر لأنظمة الكمبيوتر الأساسية. وكثيرا ما تستخدم جدران الحماية لمنع مستخدمي الانترنيت غير المرخص لهم من الدخول إلى الشبكات الخاصة المتصلة بشبكة الإنترنت، وخاصة الشبكات الداخلية (انترانيت). إن جميع الرسائل التي تدخل وتخرج من الشبكة الداخلية تمر عبر جدار الحماية الذي يقوم بفحص كل رسالة ويحجب تلك التي لا تلبي المعايير الأمنية المحددة.

بروتوكول نقل الملفات

بروتوكول نقل الملفات، هو أحد البروتوكولات على شبكة الإنترنت، يتيح نقل فعال جدا لملفات كاملة من البيانات بين أجهزة الكمبيوتر.

بروتوكول نقل **النص الفائق (HTTP)**

(Hyper Text Transport Protocol)

مجموعة من القواعد التي توفر وسائل الاتصال ونقل ملفات هايبرتكست على شبكة الويب العالمية. ويحدد برتوكول نقل النص الفائق كيفية تنسيق الرسائل وإرسالها، والإجراءات التي يجب على خوادم ومتصفحات

الويب اتخاذها استجابة للأوامر المختلفة. ويتطلب ذلك برنامج بروتوكول النص الفائق للعميل من جهة، وبرتوكول النص الفائق للخادم على الطرف المقابل. ويعتبر برتوكول نقل النص الفائق البروتوكول الأكثر شيوعا واستخداما في العالم. ويمكنك أن ترى النص المتشعب عادة في بداية كل عنوان على شبكة الإنترنت.

لغة رقم النص الفائق (HTML)

تعتبر لغة رقم النص الفائق عرفاً لإنشاء مستندات على شبكة الويب العالمية. وعادة تكون ملفات أتش تي أم أل(HTML) امتدادات HTML أو htm.

الرابط التشعبي

عنصر في وثيقة إلكترونية ترتبط بمكان يقود إلى قسم آخر في نفس الوثيقة أو إلى وثيقة مختلفة تماما. وعادة، تتم عملية الانتقال بالنقر على الرابط التشعبي.

الإنترنت

التنظيم العالمي لشبكات الحواسيب وتمتد في جميع أنحاء العالم، وتربط أجهزة الكمبيوتر مختلفة الأنواع والبروتوكولات. وتتيح شبكة الإنترنت نقل الملفات، وتسجيل الدخول عن بعد، والبريد الالكتروني، والأخبار، وغيرها من الخدمات. ولا تحتكر منظمة واحدة السيطرة على الانترنت.

موفر خدمة الإنترنت

هي المؤسسة التي توفر الخادم والبرامج المطلوبة للوصول إلى الإنترنت مقابل رسم.

إنترانت (الشبكة الداخلية)

شبكة داخلية خاصة تشبه الإنترنت داخل مؤسسة معينة، وعادة لا يسمح للجمهور غير المصرح له بالوصول إليها.

جافا

لغة برمجة مستخدمة لإنشاء برامج صغيرة (معروفة بتطبيقات)، ويتم تحميلها تلقائيا عندما تدخل موقع على

شبكة الانترنت معزز بلغة جافا. وقد طورتها شركة صن مايكروسيستمز، وتستخدم الآن في العديد من الألعاب على الإنترنت، وفي تصميم الصور.

البريد الإلكتروني غير المرغوب به أو سلسلة البريد

يسمى البريد الالكتروني التجاري غير المرغوب به ايضا "سبام" (spam).

تحتوي سلسلة رسائل البريد الإلكتروني (chain e-mail) على نفس صيغة الرسائل المرسلة عبر البريد، ولكن يتم إرسالها عن طريق شبكات البريد الإلكتروني بدلا من البريد العادي. وتعرف سلسلة الرسائل، أو سلسلة البريد الإلكتروني بأنها أي رسالة يتم إرسالها إلى واحد أو أكثر من الناس تطلب من المتلقي أن يحيلها إلى آخرين وتحتوي على بعض الوعود بالمكافأة لإحالتها أو التهديد بالعقاب لعدم القيام بذلك.

مودم

قطعة من المعدات التي تربط كمبيوتر بخط نقل بيانات – وعادة خط هاتفي. وعادة ما يستخدم الناس أجهزة المودم التي تنقل البيانات بسرعة تتراوح بين 1200 بت في الثانية إلى 19.2 كيلوبت في الثانية.

تحتوي الأجهزة اللاسلكية بعض القيود التي تزيد من مخاطر أمن المعاملات المعتمدة على الاتصال اللاسلكي التي قد تؤثر سلبا على معدلات قبول العملاء.

الجهاز الشخصي المصرفي

شكل من أشكال الخدمات المصرفية عبر الإنترنت التي تمكن العملاء من تنفيذ المعاملات المصرفية من خلال جهاز كمبيوتر عن طريق المودم. وفي معظم مشاريع الكمبيوتر الشخصي المصرفي، يقدم المصرف للعميل برنامج برمجيات مالية خاص يتيح للعميل إجراء العمليات المالية من جهاز كمبيوتره الشخصي في منزله. وثم يقوم العميل بطلب البنك عن طريق مودمه، ويحمل البيانات، ويشغل البرامج الموجودة على كمبيوتر العميل. تعرض العديد من المصارف حاليا أنظمة مصرفية حاسوبية خاصة تتيح للعملاء الحصول على أرصدة الحسابات وبيانات بطاقة الائتمان، ودفع الفواتير وتحويل الأموال بين الحسابات.

الاحتيال على الحسابات المصرفية (Phising)

القيام بإرسال بريد إلكتروني إلى مستخدم يدعي زورا أنه مؤسسة قانونية قائمة في محاولة للاحتيال على المستخدم للحصول على معلومات خاصة تستغل لسرقة الهوية. ويقوم البريد الإلكتروني بتوجيه المستخدم

بزيارة موقع ويب يطلب منه تحديث المعلومات الشخصية، مثل كلمات السر وبطاقات الائتمان، وأرقام الضمان الاجتماعي والحسابات المصرفية الخاصة الموجودة مسبقا بالمؤسسة الحقيقية. غير أن موقع الإنترنت مزيف وتم إنشاؤه لغرض سرقة معلومات المستخدم. كما يشار أيضا إلى التصيد بانتحال العلامة التجارية أو البطاقات، وهو نوع من "الخداع"، والفكرة هي زرع الطعم بهدف إيقاع البعض في الفخ وفي حين أن الكثيرين سيتجاهلون الطعم إلا أن البعض قد يغريه الطعم.

الهاتف المصرفي

تستخدم هذه الخدمة للوصول إلى شبكة (أو شبكات) المصرف باستخدام الهواتف المحمولة، وأجهزة النداء، والمساعدات الرقمية الشخصية (أو أية أجهزة مماثلة) من خلال شبكات شركات الاتصالات 'اللاسلكية. تكمل الخدمات المصرفية اللاسلكية المنتجات والخدمات المصرفية الإلكترونية (الإنترنت المصرفي).

رقم التعريف الشخصي (PIN)

رقم التعريف الشخصي. قد تستخدم بعض المصارف رقم التعريف الشخصي كمرادف لكلمة السر.

بروتوكول

مجموعة من القواعد لتبادل البيانات بين جهاز طرفي وكمبيوتر أو بين جهازي كمبيوتر.

بروكسي

جهاز يستخدم للوصول إلى الإنترنت من خلال الالتفاف حول جدار أمني وضع لضمان الأمن في نظام أو شبكة كبيرة.

البنية التحتية للمفتاح العام **PKI**

هو الاختصار للبنية التحتية للمفتاح العام، وهو نظام شهادات رقمية، وسلطات شهادات، وسلطات التسجيل الأخرى التي تتحقق من صحة هوية الأطراف المعنية وتصادق عليها في القيام بعملية عن طريق الإنترنت. وتتطور PKIs حاليا ولا توجد PKI واحدة ولا حتى أي معيار متفق عليه لإنشاء PKI.

محرك البحث

برنامج يتيح لك القيام بعمليات البحث عن طريق إدخال كلمة رئيسية للبحث عن معلومات على شبكة الانترنت.

شهادة الأمن

ملحق لرسالة إلكترونية تستخدم من قبل بروتوكول طبقة المقابس الآمنة (SSL) لإنشاء اتصال آمن والتحقق من هوية الفرد/المؤسسة.

الإدارة العليا :

أي شخص يتولى منصب مدير عام فما فوق.

العملية الإلكترونية الآمنة (SET)

إن العملية الإلكترونية الآمنة هي بروتوكول قياسي لضمان أمن عمليات بطاقات الائتمان عبر شبكات غير آمنة، وخاصة، شبكة الإنترنت. وقد تم تطوير بروتوكول SET من قبل فيزا وماستر كارد (تشمل شركات أخرى مثل GTE، آي بي إم ومايكروسوفت ونتسكيب) بدءا من عام 1996.

وتستفيد SET من استخدام تقنيات التشفير مثل الشهادات الرقمية والتشفير بالمفتاح العمومي للسماح للأطراف بالتعرف على بعضهم بعضا وتبادل المعلومات بشكل آمن.

وتم إنتشار بروتوكول SET بشكل كبير في أواخر التسعينات عندما اعتمد استخدام بطاقة الائتمان، ولكنها فشلت في كسب قبول كبير في السوق. وأسباب ذلك تشمل الحاجة إلى تنصيب برنامج العميل (المحفظة الالكترونية)، وتكلفتها وتعقيدها على التجار لتقديم الدعم، ووجود بديل بتكلفة أقل نسبيا ومناسب يعتمد على المقابس الآمنة (طبقة المقابس الآمنة SSL).

التجسس وحزمة التجسس (Sniffing, Packet Sniffing)

حزمة التجسس هي شكل من أشكال التنصت تطبق على شبكات الكمبيوتر بدلا من شبكات الهاتف. ولاقت رواجا مع شبكة إيثرنت، التي تعرف باسم شبكة "وسيط مشترك". وهذا يعني أن حركة المرور على قطاع تمر بكل المضيفين المرتبطين بهذا القطاع. وتحتوي بطاقات إيثرنت على مصفي (فلتر) يمنع جهاز المضيف من رؤية حركة المرور الموجهة إلى المحطات الأخرى. وتقوم برامج التجسس بإيقاف المصفي، وهكذا تكشف حركة الجميع.

الانتحال، مواقع الانتحال (Spoofing)

يعرف أيضا بانتحال العلامة التجارية أو البطاقات، هو نوع من "التصيد"، وهو شكل من أشكال جرائم الانترنت. والفكرة هي زرع الطعم بهدف إيقاع البعض في الفخ وفي حين أنه يمكن أن يفلت معظم الأشخاص من الطعم، إلا أن بعضهم قد يبتلعه.

طبقة المقابس الآمنة SSL

اختصار لطبقة المقابس الآمنة، وهو بروتوكول تم تطويره من قبل شركة نتسكيب لتمكين تمرير الاتصالات المشفرة والموثقة عبر الإنترنت. وتعمل طبقة SSL باستخدام مفتاح خاص لتشفير البيانات التي يتم نقلها عبر اتصال SSL. ويدعم كل من متصفح نتسكيب ومكتشف إنترنت إكسبلورر خدمة SSL، ويستخدم العديد من المواقع على شبكة الإنترنت البروتوكول للحصول على معلومات المستخدم السرية، مثل أرقام بطاقات الائتمان. وفي اتصال SSL، يجب على كل جانب من الاتصال حمل شهادة أمنية، يقوم برامج كل جانب بإرسالها إلى الآخر. ويقوم كل جانب بتشفير ما يرسله باستخدام معلومات من شهاداته، وشهادة الجانب الآخر، لضمان عدم تشفيرها إلا من قبل المتلقي المقصود، ويتأكد الطرف الآخر من أن البيانات جاءت من المكان الذي يدعي أنها أتت منه، وأن الرسالة لم يتم العبث بها.

الرمز Token:

الرمز في الحوسبة هو كائن افتراضي يتم تمريره بين الحواسيب أو أجهزة أخرى على الشبكة ويأذن لها على نحو مماثل بالتواصل. ولا يتصل إلا الجهاز صاحب الرمز لتجنب الصدام بأجهزة أخرى. في امن الحواسيب، تستخدم تقنية الرمز أجهزة ذات رقائق مدمجة تحتوي معلومات حول المالك لتحديد التصريح الأمني. ويمكن أن تكون الرموز سلاسل مفاتيح وأزرار ومجوهرات وبطاقات ذكية. والرمز في أسرة أنظمة تشغيل ويندوز هو كائن نظام يمثل موضوع عمليات مراقبة الدخول.

عنوان الموقع URL

محدد الموارد العالمي هو عنوان يحدد تماماً مورداً من موارد الشبكة العنكبوتية العالمية. ويتكون محدد الموارد من أربعة عناصر:

1- الخدمة – النص المتشعب HTTP أو بروتوكول نقل الملفات FTP أو غيرها
2- المضيف – الكمبيوتر الذي يعالج الموارد
3- رقم المنفذ (ليس ضرورياً في كثير من الأحيان لأنه يتوافق تلقائيا مع افتراضات الخدمة

المطلوبة).

4- المسار واسم ملف المورد.

صيغة محدد الموارد هي: service://hostport/path

الشبكة العنكبوتية العالمية WWW

الشبكة العالمية، كذلك تدعى الويب أو W3، هي نظام لخوادم الإنترنت تدعم وثائق تنسيق خاص. يتم تنسيق الوثائق بلغة تسمى HTML التي تدعم وصلات إلى وثائق أخرى، وكذلك الرسومات والصوتيات وملفات الفيديو. وهذا يعني أنه يمكنك أن تتحرك من وثيقة إلى أخرى ببساطة عن طريق النقر على النقط الساخنة. وليست كل خوادم الإنترنت جزءاً من الشبكة العنكبوتية العالمية.

الملحق 2

متطلبات ضوابط الأمن

يجب أن تحدد المصارف ما يلي من ضوابط أمنية مستقلة تحت مسؤولية الإدارة العليا: من أجل توضيح الموضوعات التي سيتم تناولها بصورة شاملة تم إدراج قائمة غير شاملة للضوابط أدناه تتبع المعيار الجديد ISO27001:

سياسة الأمن

هي الضوابط التي تقدم الدعم والتوجيه الإداري وتشمل ما يلي:

- وثيقة سياسة أمن المعلومات
- استعراض سياسة أمن المعلومات

تنظيم الأمن

هي الضوابط المتعلقة بإدارة أمن المعلومات داخل المؤسسة. وتغطي الضوابط المجالات التالية:

- التزام الإدارة بأمن المعلومات
- تنسيق أمن المعلومات
- توزيع مسؤوليات أمن المعلومات
- اتفاقيات السرية
- مراجعة مستقلة لأمن المعلومات

إدارة الأصول

هذه الضوابط موجودة لشرح ومراقبة وحفظ جميع الموجودات بشكل نظامي لتحظى جميع أجزاء النظام بمستوى من الحماية يتناسب مع أهميتها/قيمتها للمؤسسة. وتغطي الضوابط المجالات التالية:

- جرد الموجودات
- ملكية الأصول
- تصنيف الأصول
- وصف المعلومات ومناولتها

أمن الموارد البشرية

هذه الضوابط تغطي كافة الجوانب الأمنية المرتبطة بإدارة شؤون الموظفين التي تغطي المجالات التالية:

- الأدوار والمسؤوليات
- المراقبة
- شروط وظروف التوظيف
- مسؤوليات الإدارة
- الوعي بأمن المعلومات وتعليمه والتدريب عليه
- عملية التأديب
- مسؤوليات إنهاء العقود
- عائد الأصول
- إزالة حقوق الدخول

الأمن المادي والبيئي

هذه الضوابط تغطي الحماية المادية المباشرة للأصول والبيئات التي توجد فيها طيلة حياتها، بما في ذلك صيانتها والتخلص منها في نهاية المطاف، وتغطي المجالات التالية:

- محيط الأمن المادي
- ضوابط الدخول المادي
- مكاتب وغرف ومرافق الأمن
- حماية ضد التهديدات البيئية
- العمل في المناطق الآمنة
- مناطق دخول الجمهور وتقديم الخدمة والتحميل
- معدات الأمن

إدارة الاتصالات والعمليات

تغطي الضوابط المطلوبة لتشغيل النظام بطريقة آمنة بما يتناسب مع مستوى الحماية. وتشمل المجالات التالية:

- إجراءات تشغيل موثقة
- إدارة التغيير
- الفصل بين الواجبات
- الفصل بين المرافق التنموية والاختبارية والتشغيلية
- نظام التخطيط والقبول
- الحماية من الشيفرات الخبيثة والمتنقلة
- إدارة شبكة الأمن
- التعامل مع وسائل الإعلام
- تبادل المعلومات
- خدمات التجارة الالكترونية
- الرقابة

الرقابة على الوصول للنظام

تشمل الضوابط اللازمة لتقييد ومراقبة الوصول إلى جميع جوانب النظام، وتشمل المناطق التالية:

- سياسة التحكم في الوصول
- إدارة وصول المستخدم
- مسؤوليات المستخدم
- مراقبة الوصول إلى شبكة الاتصال
- مراقبة الوصول إلى نظام التشغيل
- مراقبة التشغيل ومعلومات الوصول
- الحوسبة المتنقلة والعمل عن بعد

اقتناء نظم المعلومات وتطويرها وصيانتها

تتطلب هذه الضوابط ضمان مراعاة أبعاد الأمن أثناء إجراء كافة التحديثات أو التغييرات على النظام، وتغطي المجالات التالية:

- متطلبات الأمن للنظم
- معالجة صحيحة في أنظمة التشغيل
- ضوابط تشفير
- أمن ملفات النظام
- الأمن في عمليات التنمية والدعم
- إدارة نقاط الضعف الفنية

إدارة حوادث أمن المعلومات

هذه الضوابط مطلوبة من أجل ضمان رفع تقارير حول حوادث أمن المعلومات ونقاط الضعف بطريقة منظمة تجعل من الممكن تنفيذ أي إجراءات تصحيحية دون تأخير، وتغطي المجالات التالية:

- رفع تقارير أحداث أمن المعلومات
- الرفع بنقاط الضعف الأمنية
- جمع الأدلة
- استسقاء الدروس من أحداث أمن المعلومات

حماية العلامة التجارية ومنع الغش

هذه الضوابط مطلوبة لحماية عملاء البنك عبر الإنترنت من عمليات الاحتيال (بما في ذلك هجمات الاصطياد وتزوير العناوين) وسوء استخدام هوية البنك في أنشطة غير مشروعة. يجب أن توفر هذه الضوابط ما يلي:

- القدرة على الكشف عن المواقع الاحتيالية المحتملة على شبكة الانترنت.
- القدرة على الكشف عن إعطاء بيانات مضللة عن البنك أو استخدام هويته بطريقة غير شرعية على شبكة الانترنت.
- القدرة على اتخاذ إجراءات لحماية عملاء البنك على مستوى العالم من الوقوع ضحايا للاحتيال على موقع مخادع معين.

إدارة استمرارية الأعمال

رغم أن هذه النقطة سيتم تغطيتها من خلال مشروع آخر، غير أننا نقترح معالجة جزء من الضوابط أيضا في هذا التقييم الأمني. وهذه الضوابط مطلوبة لضمان أن يبقى تعطل النظام في حدود المستوى المتفق عليه والمقبول، وذلك يشمل ما يلي:

- استمرارية الأعمال، وتقييم المخاطر
- وضع وتنفيذ خطط الاستمرارية
- اختبار وصيانة وإعادة تقييم خطط استمرارية الأعمال

الالتزام

هذه الضوابط مطلوبة من أجل التزام النظام بالتشريعات المعتمدة مع الحفاظ على أمن أصولها، وتغطي المجالات التالية:

- الالتزام القانوني والتنظيمي
- حماية السجلات المؤسساتية
- الوقاية من سوء استخدام مرافق معالجة المعلومات
- مراجعة الحسابات

الملحق 3

رفع تقارير بالحوادث

يجب الإبلاغ عن القائمة التالية من الحوادث من خلال البريد الإلكتروني إلى مدير إدارة التقنية البنكية، مؤسسة النقد العربي السعودي

الحادث	وقت التقرير
أي حالة من حالات الهجمات الاحتيالية للمساس بهوية العملاء وأوراق الاعتماد. (التصيد، تزوير العناوين، طروادات، برمجيات خبيثة، الخ)	يطلب من المصارف إخطار مؤسسة النقد العربي السعودي **على الفور** بعد الكشف عن الحادث. وبالإضافة إلى ذلك، يجب رفع تقرير فني مفصل في غضون أسبوع واحد.
اقتحام غير مصرح به لنظم تقنية المعلومات الخاصة بالمصرف للمساس ببيانات العملاء ذات الصلة بالمصرفية الإلكترونية.	يطلب من المصارف إخطار مؤسسة النقد العربي السعودي في غضون **يوم واحد** بعد الكشف عن الحادث.
أي تلف للبيانات ذات الصلة بالأنظمة المصرفية الالكترونية التي لا يمكن استردادها.	يطلب من المصارف إخطار مؤسسة النقد العربي السعودي **على الفور** بعد الكشف عن الحادث.

	تقرير فني مفصل في غضون أسبوع واحد.
تعطيل متعمد أو عرضي للخدمات المصرفية الكترونية	يطلب من المصارف إخطار مؤسسة النقد العربي السعودي خلال **يوم واحد** بعد الكشف عن الحادث.
أي حالة من حالات الاحتيال الداخلي ذات الصلة بالمصرفية الإلكترونية	يطلب من المصارف إخطار مؤسسة النقد العربي السعودي **على الفور**. بالإضافة إلى ذلك، يجب على المصارف تقديم تقرير مفصل عن طبيعة وتأثير الاحتيال في غضون أسبوع واحد.

ملاحظة: ينبغي أن يقدم المصرف أيضاً تحليلاً للسبب الجذري للحادث الأمني والتدابير التي اتخذها المصرف لتفادي وقوع حوادث مماثلة في المستقبل.