

المخاطر السيبرانية في الصناعة المالية الإسلامية

Cyber Risks in the Islamic Finance Industry

سرين حشمان¹، طالبة دكتوراه، المركز الجامعي مرسلي عبد الله- تيبازة، الجزائر.

hachemane_serine@outlook.com

عبد القادر حدبي، أستاذ محاضر، المركز الجامعي مرسلي عبد الله- تيبازة، الجزائر.

hadbi.abdelkader@cu-tipaza.dz

تاريخ الاستلام: 2023/09/23؛ تاريخ القبول: 2023/11/05

مستخلص:

تركز هذه الدراسة على تسليط الضوء على المخاطر السيبرانية التي تواجهها الصناعة المالية الإسلامية، وممارسات الأمن السيبراني التي تعتمد عليها المصارف الإسلامية كآليات تطوير الدفاع السيبراني والتحديات التي يمكن مواجهتها. وذلك بالاعتماد على المنهج الوصفي التحليلي للبيانات والمؤشرات الصادرة عن استبيان المجلس العام للبنوك والمؤسسات المالية الإسلامية حول الأمن السيبراني لعام 2021.

توصلت الدراسة لمجموعة من النتائج أهمها تصنيف المخاطر السيبرانية المرتبة الأولى من حيث المخاطر التي تتعرض لها المصارف والمؤسسات المالية الإسلامية، نتيجة التحول الرقمي السريع، التطورات التكنولوجية وجائحة كورونا مؤخراً، ما أثر على الصناعة المالية الإسلامية وفرض على مؤسساتها أن تكون على دراية تامة بأنواع المخاطر والتهديدات السيبرانية التي قد تتعرض لها وأن تتخذ تدابير الأمن السيبراني والتوصيات الصادرة عن الهيئات الدولية المختصة.

الكلمات المفتاحية: المخاطر السيبرانية، الأمن السيبراني، المصارف الإسلامية، الصناعة المالية الإسلامية.

تصنيف JEL: E44, G21, G22.

Abstract:

This study focuses on highlighting the cyber risks faced by the Islamic financial industry, the cyber security practices adopted by Islamic banks as cyber defense development mechanisms and the challenges that can be

¹ حشمان سرين: hachemane_serine@outlook.com

faced. Based on the descriptive and analytical approach to data and indicators issued by the General Council of Islamic Banks and Financial Institutions Questionnaire on Cyber security for 2021.

The study reached a set of results, the most important of which is the classification of cyber risks ranked first in terms of risks to which Islamic banks and financial institutions are exposed, as a result of the rapid digital transformation, technological developments and the recent Corona pandemic, which affected the Islamic financial industry and forced its institutions to be fully aware of the types of cyber risks and threats to which they may be exposed and to take cyber security measures and recommendations issued by the competent international bodies.

Keywords: Cyber Risk, Cyber security, The Islamic Banking, Islamic Financial Industry.

Jel Classification Codes : E44, G21, G22.

مقدمة

أدى ظهور التقنيات المبتكرة في نظم المعلومات والتكنولوجيا عبر زيادة اعتماد رقمنة الخدمات المصرفية إلى زيادة المخاطر السيبرانية على الصناعة المالية الإسلامية، على غرار المصارف التقليدية. تسارع تنامي المخاطر بسبب مآلات جائحة كورونا انطلاقا من الفصل الأخير لسنة 2019 والتي باتت مصدر قلق متزايد للمصارف الإسلامية في جميع أنحاء العالم. حيث ورد في الاستبيان العالمي للمصرفين الإسلاميين للمجلس العام لعامي 2020 و 2021 إلى تصنيف المخاطر السيبرانية في طليعة المخاطر التي تواجهها.

إن خطورة وكثافة الهجمات السيبرانية جعلها كواحدة من أهم المخاطر التي تواجه النظام الاقتصادي العالمي، ما يفرض على المؤسسات المالية الإسلامية تطبيق تدابير الأمن السيبراني كآلية الدفاع الإلكتروني لمجابهة هذه المخاطر. لذا، تولي له العديد من الهيئات المالية والمصرفية الدولية والسلطات التنظيمية أهمية كبيرة، وتضعه ضمن الاستراتيجيات الأمنية الواجب متابعتها ومراقبتها.

وعلى ضوء ما سبق، يمكن طرح إشكالية البحث في السؤال الرئيسي التالي:

ماهي المخاطر السيبرانية التي تهدد كيان المصارف الإسلامية وسبل مواجهتها؟

المحور الأول: الصناعة المالية الإسلامية

يأخذ المصرف الإسلامي الطابع التجاري المرخص له بتعاطي الأعمال المصرفية ضمن أحكام الشريعة الإسلامية، من أهمها قبول الودائع المصرفية على أساس عقدي القرض والمضاربة واستثمار الأموال المتجمعة لديه كالمرابحة والمشاركة والمضاربة والسلم و الاستصناع وغيرها من الأعمال التي لا تعارض الشريعة الإسلامية كالقروض والسلف. (حسين محمد سمحان وموسى عمر مبارك، 2011، ص 30)

أولاً: تطور ونشأة المصارف الإسلامية

تعود فكرة إنشاء المصارف والبنوك الإسلامية إلى رغبة العلماء بأن يسود الاقتصاد الإسلامي كامل أنحاء العالم، والذي يركز عملها على الالتزام بأحكام الشريعة الإسلامية ويستمد أسسه منها، ومن أهم المراحل التي مرت بها تجربة المصارف هي (Nathalie SCHOON, 2016, P5):

➤ **المرحلة الأولى:** تجربة ميت غمر بمصر سنة 1963 في بنوك الادخار والتي كانت بمثابة بداية محاولة تنفيذ المصارف الإسلامية، وفي نفس السنة تقرر تدريس مقياس الاقتصاد الإسلامي بجامعة أم درمان الخرطوم (السودان)، عام 1971 ظهر مصرف ناصر الاجتماعي بمصر.

➤ **المرحلة الثانية:** لأول مرة تأسس مصرفان إسلاميان خلال سنة 1975، كان الأول المصرف الإسلامي للتنمية بجدة، والثاني مصرف دبي الإسلامي.

➤ **المرحلة الثالثة:** انطلاق المصارف الإسلامية بالانتشار في مختلف الدول العربية الإسلامية، مثل بنك فيصل الإسلامي السوداني سنة 1977، وبنك فيصل الإسلامي المصري 1977، وبنك التمويل الكويتي 1977، والبنك الإسلامي الأردني للتمويل والاستثمار 1978 والمصرف الإسلامي الدولي للاستثمار والتنمية بالقاهرة سنة 1981.

ثانياً: مفهوم المصارف الإسلامية

حسب اتفاقية إنشاء الاتحاد الدولي للمصارف الإسلامية: تمثل المصارف الإسلامية تلك المؤسسات التي ينص قانون إنشائها ونظامها الأساسي على الالتزام بمبادئ الشريعة الإسلامية، وعدم التعامل بالفائدة أخذاً وعطاءً. سارت على هذا النهج كل التعاريف التي أعطيت للمصارف الإسلامية والمؤسسات المالية سواء في القوانين المنظمة لها، أو التي تبناها الفكر الاقتصادي الإسلامي (محسن أحمد الخضيرى، 1999، ص 17).

ثالثاً: خصائص المصارف الإسلامية

ينفرد العمل المصرفي الإسلامي عن العمل المصرفي التقليدي بخصائص تتمثل في (خالد محمد أحمد الجابري، 2016) توجيه جهود المصارف الإسلامية كافة نحو الاستثمار الحلال؛ الالتزام بتطبيق أحكام الشريعة الإسلامية واستبعاد التعامل بالفائدة الربوية.

رابعاً: وظائف المصارف الإسلامية

حدد البيان الصادر عن هيئة المحاسبة والمراجعة للمؤسسات المالية الإسلامية وظائف المصارف الإسلامية، على أنها إدارة أموال الغير مقابل نسبة من الربح على أساس المضاربة أو مقابل أجر مقطوع أو نسبة من المال المستثمر على أساس عقد الوكالة بالأجر، واستثمار الأموال المتاحة له من مصادر ذاتية من حسابات الاستثمار ضمن أحكام الشريعة الإسلامية، بالإضافة إلى وظيفة تقديم الخدمات المختلفة مثل تحصيل الشيكات وفتح الاعتمادات المستندية والحوالات مقابل اجر محدد، وأخيراً تقديم الخدمات الاجتماعية كالقرض الحسن والصدقات وغيرها.

المحور الثاني: المخاطر السيبرانية في الصناعة المالية الإسلامية وآليات الدفاع السيبراني

فإذا كانت دوافع مجرمي الانترنت بالخصوص مالية، فإن بيانات المؤسسات المالية تعتبر أهدافاً جذابة للغاية تحقق منها عوائد مالية عبر بيعها أو استخدامها للابتزاز. لقد ارتفعت حالات الهجمات الإلكترونية خلال الوباء من أقل من 5000 أسبوعياً في فيفري 2020 إلى أكثر من 200000 أسبوعياً في أواخر أبريل من هذا العام. (FSB)، والتي تعود بالأساس إلى التحول السريع لترتيبات العمل عن بعد وزيادة رقمنة الخدمات المالية. ما جعل هذه المؤسسات أكثر عرضة للمخاطر السيبرانية.

أولاً: ماهية المخاطر السيبرانية

تمثل المخاطر السيبرانية الناتجة عن التحول الرقمي والتطور التكنولوجي تهديداً للقطاع المالي والمصرفي، ويشكل تحدياً أمام المصارف والمؤسسات المالية الإسلامية لمواجهةها على غرار النظام المالي التقليدي.

عرف بنك التسويات الدولية المخاطر السيبرانية على أنها الخسارة المالية أو الاضطراب أو الإضرار بسمعة المؤسسة نتيجة عطل في أنظمة تكنولوجيا المعلومات الخاصة بها. (المجلس العام للبنوك والمؤسسات المالية الإسلامية، ديسمبر 2021، ص2). كما تعتبر المخاطر الإلكترونية مشكلة تجارية ذات أبعاد تقنية، حيث يؤثر على كل مجالات المؤسسة ويتأثر بها من جانب احتواء المخاطر أو تضخيمها" (علم الدين بانقا، 2019، ص12).

II-أنواع المخاطر السيبرانية

من أهم المخاطر السيبرانية التي يعتمد عليها المهاجمون في هذا المجال ما يلي (محمد قوجيل وعبد العزيز طيبة، 2022، ص190):

- خطر حجب الخدمة الموزعة (هجمات الحرمان من الخدمة): هو عبارة عن هجوم يغمر الموارد أو النطاق الترددي لنظام ما بحركة مرور غير مرغوبة (إرسال بيانات من المخترق غير ضرورية للتأثير على أداء النظام) ويمنع الاستخدام المصرح به لهذا النظام. كما تعتبر هجمات تعطيل أنظمة الكمبيوتر من خلال التسبب في حركة مرور ضخمة على خوادمها وشبكتها.
- خطر التهديد المستمر المتقدم: هو هجوم الكتروني يبقي صاحبه غير مرئي، يهدف إلى الترسد ومراقبة نشاط الشبكة والبيانات دون السعي إلى إتلاف الجهاز أو النظام.
- خطر التصيد: يتم عبر استخدام رسائل البريد الإلكتروني والتظاهر كهيئة رسمية ولكنها مزيفة، من أجل الحصول على بيانات المستخدم من خلال توجيهه إلى المواقع الاحتيالية.
- خطر بريد مؤذي: إرسال بريد الكتروني غير مطلوب، كالإعلان عن منتجات وخدمات مواقع الكترونية، وتسليم البرامج الضارة والتهديدات السيبرانية الأخرى.
- البرمجيات الخبيثة: تمثل برامج ضارة كالفيروسات والديدان وأحصنة طروادة، مصممة لإتلاف وتعطيل أجهزة الكمبيوتر والبرامج والتطبيقات، أو تسرق بياناته.
- خطر الروبوت: يستخدم لتوزيع البرامج الضارة والرسائل غير المرغوب فيها والخداع، تسمح للمتسلل بالتحكم في النظام.
- خطر الخداع والانتحال: يعني تقليد أو نسخ أو تزوير أو تمويه هوية ضارة للوصول إلى البيانات أو القيام بأنشطة ضارة أخرى.
- التهديدات من الداخل: كالموظفين أو العملاء الذين لديهم إمكانية الوصول إلى المعلومات الداخلية.

يتزايد تعقيد هذه المخاطر باستمرار نتيجة للتطورات التكنولوجية التي تؤدي إلى أنواع جديدة من هذه التهديدات. كما أن الهدف من وراء المخاطر السيبرانية يكون أما بدافع الحصول على الأموال، أو من أجل الوصول إلى معلومات المؤسسة السرية، كما يمكن أن يكون لأهداف جيوسياسية. ينتج عن هذه المخاطر أثر على المبادئ الأساسية للتكنولوجيا المعلومات وهي السرية والنزاهة والتوافر، كما يمكن للعملاء أن يفقدوا الثقة في مصرفهم أو مؤسستهم المالية مما يضر بسمعة هذه الأخيرة، ويؤثر على زعزعة الاستقرار المالي ويسبب خسائر مالية وخسائر البيانات الهامة.

III_الأطراف المسببة للمخاطر السيبرانية

تنقسم الجهات الفاعلة في مجال التهديد السيبراني إلى ست مجموعات ولكل منها مجموعة من الأهداف والدوافع، وهي (علم الدين بانقا، 2019، ص ص 15-16):

➤ **الدول القومية:** تكون هذه المجموعة ممولة بشكل جيد وغالبا ما تنخرط في هجمات متطورة وموجهة، وعادة ما تكون الدول القومية مدفوعة بجداول أعمال سياسية أو اقتصادية أو تقنية أو عسكرية، وكثيرا ما تشارك هذه الدول في التجسس الصناعي. وإذا كانت لديهم احتياجات تمويلية، فقد يقومون بهجمات فدية وسرقات إلكترونية للأموال. كما تستهدف معلومات تحديد الهوية الشخصية للتجسس على أفراد معينين. كما قد تنخرط الدول القومية في تدمير واحدة أو أكثر من شركات الدولة المستهدفة. ويحتمل أن يكون ذلك بمثابة انتقام ضد العقوبات أو غيرها من الإجراءات التي يتخذها المجتمع الدولي.

➤ **الشركات المنافسة:** تسعى هذه للحصول غير المشروع للبيانات الخاصة بالملكية الفكرية لشركة منافسة في نفس الدولة أو في دول أخرى، بما في ذلك المعلومات المالية والإستراتيجية والقوى العاملة فيها، وكثيرا ما تدعم هذا النوع من الهجمات الدول القومية لتعزيز منافسة شركاتها عالميا.

➤ **القراصنة:** يمارس القراصنة عموما أفراد أو مجموعات خاصة في جميع أنحاء العالم لديهم أجندة سياسية ويسعون لتنفيذ هجمات عالية المستوى، وتساعد هجمات القرصنة الالكترونية على نشر الدعايات أو إلحاق الضرر بمنظمات المعارضة لأسباب أيديولوجية.

➤ **الجماعات الإجرامية المنظمة:** تمارس هذه المجموعة هجمات استهدافية بدافع الربح، ويجمعون العوائد عن طريق بيع البيانات الشخصية المسروقة على شبكة الانترنت، ومن خلال تحصيل مدفوعات الفدية من القطاعين العام والخاص ومن خلال الهجمات التخريبية.

➤ **الانتهازيون:** هم عادة قراصنة هواة مدفوعين برغبة في الشهرة، وعادة ما يهاجم الانتهازيون المنظمات التي تستخدم الرموز والأساليب المتاحة على نطاق واسع، وبالتالي عادة ما تمثل هذه المجموعات أقل أشكال الجماعات المهاجمة تقدما.

➤ **المطلعين على الشركة:** يمثلون الموظفون الساخطون أو الموظفون السابقون الذين يبحثون عن الانتقام أو الربح المالي، وتزداد خطورة المطلعين على بواطن الأمور في الشركة بشكل خاص عندما يعملون جنبا إلى جنب مع جهات خارج الدولة، مما يسمح لهذه الجهات تجاوز أقوى الدفاعات السيبرانية.

كما يمكن أن تنشأ المخاطر داخل المؤسسات نتيجة لأسباب غير مقصودة كحذف البيانات بالخطأ من قبل الموظفين، أو لأسباب مقصودة عندما يستهدف المهاجمون عمدا أنظمة وشبكات الكمبيوتر للتسبب في خسارة مالية، أو يكون لأغراض سياسية. ويمكن تنفيذ الهجمات السيبرانية من قبل أطراف خارج المؤسسات مثل المنظمات الإجرامية والقرصنة والهواة. (المجلس العام للبنوك والمؤسسات المالية الإسلامية، ديسمبر 2021، ص2)

ثانيا: المخاطر السيبرانية التي تواجه المصارف المالية الإسلامية

حسب نتائج الاستبيان العالمي للمصرفيين الإسلاميين لسنة 2020 و2021، حول أكثر المخاطر التي تتعرض لها المصارف والمؤسسات المالية خاصة بعد توسع استخدام تقنيات وتطبيقات التكنولوجيا المالية، والذي قدم لاختصاصيين والفائمين على النشاط المالي. إذ كانت النتائج كما هو موضح في الشكل الموالي:

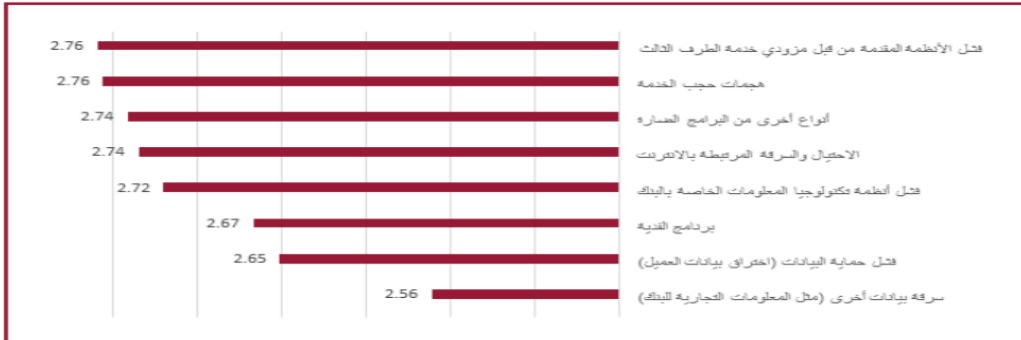
الشكل رقم (1): المخاطر الأكثر تأثيرا على المصارف والمؤسسات المالية الإسلامية



المصدر: الاستبيان العالمي للمصرفيين الإسلاميين، تقييم التأثيرات المستقبلية كالتفكير الاستراتيجي والعلامة التجارية والتكنولوجيا المالية، المجلس العام للبنوك والمؤسسات المالية الإسلامية، مملكة البحرين، 2020، ص85.

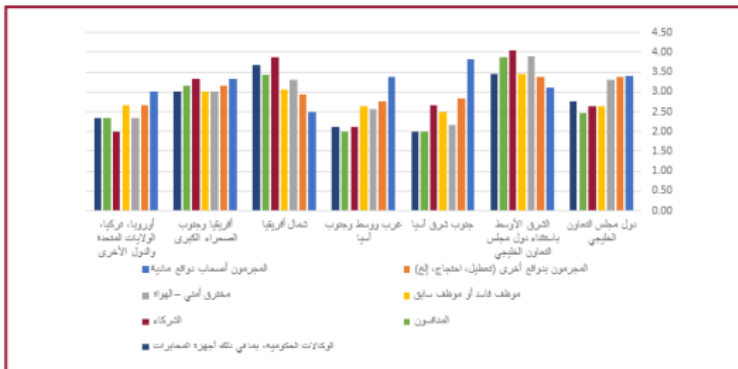
نلاحظ اتفاق المستجيبون عموما على إن تهديدات الأمن الإلكتروني من أكثر المخاطر تهديدا على المصارف والمؤسسات المالية الإسلامية وصنفت في طليعة المخاطر، ويفسر ذلك بسبب توسع استخدام تقنيات التكنولوجيا المالية في معاملاتها وخدماتها، مما زاد من احتمالية تعرضها للاختراق والاحتيال عبر الانترنت وكان هذا الخطر بقيمة 3,24. لتليها بقيمة 3,19 كانت إجابتهم حول قيود الميزانية. وفي المرتبة الثالثة تأتي مخاطر محدودية ونقص المهارات الرقمية لدى الموظفين في هذه المؤسسات، أما الخطر الأقل تأثيرا هو فقدان قاعدة العملاء في المصارف والمؤسسات المالية.

الشكل رقم (2): أنواع المخاطر السيبرانية المواجهة للمصارف الإسلامية



المصدر: المجلس العام للبنوك والمؤسسات المالية الإسلامية، "الاهتمام المتزايد بالأمن السيبراني في التمويل الإسلامي، المخاطر الرئيسية والممارسات الحالية وآليات الدفاع الإلكتروني"، العدد الخامس عشر، ديسمبر 2021.

يعد فشل الأنظمة المتقدمة من قبل مزودي خدمة الطرف الثالث، وهجمات حجب الخدمة والحرمان منها من أهم المخاطر الإلكترونية التي تواجه المصارف الإسلامية بنفس المستوى 2,76. وجاء بعدها خطر الاختيال والسرقة المرتبطتين بالإنترنت وأنواع أخرى من البرامج الضارة وغير الآمنة. وتأتي في المرتبة الأخيرة من هذه المخاطر سرقة بيانات النظام والمعلومات التجارية للمصرف. الشكل رقم (3): الأطراف المسببة للمخاطر السيبرانية التي تواجه المصارف الإسلامية



المصدر: المجلس العام للبنوك والمؤسسات المالية الإسلامية، "الاهتمام المتزايد بالأمن السيبراني في التمويل الإسلامي، المخاطر الرئيسية والممارسات الحالية وآليات الدفاع الإلكتروني"، العدد الخامس عشر، ديسمبر 2021.

يوضح الشكل رقم (3) أعلاه الأطراف التي تسبب تهديدا وتكون فاعلا للمخاطر والهجمات السيبرانية التي تواجه المصارف الإسلامية حسب كل إجابات كل منطقة، وتم تحديدها بسبعة أطراف متمثلة في المجرمون من أصحاب الدوافع المادية، مخترقي الأمن من الهواة والمبتدئين، الشركاء التجاريين، الوكالات الحكومية بما في ذلك أجهزة المخابرات، مجرمون بدوافع أخرى، موظفين فاسدين وأخيرا المنافسين.

ثالثا: إجراءات وتدابير الأمن السيبراني في المصارف الإسلامية

بما أن الخطر السيبراني يعتبر من أهم المخاطر المرتبطة بتقنيات التكنولوجيا المالية ذات العلاقة بالانترنت، تولى له العديد من الهيئات المالية والمصرفية الدولية والسلطات التنظيمية أهمية كبيرة، وتضعه ضمن الاستراتيجيات الأمنية الواجب متابعتها ومراقبتها، ولذلك يطلق عليها بالأمن السيبراني.

I- الأمن السيبراني- مفهومه ووظيفته -

يعرف الأمن السيبراني حسب الاتحاد الدولي للاتصالات على أنه "مجموع الأدوات والسياسات ومفاهيم الأمن وضوابط الأمن والمبادئ التوجيهية وإدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستعملين" (الاتحاد الدولي للاتصالات، 2010، ص 20).

عرف المعهد الوطني للمعايير والتقنية الأمريكي NIST على أنه: "النشاط أو العملية التي يتم بموجبها حماية نظم المعلومات والاتصالات والدفاع عنها ضد الضرر أو الاستخدام أو التعديل غير المصرح به أو الاستغلال" (حلف الشمال الأطلسي NATO، 2016)، والذي تتجلى وظيفته في (قوجيل محمد وعبد العزيز طيبة، 2022، ص 195):

-تأمين جميع جوانب التحول الرقمي والبيانات والقدرة على المقاومة، من خلال سرية المعلومات الحساسة وسلامة المعالجة، وتوافر الأنظمة ومخازن البيانات والشبكات الضرورية لتوفير خدمة مستمرة؛

-إدارة مخاطر الانترنت من خلال تطوير نموذج الإبلاغ الموحد الذي يوضح حوكمة المؤسسة للمخاطر السيبرانية؛

-إجراء اختبارات الاختراق دوريا بناءا على سيناريوهات الهجوم السيبراني مع إشراك مختبري الاختراق المعتمدين.

كما عرف على أنه "عبارة عن مجموعة من الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات، وتعزيز الحماية وسرية وخصوصية البيانات الشخصية واتخاذ

جميع التدابير اللازمة لحماية مستخدمي الفضاء السيبراني، وهو جزء لا يتجزأ من التكتيكات الحديثة للحروب باعتباره المجال الخامس للحروب الحديثة بعد البر والبحر والجو والفضاء" (عطية، 2019، ص104).

يمكن القول بأن الأمن السيبراني يشمل على عنصر السرية والموثوقية في عدم الكشف عن المعلومات، التكامل وسلامة المحتوى من التلاعب وعنصر الاستمرارية وذلك من خلال ضمان تقديم الخدمة دون انقطاع. (قصعة، 2020، ص380)

II- تدابير الأمن السيبراني من قبل المصارف الإسلامية

تتمثل إجراءات بناء الدفاع والأمن السيبراني في المؤسسات المالية الإسلامية مايلي (المجلس العام للبنوك والمؤسسات المالية الإسلامية، ديسمبر 2021، ص3):

➤ الامتثال للوائح والإرشادات الصادرة عن السلطات التنظيمية: تلعب هذه السلطات دوراً مهماً في ضمان الأمن السيبراني من خلال وضع معايير ومتطلبات إلزامية للأمن، دورها حماية المؤسسات المالية والمستهلكين، وتشمل المبادرات التنظيمية ووصايا المؤسسات المختصة في هذا المجال على:

- أعدت المنظمة الدولية لهيئات الأوراق المالية ولجنة المدفوعات والبنية التحتية للسوق في عام 2016 أول دليل متفق عليه دولياً حول متانة الأمن السيبراني للبنى التحتية للأسواق المالية؛

- أصدر بنك التسويات الدولية تقريراً عام 2018 يعرض ويقارن مجموعة من ممارسات متانة الأمن السيبراني التي اعتمدتها البنوك والسلطات التنظيمية والإشرافية في العديد من الدول؛

- أصدر مجلس الاستقرار المالي عام 2020 مجموعة أدوات تحدد الممارسات التي قد تتبعها المؤسسات المالية للتصدي للمخاطر والهجمات السيبرانية والتعافي منها، كما قدم عدة توصيات عن بناء وظيفة أمن سيبراني فعال؛

- أوصى البنك المركزي الأوروبي في توجيهاته الصادرة عام 2020، على التقييم المستمر للبنية التحتية لتكنولوجيا المعلومات للبنوك والمؤسسات المالية إثر الزيادة من الهجمات الإلكترونية؛

- طلبت السلطة النقدية في سنغافورة من المؤسسات المالية عام 2020، اعتماد نهج استباقي في التعامل مع أي زيادة في الطلب على الخدمات المالية عبر الإنترنت.

➤ اعتماد المصارف والمؤسسات المالية تقنيات متطورة لتعزيز قدرتها على مواجهة المخاطر السيبرانية: باستخدام تقنية الذكاء الاصطناعي فهي تساعد في فحص كميات هائلة من البيانات بكفاءة لتحديد نمط المخاطر والتقليل من تكاليف هذه الحوادث والتهديدات، كما يعزز استخدام الذكاء الاصطناعي من القدرات الدفاعية للمصارف المالية الإسلامية ضد المخاطر السيبرانية.

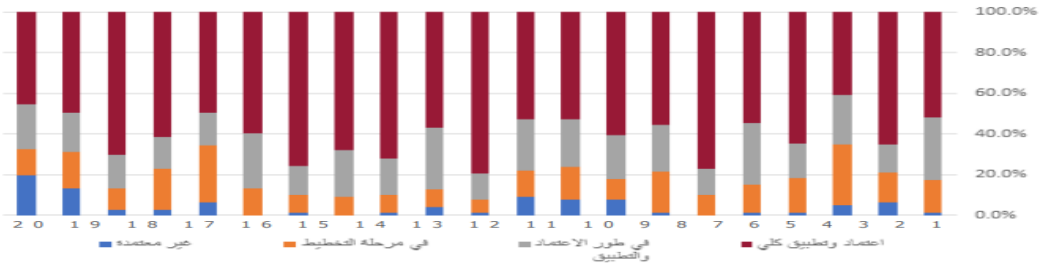
➤ تدريب و تثقيف العاملين لتحقيق المستوى المطلوب من المهارات: يجب على المصارف والمؤسسات المالية تزويد العاملين بالأدوات اللازمة للحد من المخاطر والتخفيف من حدتها، من خلال التدريب والتعليم المستمر في مجال الأمن السيبراني بالإضافة إلى المراقبة الدورية لأنظمة وبيانات المؤسسة لتتبع مصدر الخطر.

أشارت المصارف الإسلامية في الاستبيان العالمي للمصرفيين الإسلاميين للمجلس العام لسنة 2020 و 2021، أنه من أهم التدابير والإجراءات التي تعتمد عليها المصارف الإسلامية لتعزيز قدرة الأمن السيبراني تماشيا مع توصيات الهيئات الدولية، هي كالتالي:

- إجراء تدريبات كل ثلاثة أشهر لاختبار القدرة على الاستجابة لحوادث الأمن السيبراني؛
- إجراء اختبارات الاختراق لتحديد نقاط الضعف التي قد تؤثر على أنظمة وشبكات المؤسسات؛
- إجراء تحقيقات متعمقة في أعقاب حدث أو حادثة تتعلق بالأمن السيبراني؛
- تطوير استراتيجيات خاصة للأمن السيبراني؛
- تحديد نقاط الضعف في الأجهزة الالكترونية والبرامج بشكل استباقي وتوثيقها مع تقييم المخاطر؛
- تدريب الموظفين على الأمن السيبراني مرة واحدة على الأقل في السنة؛
- تعيين رئيس رسمي للأمن السيبراني كمسؤول عن تقديم إطار عمل الأمن الالكتروني؛
- طلب مصادقة لجميع عمليات الربط عن بعد بشبكة الشركة وتطبيقات الأعمال؛
- توفير ضوابط مناسبة لتصنيف المعلومات من حيث الأهمية والحساسية؛
- اعتماد أدوات لها القدرة على اكتشاف البيانات الحساسة ومنع تسريبها من شبكة الشركة؛
- تحديد إجراءات تكون فعالة في تقييم القدرات الأمنية وإدارة المخاطر السيبرانية من قبل المزودين؛

- توظيف مستويات متعددة من الأمان لفصل شبكة الشركة عن الأنظمة الخارجية؛
- القيام برصد واكتشاف الأنشطة والأحداث التي تكون ضمن دائرة الشبكات؛
- تسجيل محاولات الاختراق عن بعد مع تنبيهات عن أي نشاط ضار أو مشبوه محتمل؛
- مراقبة الأفراد المتصلين بشبكة الشركة بما في ذلك الاتصالات أو الأجهزة غير المصرح بها؛

- استخدام ذكاء التهديدات الالكترونية لتطوير إستراتيجية وإطار عمل الأمن السيبراني؛
 - وضع وتطبيق عملية استعادة الأنظمة والبيانات خلال حادث مرتبط بالأمن السيبراني؛
 - الانخراط مع الأطراف الخارجية لفهم المخاطر الموجودة بين كلا الطرفين، واتخاذ خطوات لضمان أن أنشطة التعافي مفهومة من كلاهما؛
 - توفر إرشادات غير إلزامية حول الأمن السيبراني من جهة تنظيمية أو هيئة تجارية.
- الشكل رقم (4): مستوى تنفيذ تدابير الأمن السيبراني من قبل المصارف الإسلامية



المصدر: المجلس العام للبنوك والمؤسسات المالية الإسلامية، "الاهتمام المتزايد بالأمن السيبراني في التمويل الإسلامي، المخاطر الرئيسية والممارسات الحالية وآليات الدفاع الالكتروني"، العدد الخامس عشر، ديسمبر 2021.

يوضح الشكل رقم (4) مستوى تنفيذ تدابير الأمن السيبراني من قبل المصارف الإسلامية، والتي أشارت إلى أن أغلب المستجيبين من المصارف الإسلامية هم في مرحلة اعتماد وتطبيق تدابير خاصة للأمن السيبراني.

III- تحديات المصارف الإسلامية

تواجه المصارف الإسلامية تحديات أكبر في ضمان الأمن السيبراني بسبب حجمها وموقعها، حيث يمثل الاستثمار في تدابير الأمن السيبراني الصادرة عن الهيئات الدولية، تحدياً رئيسياً للمصارف الإسلامية نظراً لكونها بنوك صغيرة ذات موارد محدودة. بالإضافة إلى ذلك، يمكن أن تؤدي العوامل الجيوسياسية في المناطق الجغرافية لهذه المصارف إلى جعل الأنظمة المالية في هذه المناطق هدفاً متزايداً للهجمات السيبرانية. كما تمثل نقاط الضعف في البنية التحتية لتكنولوجيا المعلومات في بعض البلدان الناشئة عبئاً على المصارف الإسلامية لاسيما في حالة المعاملات والخدمات المالية الرقمية التي تتم باستخدام أجهزة غير آمنة وعبر خطوط نقل غير مصممة

لحماية أمن المعاملات المالية (المجلس العام للبنوك والمؤسسات المالية الإسلامية، 2021، ص4). كما يسبب غياب المتخصصين والمهنيين المناسبين في مجال الأمن السيبراني للتعامل مع الحوادث السيبرانية تحديا داخل المصارف الإسلامية مع التطور المتزايد في أساليب المجرمين والهجمات السيبرانية.

الخاتمة

تعتبر المخاطر السيبرانية إحدى التحديات التي تواجه الصناعة المالية بشكل عام والمصارف الإسلامية بشكل خاص، انتقاما أو نصبا واحتيال. فمع زيادة الخدمات والمنتجات المالية عبر الهواتف الذكية والاستعانة بالمصادر الخارجية في تقديم هذه الخدمات تزداد مخاطر حماية الزبائن والمؤسسات المالية بذاتها. تمثل الهجمات الالكترونية أشد المخاطر التي تواجه المصارف الإسلامية بسبب ازدياد تواترها وعدم إمكانية التنبؤ بها.

وبناء على هذا يمكننا استخلاص النتائج التالية:

- جاءت الهجمات السيبرانية في طليعة المخاطر التي تواجه المصارف والمؤسسات المالية الإسلامية؛ والذي يعتبر من أهم المخاطر المرتبطة بتقنيات التكنولوجيا المالية؛
- تضمنت الهجمات على المصارف الإسلامية القرصنة من خلال طرف ثالث؛
- فرضت المخاطر التي تعترض المصارف الإسلامية على الهيئات الدولية والسلطات التنظيمية، إصدار تدابير وضوابط لتعزيز متانة وحصانة الأمن السيبراني؛
- يعزز استخدام تقنية الذكاء الاصطناعي من القدرات الدفاعية للمصارف الإسلامية ضد المخاطر السيبرانية؛
- يجب على المصارف المالية الإسلامية تدريب وتعليم العاملين في مجال الأمن السيبراني لتتبع مصدر الخطر؛

تواجه المؤسسات المالية الإسلامية تحديات وعوائق في إقامة الأمن السيبراني، كقيود الميزانيات، نقص المهنيين والخبراء، والتهديدات الداخلية.

قائمة المراجع

- المجلس العام للبنوك والمؤسسات المالية الإسلامية، "الاهتمام المتزايد بالأمن السيبراني في التمويل الإسلامي، المخاطر الرئيسية والممارسات الحالية وآليات الدفاع الالكتروني"، العدد الخامس عشر، ديسمبر 2021.
- الاتحاد الدولي للاتصالات، الأمن السيبراني، 2010.

- حلف الشمال الأطلسي NATO، من الأمن السيبراني، www.nato.int/nato-static
- حسين محمد سمحان وموسى عمر مبارك، "محااسبة المصارف الإسلامية"، دار المسيرة للنشر والتوزيع والطباعة، عمان، 2011.
- مجيد جاسم الشرع، "المحااسبة في المنظمات المالية -المصارف الإسلامية-"، إثراء للنشر والتوزيع، الشارقة، 2008.
- محسن أحمد الخضيرى، "البنوك الإسلامية"، ايتراك للنشر والتوزيع، 1999.
- عطية إدريس، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، مجلة مصداقية، المجلد 1، العدد1، 2019.
- علم الدين بانقا، "مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي"، المعهد العربي للتخطيط، مجلة الدراسات التنموية، العدد 63، الكويت، 2019.
- خالد محمد أحمد الجابري، "البنوك الإسلامية مقابل البنوك التجارية-دراسة نظرية مقارنة-"، مجلة اقتصاد الإسلامية العالمية، العدد3، 2016.
- قوجيل محمد وعبد العزيز طيبة، "مخاطر التكنولوجيا المالية واداراتها في القطاع المصرفي-دراسة تنظيمية احترازية"، مجلة الاقتصاد والمالية، المجلد 8، العدد 2، 2022.
- NATALIE SCHOON Modern Islamic Banking, Products and Processes in Practice, John Wiley & Sons Ltd, 2016.