

الأمن السيبراني في البنوك الجزائرية التحديات والإستراتيجيات Cybersecurity in Algerian Banks: Challenges and Strategies

حشروف فاطمة الزهراء¹، صديقي وحيدة²

¹ مخبر التسويق والابتكار بسيدي بلعباس، المركز الجامعي نور بشير البيض (الجزائر)، f.hacherouf@cu-elbayadh.dz

² مخبر تقييم واستشراف السياسات الاقتصادية وسياسات المؤسسة، المركز الجامعي مغنية (الجزائر)،

Seddiki.wahida@cumaghnia.dz

تاريخ النشر: 2025/05/25

تاريخ القبول: 2025/04/17

تاريخ الاستلام: 2025/03/05

ملخص:

تهدف من خلال هذه الدراسة إلى تسليط الضوء على التحديات التي تواجهها البنوك الجزائرية في مجال الأمن السيبراني في ظل التحول الرقمي المتسارع وزيادة الاعتماد على التكنولوجيا في تقديم الخدمات المصرفية وتوسع استخدام الإنترنت في المعاملات المالية وهو ما جعل البنوك الجزائرية تواجه تحديات كبيرة وستتطرق إلى أهم الإستراتيجيات الممكنة للتصدي لهذه التحديات، إعتمدنا في بحثنا هذا على المنهج الوصفي التحليلي.

ومن أهم النتائج التي توصلت إليها الدراسة أن البنوك الجزائرية تعمل على تحديث وتطوير أنظمتها الإلكترونية وأنظمة الأمن السيبراني، بهدف تقليل أو تجنب المخاطر التي قد يدركها العملاء، خاصة تلك المتعلقة بالخدمات الرقمية المقدمة و كذا ضرورة وجود استراتيجية للأمن السيبراني تعتمد عليها كل مؤسسة مالية وفقاً لممارسات إدارة المخاطر.

كلمات مفتاحية: الأمن السيبراني، الفضاء السيبراني، الجرائم الإلكترونية الفيروسات الإلكترونية

تصنيف JEL: L86، D80، G2

Abstract:

This study aims to highlight the challenges faced by Algerian banks in the field of cybersecurity amidst the rapid digital transformation and the increased reliance on technology in providing banking services. The expansion of internet usage in financial transactions has led Algerian banks to face significant challenges. The study will address the most important strategies to tackle these challenges. The research relies on the descriptive-analytical approach.

one of the key findings of the study is that Algerian banks are working on updating and developing their electronic systems and cybersecurity measures in order to reduce or avoid risks that might affect customers, particularly those related to the digital services provided.

Keywords : Cybersécurité, Cyberspace, Cybercrimes, Computer Viruses

JEL Classification: G2، D80، L86

1. مقدمة :

في ظل العصر الرقمي الحالي، أصبح الأمن السيبراني جزءاً لا يتجزأ من استراتيجيات الأمان المؤسسي على مستوى العالم. ومع تزايد الاعتماد على التقنيات الحديثة، تتضاعف التهديدات التي يمكن أن تواجه المؤسسات في مختلف القطاعات، لا سيما في القطاع المصرفي الذي يعتبر واحداً من أكثر القطاعات حساسية. ففي هذا الإطار، تبرز البنوك الجزائرية كأحد الأمثلة على التحديات التي تواجهها هذا التحول الرقمي. رغم التقدم النسبي في استخدام الحلول الرقمية، لا تزال العديد من البنوك الجزائرية تعتمد على بنية تحتية قديمة، مما يعيق قدرتها على مواجهة المخاطر السيبرانية المتزايدة. هذه الفجوة التكنولوجية تشكل خطراً كبيراً على عمليات البنوك وعلى سمعتها، مما يعزز من ضرورة التركيز على الأمن السيبراني بشكل أكثر جدية.

تتمثل التحديات الرئيسية التي تواجهها البنوك الجزائرية في قلة الوعي الكافي بالأمن السيبراني بين الموظفين والعملاء على حد سواء، مما يجعلها عرضة للهجمات التي قد تستهدف البيانات الحساسة، مثل معلومات الحسابات البنكية أو المعاملات المالية. بالإضافة إلى ذلك، هناك نقص في الاستثمار الكافي في تقنيات الأمان الحديثة التي يمكن أن تضمن حماية فعالة ضد هذه التهديدات. في الوقت الذي تتسارع فيه وتيرة الابتكارات الرقمية، تظل هذه البنوك في حاجة ماسة إلى إعادة التفكير في استراتيجياتها الأمنية، وتعزيز قدراتها على مواجهة المخاطر الرقمية التي قد تؤثر بشكل كبير على استقرار النظام المالي.

هذه التحديات تتطلب استجابة سريعة ومدروسة، حيث ينبغي على البنوك الجزائرية أن تعمل على تحديث بنيتها التحتية التكنولوجية، وتدريب موظفيها على أحدث ممارسات الأمن السيبراني، وتعزيز ثقافة الوعي الإلكتروني في جميع مستويات العمل. علاوة على ذلك، لا بد من تطوير أطر قانونية وتنظيمية تستجيب للتحديات الحديثة، بما يضمن استدامة التحول الرقمي بشكل آمن وفعال.

من خلال هذه المداخل، سيتم التركيز على التحديات التي تواجه البنوك الجزائرية في مجال الأمن السيبراني وكيفية التغلب عليها، بالإضافة إلى استعراض استراتيجيات مبتكرة تساعد هذه المؤسسات المالية في تحسين قدرتها على حماية بيانات عملائها ومواجهة الهجمات الإلكترونية وفي هذا السياق، سوف نطرح الإشكالية التالية:

1.1 إشكالية البحث :

• كيف يمكن للبنوك الجزائرية مواجهة التحديات السيبرانية؟

2.1 فرضيات البحث:

- لا يقتصر الأمن السيبراني على حماية البيانات والمعلومات بل يتجاوزها إلى تعزيز الثقة في النظام المالي.
- مواجهة التحديات السيبرانية يعتمد بشكل أساسي على تطوير سياسات وإستراتيجية شاملة لإدارة المخاطر السيبرانية

- زيادة الوعي الأمني لدى العملاء يمثل أحد العوامل الرئيسية لتقليل المخاطر السيبرانية.

3.1 المنهج المتبع:

- المنهج الوصفي التحليلي: من خلال وصف الظواهر المرتبطة بالأمن السيبراني في البنوك الجزائرية وتحليل التحديات والفرص.

- المنهج الاستقرائي: من خلال استقراء البيانات والمعلومات المتاحة من الواقع العملي في البنوك الجزائرية للوصول إلى استنتاجات عامة حول فعالية استراتيجيات الأمن السيبراني.

4.1 تقسيمات الدراسة:

المحور الأول: مفهوم الأمن السيبراني وتأثيره على المؤسسات الاقتصادية

المحور الثاني: التحديات التي تواجه البنوك الجزائرية في مجال الأمن السيبراني

المحور الثالث: إستراتيجيات تعزيز الأمن السيبراني في البنوك الجزائرية

2. مفهوم الأمن السيبراني و تأثيره على المؤسسات الاقتصادية

1.2 الأمن السيبراني (Cybersecurity) هو مجموعة من الوسائل التقنية والتنظيمية والإدارية التي تُستخدم لحماية المعلومات والأنظمة الإلكترونية من الاستخدام غير المصرح به أو الاستغلال السيئ. يهدف الأمن السيبراني إلى ضمان استمرارية عمل نظم المعلومات من خلال:

- منع الوصول غير المصرح به إلى البيانات والأنظمة.

- الحفاظ على سرية البيانات وضمان خصوصيتها، مما يعني منع تسريب أو التلاعب بالمعلومات.

- استعادة البيانات والأنظمة في حال حدوث هجمات أو خلل، لضمان استمرارية العمل وعدم تأثر العمليات المهمة.

(يعقوب، 2022، صفحة 1407)

2.2 الفضاء السيبراني: يمكن القول أن الفضاء السيبراني يشمل التفاعل بين الأشخاص، الأنظمة الرقمية، والتكنولوجيا. هذه البيئة تتيح الاتصال وتبادل البيانات عبر الشبكات الإلكترونية مثل الإنترنت، وتضم أدوات ومكونات من البرمجيات، الأجهزة، والبنية التحتية التي تساهم في التفاعل بين المستخدمين في بيئة رقمية. (زروقة، 2019)

3.2 أبعاد الأمن السيبراني:

يشمل الأمن السيبراني خمسة أبعاد رئيسية، تكمل بعضها البعض وتؤثر بشكل مباشر في حماية الفضاء الرقمي على مختلف الأصعدة:

- **الأبعاد العسكرية:** يتعلق بالأمن السيبراني في المجال العسكري، حيث يُستخدم لتسهيل التواصل بين الوحدات العسكرية وتبادل المعلومات بسرعة. لكن، إذا لم تكن الشبكة الإلكترونية محمية بشكل جيد، قد تتعرض للهجمات التي تعطل العمليات العسكرية وأنظمة الدفاع.

- **الأبعاد الاقتصادية:** يرتبط الأمن السيبراني ارتباطاً وثيقاً بالاقتصاد الرقمي، حيث يُساهم في تأمين المعاملات المالية الإلكترونية وحماية البيانات التجارية. كما يلعب دوراً مهماً في مواجهة الجرائم المالية مثل غسل الأموال والتهرب الضريبي.

- **الأبعاد السياسية:** يتعلق بحماية النظام السياسي ومصالح الدولة من التهديدات الإلكترونية. حيث يمكن استخدام الإنترنت للتأثير على الرأي العام وترويج السياسات، مما يجعل الأمن السيبراني ضرورياً لضمان استقرار النظام السياسي وحماية المصالح الوطنية.

- **الأبعاد القانونية:** يشمل العلاقة بين القانون والتكنولوجيا، حيث تفرض التطورات التكنولوجية الحاجة لتحديث التشريعات القانونية لمواكبة الجرائم السيبرانية. تُعتبر هذه الجرائم معقدة بسبب صعوبة تحديد هوية الجناة، وقد تتجاوز الحدود

الجغرافية، مما يستدعي تطوير قوانين فعالة لمكافحةها. (عطية، 2019)

4.2 أهمية الأمن السيبراني

يعد الأمن السيبراني عنصراً أساسياً في مكافحة الجرائم الإلكترونية التي تنشأ في الفضاء الرقمي أو الافتراضي. هذه الجرائم، التي يُنفذها أفراد أو جماعات ذوو مهارات عالية في مجال التقنية، تسبب أضراراً جسيمة للمجتمعات والأفراد. في عالمنا المعاصر، الذي أصبح مترابطاً من خلال الإنترنت، أصبح الأمن السيبراني جزءاً لا غنى عنه في حياتنا اليومية على كافة الأصعدة السياسية والاقتصادية والاجتماعية. فقد أصبح ركيزة أساسية في المعاملات الإلكترونية للأفراد والدول على حد سواء، ويُعتبر الآن عنصراً حيوياً للأمن القومي والأمن الجماعي.

العلاقة بين التكنولوجيا والأمن تتزايد بشكل متسارع، حيث يُحتمل أن تتعرض المصالح الاستراتيجية للعديد من الأطراف إلى تهديدات إلكترونية خطيرة. هذا يبرز الدور الحيوي للأنظمة الإلكترونية في حماية هذه المصالح، مما يجعل الأمن السيبراني ركيزة أساسية لضمان استقرار النظام الرقمي وحمايته. (aicha، 2023)

العلاقة بين التكنولوجيا والأمن تتسارع بشكل متزايد، حيث يُحتمل أن تتعرض المصالح الاستراتيجية للعديد من الأطراف، سواء كانت حكومات أو شركات أو أفراد، إلى تهديدات إلكترونية متزايدة التعقيد والخطورة. وهذا يبرز بشكل جلي الدور الحيوي الذي تلعبه الأنظمة الإلكترونية في حماية هذه المصالح. إذا كان التقدم التكنولوجي يعزز من سرعة الاتصال وسهولة الوصول إلى المعلومات، فإنه أيضاً يزيد من تعقيد التهديدات السيبرانية ويجعل من الضروري تبني حلول أمنية متطورة ومرنة.

إن الأمن السيبراني لا يقتصر فقط على حماية البيانات، بل يشمل أيضاً حماية النظم الحيوية التي تشكل العمود الفقري للتفاعل الرقمي في العالم المعاصر. ولذلك، يصبح الأمن السيبراني ركيزة أساسية لضمان استقرار النظام الرقمي وحمايته من التهديدات المتزايدة التي قد تهدد أمن الأفراد والشركات والدول على حد سواء.

5.2 تأثير الهجمات السيبرانية على المؤسسات الاقتصادية

تؤدي الهجمات السيبرانية إلى خسائر مالية ضخمة قد تصل إلى مليارات الدولارات سنوياً. تعرضت العديد من الشركات الاقتصادية لهجمات سيبرانية استهدفت بياناتها باستخدام أسلوب الاختراق. على سبيل المثال، تعرضت شركة eBay الأمريكية في عام 2014 لسرقة 140 مليون حساب مستخدم، بينما تعرضت شركة الطيران البريطانية في عام 2018 لهجوم سيبراني كبير أدى إلى تدهور قيمة أسهم الشركة بشكل ملحوظ في البورصة (عزالدين، 2022)، صفحة 116) فعلى سبيل المثال شركة APPLE فعلى الرغم من سمعة شركة "آبل" كمؤسسة رائدة في مجال التكنولوجيا وأمن المعلومات، فقد تعرضت لخرق سيبراني غير متوقع قام به مراهق أسترالي يبلغ من العمر 16 عاماً. تمكن هذا المراهق من اختراق خوادم الشركة وسرقة حوالي 100 جيجابايت من البيانات الحساسة.

من الناحية الاقتصادية، حققت شركة "آبل" في عام 2019 إيرادات بلغت 260.2 مليار دولار أمريكي، مع تحقيق أرباح إجمالية بلغت 55.3 مليار دولار. كما وصلت قيمة أصول الشركة إلى 338.5 مليار دولار، في حين بلغ عدد موظفيها 137 ألف موظف. تعكس هذه الأرقام مكانة الشركة البارزة على الصعيدين الاقتصادي والتكنولوجي عالمياً.

(https://www.argaam.com/ar، 2021)

إليك الجدول التالي الذي يوضح:

الجدول رقم (1): ترتيب الشركات التي تعرضت لجرائم إلكترونية في عامي 2024 و2025

التاريخ	الشركة	النوع
1 فبراير 2024	Viamedis	تسريب بيانات ضخمة لمؤمنين
1 فبراير 2024	Almerys	تسريب بيانات ضخمة لمؤمنين
2 فبراير 2024	Etesia	هجوم "رانسوم وير"
28 فبراير 2024	Sidaction	سرقة بيانات المتبرعين
29 مارس 2024	Seiko و Hoya	اختراق خادم وتعطيل جزئي للإنتاج
3 أبريل 2024	باريس سان جيرمان (PSG)	محاولة اختراق لبوابة التذاكر مع احتمال سرقة بيانات شخصية
15 أبريل 2024	Le Slip Français	سرقة بيانات 696,000 عميل
19 أبريل 2024	Speedy France	سرقة بيانات شخصية

المصدر: <https://www.jedha.co/formation-cybersecurite/liste>

الهجمات السيبرانية تشكل تهديداً كبيراً للعديد من القطاعات الاقتصادية، حيث تؤثر على العمليات التجارية والمالية وتضر بسمعة الشركات. فيما يلي بعض القطاعات الاقتصادية الأكثر تأثراً بهذه الهجمات

الشكل رقم (1): القطاعات الاقتصادية الأكثر تأثراً بالهجمات السيبرانية.



المصدر: (عزالدين، 2022)

تترك الهجمات الإلكترونية تداعيات اقتصادية واجتماعية كبيرة على الشركات. الخسائر المالية تتمثل في تعطيل العمليات التجارية ودفع فدية في حالة هجمات "الرانسوم وير"، بالإضافة إلى فقدان البيانات التي يصعب استعادتها. كما يؤدي تسريب البيانات إلى فقدان ثقة العملاء والمستثمرين، مما قد يضر بسمعة الشركة ويؤدي إلى تراجع قاعدة عملائها. أما تكاليف التعافي فتشمل استعادة البيانات والتحقيق في الحادث، إضافة إلى تحسين الأمان لضمان عدم تكرار الهجمات، مما يشكل عبئاً مالياً وزمنياً على الشركات.

6.2 أثر الأمن السيبراني على الأسواق المالية

في ظل تزايد الرقمنة، وتطور التقنيات، وتصاعد التوترات الجيوسياسية، تزداد المخاطر الإلكترونية رغم أن الحوادث الإلكترونية لم تكن حتى الآن منهجية، إلا أن خطر الخسائر الكبيرة من هذه الحوادث قد زاد ويعتبر القطاع المالي معرضاً بشكل كبير، وقد تشكل الحوادث الإلكترونية الخطيرة مخاطر على الاستقرار المالي الكلي من خلال فقدان الثقة، وتعطيل الخدمات الحيوية، وانتقال الآثار إلى مؤسسات أخرى من خلال الروابط التكنولوجية والمالية.

فبالرغم من تحسين التشريعات الإلكترونية وترتيبات الحوكمة المتعلقة بالأمن السيبراني في الشركات إلا أن أطر السياسات الإلكترونية لا تزال غير كافية بشكل عام، خاصة في الأسواق الناشئة والاقتصادات النامية. لذلك، يجب تعزيز مرونة القطاع المالي في مواجهة المخاطر الإلكترونية من خلال تطوير استراتيجيات وطنية للأمن السيبراني المناسبة، وأطر تنظيمية وإشرافية ملائمة، وقوة عمل قادرة على التعامل مع الأمن السيبراني، وترتيبات لتبادل المعلومات على الصعيدين المحلي والدولي. ولتمكين المراقبة الفعالة للمخاطر الإلكترونية، يجب تعزيز تقارير الحوادث الإلكترونية. ينبغي على المشرفين تحميل أعضاء مجالس الإدارة مسؤولية إدارة الأمن السيبراني في الشركات المالية وتعزيز ثقافة المخاطر المناسبة، والنظافة السيبرانية، والتدريب والوعي في مجال الأمن السيبراني. للحد من الاضطرابات المحتملة، يجب على الشركات المالية تطوير واختبار إجراءات الاستجابة والتعافي. يجب على السلطات الوطنية تطوير بروتوكولات استجابة فعالة وأطر لإدارة الأزمات (Fund., 2024).

الشكل رقم (2): تهديد الحوادث السيبرانية على الإستقرار المالي الكلي

Cyber incidents pose an increasing threat to macrofinancial stability.



SOURCE: International Monetary Fund

يمثل الشكل البياني تهديد الحوادث السيبرانية (Cyber Incidents) على الإستقرار المالي الكلي (Macrofinancial Stability). وهي تتضمن رسماً بيانياً يوضح الحد الأقصى المقدّر للخسائر السنوية للشركات نتيجة لهذه الحوادث في عامي 2017 و2021، بالإضافة إلى مجموعة من السياسات المقترحة لمواجهة هذه التهديدات.

التحليل: المحور العمودي يمثل الخسائر السنوية القصوى المقدرة للشركات بمليارات الدولارات، المحور الأفقي يعرض نقطتين رئيسيتين: المتوسط (Median) والنسبة المئوية. اللون البرتقالي يمثل عام 2017، بينما اللون الأخضر يمثل عام

2021، من الرسم يتضح أن الخسائر المقدرة ازدادت بشكل ملحوظ بين 2017 و2021، خصوصاً عند النسبة المئوية الـ 90، حيث كانت أقل من 1 مليار دولار في 2017، لكنها قفزت إلى أكثر من 2.5 مليار دولار في 2021.

السياسات المقترحة لمواجهة تهديدات الهجمات السيبرانية: تطوير استراتيجيات وطنية للأمن السيبراني من خلال وضع تنظيمات ورقابة فعالة وكذا تحسين الإبلاغ عن البيانات وتبادل المعلومات لتعزيز الوعي بالمخاطر السيبراني وتعزيز إجراءات الاستجابة والتعافي لتحسين قدرة المؤسسات على مواجهة الحوادث السيبرانية وتقليل تأثيرها. إن التهديدات السيبرانية للشركات أصبحت أكثر خطورة خلال السنوات الأخيرة، حيث زادت الخسائر السنوية المقدرة بشكل ملحوظ. ومن أجل حماية الاستقرار المالي، هناك حاجة إلى سياسات فعالة لتعزيز الأمن السيبراني والاستجابة للحوادث.

3. التحديات التي تواجه البنوك الجزائرية في مجال الأمن السيبراني

في عصر التحول الرقمي، تواجه البنوك والمؤسسات المالية العديد من المخاطر التي قد تؤثر على أمانها واستقرارها المالي و من أبرز هذه المخاطر:

1.3 الفيروسات وبرامج التجسس والتسريبات:

يعتبر تسريب كلمات السر أحد أكبر التهديدات الأمنية في البنوك والمؤسسات المالية، حيث تُستخدم كلمات السر للتعرف على هوية العميل في الأنظمة الإلكترونية. أي تسريب لهذه المعلومات قد يتيح للمهاجمين الوصول إلى حسابات العملاء بشكل غير قانوني. وتستخدم كلمات السر في العديد من الأنظمة مثل الإنترنت المصرفي، الصراف الآلي، والهاتف المصرفي.

الفيروسات هي برامج خبيثة قد تتسلل إلى أنظمة الكمبيوتر دون علم المستخدم بهدف تدمير البيانات أو تعطيل النظام. كما يمكن أن تستخدم الفيروسات لسرقة المعلومات الشخصية أو المصرفية، ما يجعلها تهديداً خطيراً للبنوك والمؤسسات المالية. تنتقل الفيروسات عبر الإنترنت، البريد الإلكتروني، والوسائط المتنقلة مثل الأقراص المدججة (CD)، الأقراص المرنة

(Floppy Disk)، وشرائح الذاكرة (Memory Stick). (موراد، 2023، صفحة 1407)

2.3 جمع المعلومات الاقتصادية الاستخباراتية:

يتم عبر اختراق قواعد البيانات المالية والمصرفية وقواعد بيانات الشركات والبنوك، بهدف جمع معلومات قد تؤثر على الأمن الوطني للدول. كما يتم التجسس على المسؤولين الماليين ووزراء المالية ورؤساء الشركات الكبرى. في هذا السياق، أصدر الرئيس الأمريكي الأسبق باراك أوباما خلال فترة ولايته الثانية أوامر بوقف التنصت على مقرري صندوق النقد الدولي والبنك الدولي، وذلك في إطار مراجعة أنشطة جمع المعلومات الاستخباراتية بعد التسريبات التي كشف عنها المتعاقد السابق مع وكالة الأمن القومي إدوارد سنودن، والتي أوضحت برامج لجمع بيانات ضخمة عن حلفاء وأعداء الولايات المتحدة، بالإضافة إلى المواطنين الأمريكيين.

وفي واقعة أخرى، في عام 2014، شنت كوريا الشمالية هجوماً إلكترونياً على شركة سوني للإنتاج السينمائي (Sony Pictures Entertainment)، مما أدى إلى تعطيل آلاف أجهزة الكمبيوتر الخاصة بالشركة. كما تم اختراق معلوماتها التجارية السرية وسرقة نسخ رقمية لأفلام لم تُطلق بعد، بالإضافة إلى آلاف المستندات التي تحتوي على بيانات حساسة عن شخصيات بارزة وموظفي الشركة (كلاع، 2022، صفحة 303)

3.3 نقص الكفاءات المتخصصة

يواجه قطاع الأمن السيبراني نقصاً في الكفاءات المتخصصة اللازمة للتصدي للتهديدات المتزايدة، مما يعزز الحاجة الملحة للمؤسسات للحصول على خبرات متخصصة في هذا المجال. ورغم أن هذا النقص يفتح فرصاً كبيرة للعمل في القطاع، إلا أنه يشكل تحدياً في التكيف السريع مع التهديدات المستمرة والمتجددة. (<https://batdacademy.com>)

4.3 البنى التحتية القديمة:

رغم تزايد الرقمنة، لا تزال العديد من الصناعات تعتمد بشكل كبير على أنظمة الأمان التقليدية، مما يتيح للمهاجمين السيبرانيين فرصة الاستفادة من الثغرات الموجودة في البنية التحتية القديمة. علاوة على ذلك، تعتمد معظم الشركات على مصادر خارجية لإدارة العمليات غير المرتبطة بكفاءاتها الأساسية، مما يؤدي إلى شبكة معقدة من التقنيات والخدمات التي تعاني من مشكلات، مما يزيد من سطح الهجوم ويفقد الشركات الرؤية والتحكم الكافيين. بالإضافة إلى ذلك، يشكل نقص الميزانية والخبرة في مجال الأمن السيبراني تحدياً إضافياً للشركات الصغيرة. (تصاعد تهديدات الأمن السيبراني على البنى التحتية الحرجة في الشرق الأوسط، 2023)

4. إستراتيجيات تعزيز الأمن السيبراني في البنوك الجزائرية

شهدت الجزائر في السنوات الأخيرة تطوراً سريعاً في مجال تكنولوجيا المعلومات والاتصالات، مما يشكل شرطاً ضرورياً للتحويل نحو الاقتصاد الرقمي واعتماد نهج الحكومة الإلكترونية الذي يركز على المواطن. ومع ذلك، فإن هذا التحول يتطلب تأمين وحماية جميع الأنظمة الرقمية وتدفقات المعلومات الخاصة بها. هذا وقد أدت التهديدات المحتملة للهجمات السيبرانية ضد تكنولوجيا المعلومات والاتصالات إلى خسائر اقتصادية وإلى خلق مناخ من انعدام الأمن وعدم اليقين تجاه الخدمات الرقمية. وهذا ما يستدعي تطبيق تدابير مضادة تحمي المؤسسات والبنى التحتية الحيوية، وتحافظ على المصالح الحيوية للبلاد وتعزز الأمن الوطني، والبنوك باعتبارها من أهم المؤسسات المعرضة للهجمات السيبرانية فإنها سعت بدورها إلى البحث عن أساليب وحلول للتقليل من هذه المخاطر أو تجنبها وفقاً لاستراتيجية أمنية تعتبر جزءاً لا يتجزأ من الإستراتيجية الوطنية الشاملة لتعزيز الأمن السيبراني وتمثل أهم عناصر هاته الاستراتيجية فيما يلي:

1.4 أهمية وجود معايير محددة تنظم المخاطر السيبرانية

تعدد الآراء والوجهات حول كيفية تنظيم مخاطر الإنترنت، فبينما يرى البعض أن الطبيعة المتغيرة والمتطورة باستمرار للهجمات السيبرانية تجعل من الصعب تحديد إطار تنظيمي ثابت لها، فإنهم يعتبرون أن القضايا المتعلقة بالإنترنت يمكن إدراجها ضمن الأطر التنظيمية الحالية التي تتعامل مع المخاطر التشغيلية والتقنيات المصرفية. هذا الرأي يعتمد على أن المؤسسات المالية يمكنها تكيف استراتيجيات الأمن السيبراني ضمن الأنظمة الموجودة، على اعتبار أن هذه الأنظمة قد تغطي بعض الجوانب المتعلقة بالتهديدات السيبرانية. ومع ذلك، لا يمكن إغفال أن المخاطر الرقمية تتسم بخصوصية تتطلب استجابة مرنة وسريعة، وبالتالي فإن البعض يرى أنه من الضروري إنشاء هيكل تنظيمي متخصص يركز على معالجة التحديات الفريدة التي تطرحها هذه المخاطر، خاصة في ظل التحول السريع نحو الرقمية في القطاع المالي في السنوات الأخيرة.

يشير آخرون إلى أن المؤسسات المالية يجب أن تواكب التطور المستمر في المخاطر السيبرانية من خلال البحث المستمر عن تدابير وقائية فعالة، وهو ما يتطلب وضع لوائح تنظيمية قوية. هذه اللوائح يمكن أن توضح السياسات والخطوات التي يجب أن يتبناها مجلس إدارة المؤسسة، وبالتالي تعزيز الحوافز اللازمة للاستثمار المستمر في أمن المعلومات. على الرغم من أن تصنيف

المخاطر السيبرانية ضمن المخاطر التشغيلية قد يبدو مناسباً في بعض الأحيان، إلا أن هذه الطريقة لا تعد كافية لمواجهة التحديات المتزايدة. حيث يتطلب الوضع الراهن وضع استراتيجيات واضحة ومفصلة لإدارة المخاطر الإلكترونية، وتحديث المعايير الرقابية للبنوك لتشمل متطلبات خاصة بالأمن السيبراني.

لذلك، ينبغي أن تشمل المعايير الرقابية الحديثة على أطر شاملة تهدف إلى إدارة المخاطر السيبرانية بشكل منفصل وفعال. من الضروري أن تتضمن هذه المعايير سياسات وإجراءات واضحة يجب أن تلتزم بها البنوك لضمان حماية بيانات عملائها وضمان سلامة المعاملات المصرفية الرقمية. كما يجب أن تتم مراجعة هذه السياسات بشكل دوري من قبل مجالس الإدارة، خصوصاً مع تزايد حجم التهديدات والهجمات السيبرانية في القطاع المالي. هذا النوع من المراجعات يضمن البقاء على اطلاع دائم بأحدث أساليب الهجوم والتقنيات المتاحة لمكافحتها، ومن أهم المعايير المنظمة للمخاطر السيبرانية نجد (اسماعيل، 2019)

1.1.4 الحوكمة الإلكترونية: الحوكمة الرقمية هي استخدام تقنيات المعلومات والاتصالات بهدف تعزيز الحوكمة

الفعالة، مما يساهم في تحسين وتطوير الأداء الحكومي وزيادة الشفافية والكفاءة. ويمكن تلخيص عناصر الحوكمة الرقمية في النقاط التالية:

الإدارة الرقمية: تشير إلى تحسين العمليات الحكومية عبر توظيف التكنولوجيا لخفض النفقات وتحسين سير العمل الحكومي، وذلك من خلال تسهيل التواصل والتنسيق بين الهيئات الحكومية المختلفة.

- المواطنون الرقميون: تعني تمكين المواطنين من التفاعل مع الحكومة بشكل إلكتروني، مما يساهم في تعزيز الديمقراطية من

خلال إشراك المواطنين في اتخاذ القرارات وتحسين جودة الخدمات العامة عبر الاستماع إلى آرائهم واحتياجاتهم.

- المجتمع الرقمي: يشمل هذا العنصر تعزيز التعاون بين الحكومة وقطاعات أخرى مثل القطاع الخاص والمجتمع المدني، بهدف تحسين التنسيق والعمل المشترك لتحقيق أهداف التنمية الشاملة (إيمان، 2023).

و يتجلى ذلك من خلال وجوب وجود استراتيجية للأمن السيبراني بحيث تضع كل مؤسسة مالية استراتيجية الأمن السيبراني الخاصة بها وفقاً لممارسات إدارة المخاطر المستندة إلى عدة مبادئ. تقوم الجهات الرقابية بمراجعة هذه الاستراتيجيات كجزء من تقييمها للممارسات الشاملة لإدارة المخاطر في المؤسسة. كما أن جميع الجهات الرقابية تؤكد على أهمية الأدوار والمسؤوليات الإدارية والضوابط الخاصة بالحوكمة الإلكترونية إضافة إلى أهمية الأدوار والمسؤوليات الإدارية والضوابط الخاصة بالحوكمة الإلكترونية. إضافة إلى أهمية تنمية الوعي الثقافي للأمن السيبراني للعاملين في القطاعات المالية. كما تؤكد على أهمية توافر الكوادر المدربة القادرة على تحمل المسؤوليات والقيام بالمهام الوظيفية الموكلة إليها في مجال الأمن السيبراني. (اسماعيل، 2019)

2.1.4 مفاهيم حول إدارة المخاطر واختبارها وكيفية التغلب على الانتهاكات: و يتمثل ذلك في تحديد طرق الرقابة على الأمن السيبراني، ضوابط أمن المعلومات وطرق اختبارها وضمان استقلاليتها، مدى الاستجابة للتغلب على المخاطر، ومقاييس الأمن السيبراني والمرونة. (اسماعيل، 2019)

3.1.4 التواصل وتبادل المعلومات: من بين الأنماط المتعارف عليها للتواصل في مجال مشاركة أهم الممارسات في مجال الأمن السيبراني، يعتبر مشاركة المعلومات بين البنوك، والمشاركة بين البنوك والجهات الرقابية ومشاركة تلك المعلومات مع الأجهزة الأمنية من أكثر الممارسات المتعارف عليها في هذا المجال.

4.1.4 تعهيد أمن نظم المعلومات والأنظمة الإلكترونية إلى جهة ثالثة: إن الاستخدام المكثف لخدمات التعهيد إلى طرف ثالث يزيد من التحدي أمام الهيئات والجهات الرقابية للحصول على رؤية كاملة للضوابط المعمول بها ومستوى المخاطر.

هذا وتمثل خدمات التعهيد إلى جهة ثالثة في كافة أشكال الاستعانة بمصادر خارجية بما في ذلك خدمات الحوسبة السحابية، والخدمات والمنتجات المعيارية وغير المعيارية التي لا تعتبر عادة مصادر خارجية، خطوط الاتصالات السلكية واللاسلكية، الأجهزة والبرامج التجارية.. والأطراف الأخرى مثل (المؤسسات المالية أو غير المالية) والمؤسسات المالية الدولية (مثل أنظمة الدفع والتسوية، منصات التداول، أمناء حفظ الأوراق المالية المركزية..).

2.4 المرجع الوطني لأمن المعلومات (RNSI):

أصدرت الجزائر مرجعا وطنيا لأمن المعلومات والذي يعتبر إطارا تنظيميا للأمن السيبراني سنة 2020 يتضمن عشرين مجالا تبعا للنسخة الأولى التي تم إطلاقها سنة 2016 بقيادة وزارة البريد والاتصالات السلكية واللاسلكية والشؤون الرقمية والتي تشمل سبعة محاور فقط. والهدف من وراء إعداد هذا المرجع يكمن في إقامة حوكمة ونهج موحد لأمن المعلومات داخل الهيئات والمؤسسات. هذا المرجع يحدد الحد الأدنى من المتطلبات المتعلقة بالأمن وذلك من أجل تسيير ومقاومة والتقليل من أثر التهديدات المتوقعة. زيادة على ذلك، فإن مرجع أمن المعلومات يقدم الضوابط الأمنية وأفضل المؤسسات التي يمكن ان تتبناها الهيئات العمومية، مع التركيز على تدريب وتوعية المستخدمين بالمخاطر التي تنطوي عليها، والتقييم الدوري للضوابط من أجل ضمان الاستجابة المستمرة للمتطلبات الأمنية والامتثال للالتزامات التنظيمية. و تتمثل المجالات التي يتضمنها هذا المرجع في : الأمن المادي ، أنترنت الأشياء ، المراقبة و تسجيل الوقائع ، إدارة الحوادث الأمنية ، تسيير استمرارية النشاطات ، الموارد البشرية، الأمن المتعلق باستخدام مواقع التواصل الاجتماعي ،دمج الأمن خلال دورة حياة تطوير البرمجيات ،متطلبات الأمن لمشاريع تكنولوجيا الاعلام و الاتصال ،العلاقة مع الأطراف الثالثة ،إدارة الموجودات ،حماية البيانات ذات الطابع الشخصي ،إدارة و مراقبة النفاذ، أمن أجهزة الموجودات ذات الطابع الشخصي ،إدارة و مراقبة النفاذ ،أمن أجهزة المحمول ،أمن الشبكات ،أمن أنظمة المعلومات ،الأمن المتعلق بالتشغيل ،أمن أنظمة المعلومات بالغ الأهمية ،أمن الحوسبة السحابية و التشفير . (Referential de security des information, -2025)

3.4 حماية و تأمين النطاق المعلوماتي

وتم ذلك من خلال التركيز على ثلاث نقاط رئيسية تتمثل في:

1.3.4 الجانب القانوني: حيث تم إصدار جملة من القوانين التنظيمية أهمها قانون 04-15 المتضمن تعديل قانون العقوبات ،حيث خصص قسمه السابع مكررا للمساس بأنظمة المعالجة الآلية للمعطيات.

إصدار القانون 04-09 المؤرخ في 05 أوت 2009 والذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها حيث يهدف هذا القانون إلى حماية أنظمة معالجة البيانات الآلية من الجرائم.

نص المادة 394 مكرر 1 من قانون العقوبات الجزائري التي نصت على أنه “يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500000 دج إلى 2000000 دج كل من أدخل عن طريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها “. (عائشة، 2023)

2.3.4 التطوير التقني: تعتبر طبيعة الجريمة الالكترونية و انفرادها بسميزات خاصة كانهدام الحواجز الجغرافية ،و صعوبة الكشف عن هوية المستخدم من الدواعي التي تفرض التسليح بأحدث الوسائل التقنية للتمكن من مجابهة أخطارها ، و لهذا يستلزم على الجهات المختصة بالأمن السيبراني و التحقيق في الجرائم المتصلة بالمعلوماتية أن تمتلك الوسائل و التقنيات اللازمة و التي يمكن حصر أهمها في: (عائشة، 2023)

- تنمية وتعزيز القدرات البشرية

- توافر أحدث المعدات التكنولوجية في مجال الإعلام الآلي، الاتصالات اللاسلكية.

- التمتع بقاعدة بيانات واسعة محدثة باستمرار

- القدرة على تصميم البرامج المعلوماتية وتطويرها

3.3.4 الجهاز العملي: و يتمثل في مختلف المراكز و الوحدات التي تم إنشاؤها لغرض مواجهة الجريمة الالكترونية و ضمان

الامن السيبراني لمختلف المؤسسات منها (عائشة، 2023)

- مركز الوقاية من جرائم الاعلام الآلي والجرائم المعلوماتية للدرك الوطني

- المعهد الوطني للأدلة الجنائية وعلو الاجرام للدرك الوطني

- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني

- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها

استحداث قطب جزائي جديد مكلف بمتابعة الجرائم السيبرانية

4.3.4 جاهزية بنية الجهاز المصرفي المادية و البشرية

تسعى مختلف البنوك والمصارف إلى تهيئة وتحديث أنظمتها الإلكترونية وانظمة الامن السيبراني وكذا التطوير من كفاءة مواردها البشرية للتقليل أو تجنب المخاطر المدركة للعملاء المرتبطة خصوصا بالخدمات الرقمية المقدمة.

5.3.4 تطوير أنظمة أمن المعلومات المصرفية

أن مفهوم الأمن السيبراني يندرج ضمن مفهوم أمن المعلومات لأنه أشمل وأوسع نطاقاً. تتنوع هذه المخاطر وتزداد مع تعدد أساليب القرصنة والاختراق، ونظراً لأن العامل البشري يعد أحد أسبابها الرئيسية، يتم تصنيفها كأحد أشكال المخاطر التشغيلية، ويتم إدارتها ضمن هذا النطاق. هذا وقد تم تسجيل أن القطاع المالي يعتبر هدفاً في مواجهة الهجمات السيبرانية، نظراً لقدرة القراصنة على نشر الهجوم بسرعة عبر النظام المالي المترابط، بالإضافة إلى أن العديد من المؤسسات المالية لا تزال تعتمد على الأنظمة الرقمية القديمة. وقد تم رصد 91% من الهجمات في البنوك، وكان أكثر من 68% منها عبارة عن

هجمات تصيد إلكتروني خلال عام 2020 (LAIB, 2021)

لذلك فإن أغلبية البنوك تسعى إلى تطوير أنظمة المعلومات الخاصة بها وبحمية العملاء من خلال ضمان ثلاث مبادئ أساسية والمتمثلة في سرية المعلومة، صحة المعلومة وتوافر المعلومة.

5. الخاتمة:

ختاماً، يمكن القول إن الأمن السيبراني في البنوك الجزائرية يعد حجر الزاوية لضمان استقرار النظام المالي في مواجهة التحديات الرقمية المعاصرة. في الوقت الذي تتسارع فيه وتيرة التحول الرقمي في القطاع المصرفي، تبقى البنوك بحاجة ماسة إلى تطوير استراتيجيات مبتكرة تتماشى مع هذه التحولات، وفي نفس الوقت تكون قادرة على التصدي للتهديدات السيبرانية التي قد تنشأ في المستقبل.

إن الأمن السيبراني يجب أن يُنظر إليه من قبل البنوك الجزائرية ليس فقط كآلية دفاعية لحماية البيانات والأنظمة من الهجمات، بل كاستثمار طويل المدى يعود بالفائدة على جميع الأطراف المعنية. فهو يعزز ثقة العملاء في المؤسسات المالية ويؤمن استمرارية العمليات المصرفية بشكل آمن، مما يساهم بشكل كبير في الحفاظ على سمعة القطاع المصرفي ككل. إن تبني نهج استباقي في هذا المجال هو ما سيجعل البنوك الجزائرية قادرة على مواجهة تحديات العصر الرقمي بثقة وثبات ومن المهم أيضاً

أن يركز هذا النظام الأمني على شراكات استراتيجية مع الهيئات الحكومية والقطاع الخاص، حيث أن التعاون بين جميع الأطراف المعنية يساهم في تعزيز الجهود الأمنية، وتبادل المعرفة والخبرات لمواكبة أحدث التقنيات والتهديدات السيبرانية. بالإضافة إلى ذلك، يجب أن تتبنى البنوك برامج تدريبية مستمرة لموظفيها على تقنيات الأمن السيبراني الحديثة، كما يجب رفع الوعي لدى العملاء حول أهمية حماية بياناتهم الشخصية والمعاملات المصرفية.

وفي النهاية، مع التوجه الصحيح والاستثمار المستمر في تقنيات الأمن السيبراني، يمكن للبنوك الجزائرية أن تبني بيئة مصرفية آمنة ومرنة، قادرة على التكيف مع التحديات المستقبلية. هذا سيمكنها من المحافظة على استقرار النظام المالي وتعزيز الثقة في القطاع المصرفي، مما يساهم في تحقيق تنمية اقتصادية مستدامة في البلاد.

1.5 النتائج:

- تعزيز الوعي الأمني لدى العملاء والمستخدمين من العوامل الأساسية في الحد من المخاطر المرتبطة بالتهديدات السيبرانية.
- تعمل البنوك على تحديث وتطوير أنظمتها الإلكترونية وأنظمة الأمن السيبراني، بهدف تقليل أو تجنب المخاطر التي قد يدرکہا العملاء، خاصة تلك المتعلقة بالخدمات الرقمية المقدمة.
- نتيجةً للحكومة الإلكترونية يتبين ضرورة وجود استراتيجية للأمن السيبراني تعتمد عليها كل مؤسسة مالية وفقاً لممارسات إدارة المخاطر، حيث تقوم الجهات الرقابية بمراجعة هذه الاستراتيجيات ضمن تقييمها للممارسات الشاملة لإدارة المخاطر -ترك الهجمات الإلكترونية تداعيات اقتصادية واجتماعية كبيرة على الشركات، تشمل خسائر مالية نتيجة تعطيل العمليات، وفقدان البيانات، بالإضافة إلى تراجع ثقة العملاء والمستثمرين، مما يؤثر سلباً على سمعة الشركة

2.5 التوصيات :

- ينبغي على البنوك الجزائرية الاستثمار في التقنيات الحديثة مثل الذكاء الاصطناعي، وتعلم الآلة، لتوفير حماية متقدمة ضد الهجمات السيبرانية، وضمان استمرارية النظام المالي.
- توصي الدراسة بضرورة قيام البنوك الجزائرية بتحديث وتطوير البنية التحتية للأمن السيبراني بشكل دوري لمواكبة التغيرات التكنولوجية المتسارعة وزيادة القدرة على مواجهة التهديدات الإلكترونية الحديثة.
- يجب على البنوك الجزائرية إنشاء وحدات متخصصة للأمن السيبراني ، تتولى مهام مراقبة الأنظمة بشكل مستمر وتطوير خطط إتراتيجية لمواجهة للتهديدات

6. الهوامش والإحالات

Fund., I. M. (2024). *Global Financial Stability Report*.

<https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024>.

./ (بلا تاريخ). ما هو مستقبل الأمن السيبراني؟ <https://batdacademy.com>

<https://batdacademy.com/ar/post/%D9%85%D8%A7-%D9%87%D9%88-%D9%85%D8%B3%D8%AA%D9%82%D8%A8%D9%84-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A>.

.(2021)<https://www.argaam.com/ar> .

Kada aicha .(2023) .The security and cyber defence realities and difficulties in Algeria . *Journal of Police and Legal Sciences*.

