الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة محمد خيضر – بسكرة –
كلية العلوم الاقتصادية والتجارية وعلوم التسيير
قسم العلوم التجارية

الموضـــــــــوع:

مساهمة الأمن السيبراني في تعزيز الاستقرار المالي
دراسة حالة: شركة تارجت *Target*

مذكرة مقدمة كجزء من متطلبات نيل شهادة ماستر أكاديمي في العلوم التجارية
تخصص: مالية وتجارة دولية

من إعداد الطلبة:

- منال بوزرقون
- هناء بوزيان

الأستاذ (ة) المشرف(ة)

أ. د/ الغالي بن براهيم

لجنة المناقشة

أعضاء اللجـنة	الرتبة	الصـفـة	الجامعة
- عمري ريمة	أستاذ محاضر (أ)	رئيسا	بسكرة
- الغالي بن براهيم	أستاذ	مقررا	بسكرة
- دبابش رفيعة	أستاذ محاضر (أ)	مناقشا	بسكرة

الموسم الجامعي: 2024/2025

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة محمد خيضر – بسكرة –
كلية العلوم الاقتصادية والتجارية وعلوم التسيير
قسم العلوم التجارية

الموضـــــــــوع:

مساهمة الأمن السيبراني في تعزيز الاستقرار المالي
دراسة حالة: شركة تارجت *Target*

مذكرة مقدمة كجزء من متطلبات نيل شهادة ماستر أكاديمي في العلوم التجارية
تخصص: مالية وتجارة دولية

من إعداد الطلبة:

- منال بوزرقون
- هناء بوزيان

الأستاذ (ة) المشرف(ة)

أ. د/ الغالي بن براهيم

لجنة المناقشة

أعضاء اللجـنة	الرتبة	الصـفـة	الجامعة
- عمري ريمة	أستاذ محاضر (أ)	رئيسا	بسكرة
- الغالي بن براهيم	أستاذ	مشرفا	بسكرة
- دبابش رفيعة	أستاذ محاضر (أ)	مناقشا	بسكرة

الموسم الجامعي: 2024/2025

بسم الله الرحمان الرحيم

شكر وعرفان

بسم الله الرحمان الرحيم

الحمد لله الذي وفقني وسدد خطاي لإتمام هذه المذكرة بنجاح. أتقدم بخالص الشكر والتقدير إلى كل الأشخاص الذين ساهموا في إنجاز هذا العمل العلمي.

شكرا لأسرتي العزيزة التي كانت دائما مصدر الدعم والتشجيع لي من خلال هذه الرحلة العلمية.

شكرا لأساتذتي الكرام الذين شاركوني من خبراتهم الثمينة وقدموا لي الإرشاد والنصح لتحقيق أفضل النتائج، وفتحوا لي آفاقا جديدة في المعرفة. وبالأخص الأستاذ المشرف **"الغالي بن براهيم"** على هذا العمل، شكرا على ارشاداته القيمة التي كانت سببا في نجاح هذا العمل.

شكرا لكل زملائي الذين شاركوني الأفكار والتجارب وساهموا في إثراء مذكرتي بآرائهم وملاحظاتهم القيمة.

تقديري العميق لكل من قام بمساعدتي في إنجاز هذه المذكرة، ولن أنسى أبدا العطاء الكبير الذي قدمتموه.

تقبلوا مني فائق الاحترام والتقدير، وجزاكم الله خيرا.

والسلام عليكم ورحمة الله تعالى وبركاته.

الإهداء

يقول الله تعالى: {يرفع الله الذين آمنوا منكم والذين أوتوا العلم درجات والله بما تعملون خبير} المجادلة: 11

إلى مصدر الأمان الذي استمد منه قوتي، إلى من كانت الداعم الأول لتحقيق طموحي، إلى رفيقة رحلتي وحبيبة أيامي ومعلمتي الأولى وملهمتي، إلى القلب الحنون والصافي.

الى أمي الغالية

إلى من مهد طريق العلم لي، إلى من أنار دروب علمي بنور لا ينطفئ، العزيز الذي سار في كل دروب وفي كل طريق حتى وصولي إلى هنا، شكرا على صبرك وعلى حبك وعلى كل ما قدمته لي.

الى أبي الغالي

إلى من أتقاسم معهم الضحك والحزن، إلى من يمنحونني السعادة والدفء والنور، أود ان أهديكم هذا العمل المتواضع ليكون فخرا لكم.

إخوتي وأخواتي

إلى روح أختي الطاهرة دمت بنعيم ربي حتى نلتقي، اللهم اجعل قبرها روضة من رياض الجنة واغفر لها وارحمها واجبر قلوبنا على فراقها.

إلى صديقتي ورفيقة دربي في العمل والتي ساندتني عندما كان الأمر صعبا قليلا لك مني كل الحب والاحترام والتقدير.

هناء

إلى صديقاتي المقربات الجميلات، فراشاتي، أتمنى لكم حياة مليئة بالمفاجآت والخيرات والعمل والزوج الصالح الذي يسعدكم.

الى كل من أحبه

منال

الإهداء

يقول الله تعالى:{ **وقُلِ اعْمَلُوا فَسَيَرَى اللهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ**} التوبة:105

الحمد الله الذي بفضله تحقق الغايات بعد الاستعانة به وانهاء الدرب بتوفيقه، عظم المراد وهان الطريق فجاءت لذة الوصول لتمحي مشقة السنين.

إلى من أحمل اسمه فخرا واعتزازا، إلى من غيبه التراب، ولم تغب ذكراه عن قلبي، إلى من فارقني بجسده، وبقيت روحه ترافقني وتؤنس دربي أهدي هذا النجاح لروحك الطاهرة، **والدي الغالي – رحمه الله–**

الى رفيقة الروح مؤنسة الدرب الى من مسكت بيدي لنهاية المشوار جنتي امي اهديك نجاحي وتخرجي فما كان ليتحقق لولا توفيق الله ثم رفع كفيك بعد كل صلاة. **أمي الغالية**

إلى أولئك الذين تقاسموا معي تفاصيل الحياة، وشاركوني الصمت قبل الكلام، والثقل قبل الإنجاز إلى إخوتي وأخواتي كل باسمه، الذين كانوا الحصن في أوقات الانكسار، والدافع حين خفت العزم، والفرح حين حل النجاح.

إلى من كانت لي الأخت، والصديقة، يا من جمعتنا الجامعة وفرقتنا الطرق بعد التخرج، إلى من تقاسمت معي مشقة السهر وعزيمة الجد والاجتهاد لا يسعني إلا أن أقول: أن هذا الإنجاز لا يكتمل فرحه إلا بمشاركتك صديقتي الصدوقة

منال

إلى من جمعتني بهن الأيام لا صدفة، بل نعمة إلى من كن رفيقات السعي، وسند الدرب، وصوت الطمأنينة في زحام التحديات، إلى صديقاتي العزيزات كنتن زادا للروح وبهجة في الطريق، أهدي هذا النجاح إلى تلك الأرواح النقية التي ما بخلت يوما بمساندتي، فكنتن من أجمل ما كسبته في هذه الرحلة.

هناء

ملخص:

من أبرز التهديدات التي تتعرض لها الشركات هي محاولات سرقة أموال العملاء وبياناتهم، لا سيما عندما تفتقر الشركة إلى نظام أمني قوي أو اعتماد تقنيات الأمن السيبراني الفعالة، مما يزيد من صعوبة التصدي لهذه الهجمات وتقليل الخسائر المالية الناتجة عنها.

وعلى هذا الأساس أتت هذه الدراسة الموسومة ب: **مساهمة الأمن السيبراني في تعزيز الاستقرار المالي (دراسة حالة شركة تارجت)**، لتحليل متغيرين رئيسيين: الأمن السيبراني كمتغير مستقل والاستقرار المالي كمتغير تابع مع استكشاف العلاقة بينهما.أما على الصعيد التطبيقي، فقد ركزت الدراسة على تحليل استراتيجيات الأمن السيبراني المعتمدة في شركة تارجت، وتقييم أدائها المالي خلال الفترة (2022–2024)، إلى جانب تحليل الآثار المالية الناتجة عن الهجمات الإلكترونية التي تعرضت لها خلال سنة 2013. كما تم تقييم مسار تعافي الشركة من تلك الهجمات وصولا إلى تحقيق الاستقرار المالي. وقد خلصت الدراسة إلى أن الأمن السيبراني يعد تقنية معتمدة لحماية البيانات الحساسة للشركة والعملاء، والحد من المخاطر التي تهدد أمن المنظمة واستقرارها المالي.

الكلمات المفتاحية: الأمن السيبراني، الاستقرار المالي، التهديدات السيبرانية، الهجومات السيبرانية.

Summary :

One of the most prominent threats facing companies is attempts to steal customers money and data, especially when the company lacks a strong security system or relies on ineffective cybersecurity technologies. This makes it more difficult to counter these attacks and reduce the resulting Financial losses.

Based on this, this study, titled "**The Contribution of Cybersecurity to Enhancing Financial Stability (A Case Study of Target Corporation)**" was conducted to analyse two main variables : cyber Security as an independent variable and financial stability as a dependent variable, while exploring the relationship between them. On the practical level, the study focused on analyzing the cybersecurity strategies adopted by Target Corporation and evaluating its financial performance during the period (2022–2024), in addition to analyzing the financial impacts of the cyberattacks it experienced in 2013. The study also assessed the company's recovery path from those attacks until it achieved financial stability. The study concluded that cybersecurity is an essential technology for protecting the sensitive data of companies and customers, as well as mitigating risks that threaten an organization's security and financial stability.

Keywords : Cybersecurity, financial stability, cyber threats, cyberattacks.

.

فهرس المحتويات

قائمة الجداول والأشكال

الاختصار/الرمز	شرح الرمز باللغة الأجنبية	ترجمة الرمز باللغة العربية
tgt	Target corporation	شركة تارجت
IOT	Internet of things	انترنت الأشياء
DOS	Disk operating system	الحرمان من الخدمة
DDOS	Distributed denial of services	رفض أداء الخدمة
SCO	Shanghai cooperation organization	منظمة شنغهاي للتعاون
IT	Information technology	أنظمة الرقابة
EXW	Early warning	الإنذار المبكر
C	Capital adequacy	كفاية رأس المال
A	Asset quality	جودة الأصول
M	Management integrity	سلامة الإدارة
E	profitability	الربحية
L	liquidity	السيولة
S	Market sensitivity	حساسية السوق
IOS	iphone operating system	نظام تشغيل ايفون

مقدمة

تمهيد:

في ظل التحولات المتسارعة والتغيرات الجوهرية التي يشهدها النظام المالي العالمي، بما يشمل التطورات التكنولوجية المتلاحقة والأزمات المتكررة والتهديدات السيبرانية المتنامية التي تستهدف البنية التحتية المالية، برزت الحاجة الماسة إلى تطوير آليات أكثر فاعلية لتعزيز مرونة القطاع المالي. وقد تباينت آراء الخبراء والمحللين حول السبل المثلى لمواجهة هذه التحديات، لا سيما فيما يتعلق بتطوير منهجيات استباقية للكشف المبكر عن المخاطر المحتملة والتخفيف من آثارها قبل تجسدها.

يعرف الأمن السيبراني بأنه الحقل المعرفي الذي يهتم بحماية البنى الرقمية، بما في ذلك الأنظمة الحاسوبية والشبكات وقواعد البيانات، من الهجمات الإلكترونية والاختراقات غير المصرح بها. ويتضمن هذا المجال تطبيق مجموعة متكاملة من التقنيات المتقدمة والممارسات الأمنية والبروتوكولات الوقائية لضمان حماية المعلومات الرقمية والحفاظ على سريتها وسلامتها وتوافرها. كما يشمل الأمن السيبراني استراتيجيات شاملة تعتمد على أدوات متطورة للتصدي للتهديدات الإلكترونية، إلى جانب برامج توعوية تهدف إلى تعزيز الثقافة الأمنية لدى المستخدمين وترسيخ الممارسات الآمنة في التعامل مع الأنظمة الرقمية.

لقد اكتسب موضوع الحفاظ على الاستقرار المالي أولوية متزايدة في الأجندة الاقتصادية العالمية، خاصة في أعقاب الأزمات المالية الدولية. ويتجلى هذا الاهتمام من خلال التقارير الدورية التي تصدرها البنوك المركزية والمؤسسات المالية الدولية كصندوق النقد الدولي والبنك الدولي وبنك التسويات الدولية، والتي تخصص حيزا كبيرا لرصد مؤشرات الاستقرار المالي وتحليلها. وتكمن الإشكالية الرئيسية في تعقيد تحقيق الاستقرار المالي نظرا لغياب معايير محددة واضحة يمكن الاعتماد عليها خلال التقلبات الدورية للاقتصاد الكلي، مما يجعل من عملية ضبطه تحدياً كبيراً يتطلب مقاربات متعددة الأبعاد.

تتجلى العلاقة التكاملية بين الأمن السيبراني والاستقرار المالي في إطار تكامل وظيفي قائم على الاعتماد المتبادل، حيث يشكلان معا منظومة متكاملة لمواجهة التهديدات السيبرانية المتنامية التي تستهدف المؤسسات المالية بمختلف تصنيفاتها، يستند هذا التكامل إلى أسس منهجية مشتركة تتمثل في تحليل البيانات الضخمة وتقييم المخاطر، بهدف صياغة استراتيجيات وقائية واستباقية تعزز مرونة القطاع المالي. يتجسد التقاطع الاستراتيجي بين المجالين في اشتراكهما في الهدف الجوهري المتمثل في حماية البنية التحتية المالية من التهديدات السيبرانية التي قد تتسبب في اضطرابات نظامية أو خسائر اقتصادية كارثية. هذا الترابط البنيوي بين

الأمن الرقمي والاستقرار المالي يعكس التحول الجوهري في طبيعة المخاطر المالية في العصر الرقمي، حيث أصبح الأمن السيبراني مدخلا أساسيا لتحقيق الاستقرار المالي المستدام.

1. إشكالية الدراسة:

على ضوء ما تقدم، تسعى هذه الدراسة إلى إبراز دور الأمن السيبراني في تعزيز الاستقرار المالي ومن هذا المنطلق جاءت إشكالية الدراسة على النحو التالي:

➢ **كيف يمكن للأمن السيبراني أن يساهم بشكل فعال في تعزيز الاستقرار المالي في شركة target؟**

وتندرج تحت هذه الإشكالية الرئيسية مجموعة من التساؤلات الفرعية التالية:

أ. ما طبيعة العلاقة بين مستوى الأمن السيبراني ومؤشرات السلامة المالية، وكيف ينعكس ذلك على ثقة المتعاملين في النظام المالي؟

ب. ما الدور الذي يلعبه الأمن السيبراني في تعزيز فعالية نظم الإنذار المبكر داخل النظام المالي، وما مدى إسهامه في تمكين الجهات الرقابية من الكشف الاستباقي والاستجابة الفعالة للتهديدات المالية المحتملة؟

ج. كيف يسهم الأمن السيبراني في تعزيز كفاءة تطبيق سياسات الحيطة الكلية، وفي تقليص المخاطر التكنولوجية التي تواجه المؤسسات المالية؟

د. إلى أي حد يمكن للأمن السيبراني أن يسهم في تعزيز سرعة ودقة اكتشاف التهديدات التي قد تعرض سلامة البيانات المالية للخطر؟

2. الدراسات السابقة:

إن الدراسات المتخصصة والمعمقة التي تتناول موضوعات وأبحاث حول الأمن السيبراني هي من الموضوعات القليلة جدا إذا قورنت بالكتابات والأبحاث التي تناولت الاستقرار المالي بشكل عام من حيث المفهوم والتعريف...، على الرغم من وجود بعض المحاولات والمقترحات المعالجة لمثل هكذا مواضيع، نذكر أهم هذه الدراسة والأبحاث، فيما يلي:

الدراسات باللغة العربية:

أ. دراسة إسلام فوزي، (2019)، مقال بعنوان" **الأمن السيبراني الأبعاد الاجتماعية والقانونية تحليل سوسيولوجي"**، المجلة الاجتماعية القومية، جامعة دمنهور، كلية الآداب، قسم علم الاجتماع، المجلد 56، العدد الثاني، مصر، عدد الصفحات، يتمحور الهدف الرئيسي لهذه الدراسة حول التحليل السوسيولوجي لأبعاد الأمن السيبراني المصري، ولتحقيق هدف الدراسة تم الاعتماد على منهج التحليل الوصفي وطريقة التحليل

الثانوي "البيانات الجاهزة" لركائز وممارسات الأمن السيبراني خلال العشر سنوات السابقة بدءا من 2009 مع إنشاء أول مركز طوارئ لتلقي الشكاوي**(CERT)** وحتى 2019 مع تنظيم ماستر كارد لأول منتدى حول الأمن السيبراني في القاهرة.

وتوصلت هذه الدراسة إلى جملة من النتائج أبرزها: ارتكز الأمن السيبراني في ضوء الأبعاد الاجتماعية على بنية تحتية تمثلت في استحداث مركز الطوارئ واستمرار الخدمة فيه 24 ساعة، وكذلك إنشاء المجلس الأعلى للأمن السيبراني الذي خضع لوزارة الاتصالات. ومن قبل وجود غرفة صناعة تكنولوجيا المعلومات والاتصالات ومركز معلومات بمجلس الوزراء، وهذا قطعا ينعكس على الأمن القومي. ومن النتائج أيضا أن مصر شاركت في اتفاقيات تعاون كثيرة مع العديد من الدول حول الأمن السيبراني واحتلت مراكز متقدمة ونالت جوائز متعددة ما جعلها تتغلب على أزمات الثقة.

ب. دراسة بوبكر مصطفى، (2014-2015)، بحث بعنوان" **الاستقرار المالي في إطار مقاربة الاحتراز الكلي-حالة النظام المصرفي الجزائري-**، (أطروحة دكتورا)، قسم التسيير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة الجزائر 3، عدد الصفحات، تهدف هذه الدراسة إلى تبيان مدى نجاعة الرقابة الاحترازية السارية المفعول في ضبط الاستقرار المالي وبيان مدى التحكم في الحفاظ على الاستقرار المالي من خلال المنظمات المالية الدولية والتي تعمل أيضا على تجنب عدم الاستقرار المالي مستقبلا من خلال جهودها في الحفاظ على الاستقرار المالي العالمي، وأيضا ضرورة مواصلة الإصلاحات المالية والمصرفية محليا وضرورة تجانسها مع التوجهات العالمية لتجنب أي أزمة مالية مستقبلية محليا والاستفادة من تجارب الإصلاحات الاحترازية الكلية عالميا. ولتحقيق أهداف الدراسة تم اعتماد المنهج التحليلي الوصفي لاستعراض أهم المفاهيم الخاصة بالاستقرار المالي، كما نعتمد استخدام الأسلوب الاحصائي من خلال الاستعانة بمجموعة من الأدوات الإحصائية الملائمة لتحليل مجموعة البيانات والمعلومات وتحديد المؤشرات الخاصة بالاستقرار المالي من أجل الحكم على مدى متانة النظام المصرفي الجزائري ونقاط ضعفه وقوته.

وتوصلت هذه الدراسة إلى مجموعة من النتائج أبرزها: أن الاستقرار المالي يتحدد من خلال الكشف والحد من التقلبات الدورية، أو بمعنى الحد من سلوك البنوك في مسايرة توجهات النمو الاقتصادي لجنب الافراط في الائتمان. ويجب تعزيز الأطر التنظيمية والرقابية السارية المفعول وتحسين نقاط ضعفها الرئيسية ووضع القواعد التي تسمح بمقاومة المخاطر غير المتوقعة التي قد تتسبب في أزمات مالية مستقبلية. هذه المبادئ ضرورية لخفض المخاطر على الأسواق المالية، والأنظمة المالية والمصرفية وخفض تكاليفها.

ج. دراسة زينب عبد الحفيظ أحمد قاسم، (2022)، بحث بعنوان "**أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك**"، المؤتمر الدولي العلمي الأول، جامعة عين شمس، كلية التجارة، قسم المحاسبة والمراجعة، مصر، عدد الصفحات، هدفت الدراسة إلى التعرف على أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين، وتقديم تشخيص لواقع إدارة مخاطر الأمن السيبراني من أجل دعم تطبيق الشمول المالي لتعزيز الاستقرار المالي لهذه البنوك، ولتحقيق هدف الدراسة تم الاعتماد على المنهج الوصفي التحليلي واستخدمت الاستبانة كأداة لجمع المعلومات ووزعت بعد تقييمها وتحكيمها من عدد من المتخصصين على عبنة الدراسة والتي بلغت 90 مفردة.

وتوصلت هذه الدراسة إلى مجموعة من النتائج أبرزها: أنه يوجد أثر لإدارة مخاطر الأمن السيبراني على دعم الاستقرار المالي والشمول المالي في البنوك المدرجة في بورصة فلسطين، كما تقوم البنوك المدرجة في بورصة فلسطين بالتصدي للمخاطر السيبرانية من خلال توفير بيئة مناسبة للأمن السيبراني بهدف دعم الشمول المالي، وتوصلت أيضا أن المخاطر المتعلقة بالاختراقات يمكن أن تزعزع الاستقرار المالي وتحقق خسائر مالية يمكن أن تتكبدها البنوك، ويوجد فريق للاستجابة لحوادث الأمن السيبراني من أجل تطوير منظومة الأمن السيبراني لتعزيز الاستقرار المالي.

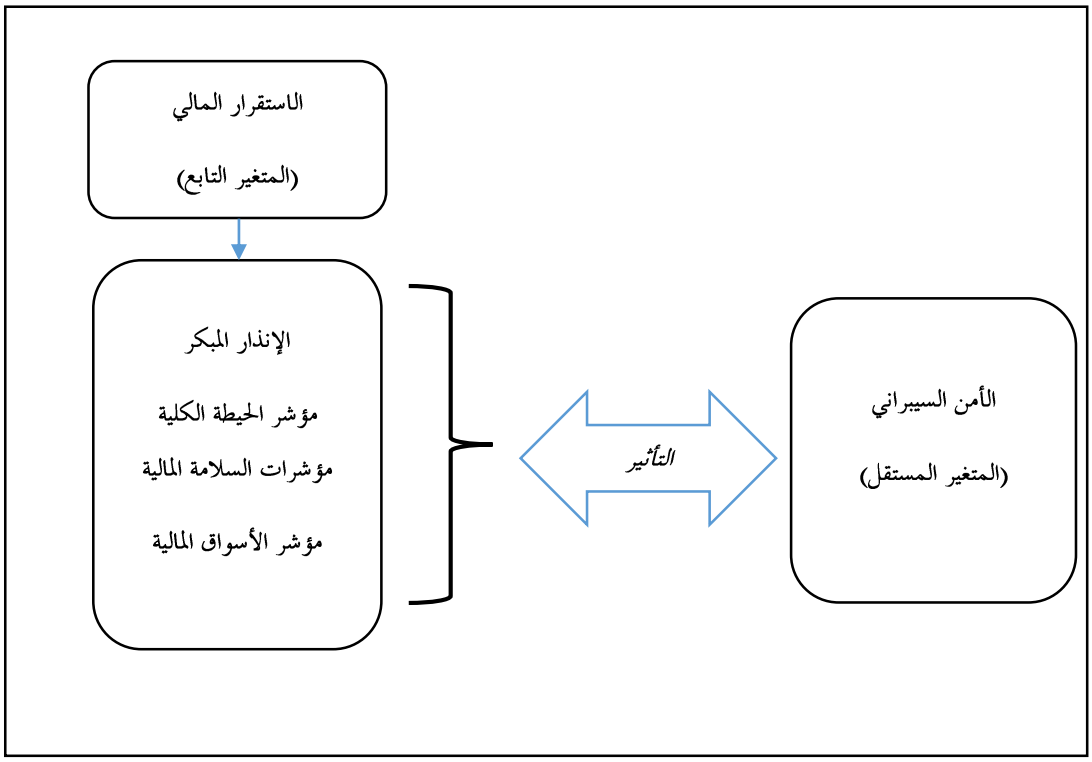
ومن خلال الدراسات السابقة يمكن تقديم الإضافة التي قدمتها الدراسة:

على ضوء الدراسات السابقة والنواقص، جاءت الدراسة الموسومة ب: **مساهمة الأمن السيبراني في تعزيز الاستقرار المالي (دراسة حالة شركة Target)**، حيث أضافت هذه الدراسة بعدا عمليا يربط بين الفشل الأمني والعواقب المالية المباشرة إذا لم تعتمد الشركة على تقنيات حديثة كالأمن السيبراني لحماية بيانات عملائها من خلال إجراءات واحتياطات أمنية تقوم بها، مع تقديم حلول استباقية لتعزيز المرونة المالية عبر الأمن السيبراني. كما تم التركيز بشكل كبير على ضرورة تبني الشركات للأمن السيبراني واعتباره ركيزة أساسية للحفاظ على التوازن المالي.

3. نموذج الدراسة:

اشتملت دراستنا على نوعين من المتغيرات وذلك على النحو التالي: المتغير الأول المستقل يتمثل في الأمن السيبراني، والمتغير الثاني التابع يتمثل في الاستقرار المالي، وقد قمنا بصياغة نموذج من أجل معالجة الإشكالية المطروحة، وذلك من خلال الشكل الآتي:

الشكل رقم (01): نموذج الدراسة



المصدر: من اعداد الطالبتين بالاعتماد على الدراسات السابقة.

من خلال الشكل يلاحظ بأن الدراسة تحتوي على متغيرين رئيسيين هما: المتغير المستقل (الأمن السيبراني) والمتغير التابع (الاستقرار المالي)، يمكن شرح نموذج الدراسة انطلاقا من علاقة الأمن السيبراني بمؤشرات الاستقرار المالي وهي: الإنذار المبكر، مؤشر الحيطة الكلية، مؤشرات السلامة المالية، مؤشر الأسواق المالية. مما ينتج عنه علاقة تأثير بين الأمن السيبراني ومؤشرات الاستقرار المالي.

4. فرضيات الدراسة:

للإجابة على الإشكالية المطروحة ثمت صياغة الفرضية الرئيسية على النحو التالي:

أ. يسهم الامن السيبراني في تعزيز الاستقرار المالي لشركة **Target**، من خلال تقليل المخاطر المرتبطة بالتهديدات السيبرانية.

وتندرج تحت الفرضية الرئيسية الفرضيات الفرعية التالية:

– يرتبط تحسين مستوى الأمن السيبراني بارتفاع مؤشرات السلامة المالية، من خلال تقليص مخاطر الاختراقات وتعزيز ثقة المتعاملين في استقرار النظام المالي.

-يقوم الأمن السيبراني بدور محوري في تعزيز كفاءة نظم الإنذار المبكر داخل النظام المالي، مما يمكن الجهات الرقابية من الكشف الاستباقي والاستجابة الفعالة للتهديدات المالية المحتملة.

-يساعد الأمن السيبراني في رفع كفاءة تطبيق سياسات الحيطة الكلية، من خلال تقليص المخاطر التكنولوجية التي تواجه المؤسسات المالية.

-يساهم الأمن السيبراني بشكل فعال في تحسين سرعة ودقة اكتشاف التهديدات التي قد تؤثر على سلامة البيانات المالية.

5. التموضع الإيستومولوجي:

إن البحث العلمي وعلى وجه الخصوص البحث في ميدان التجارة يتطلب تحديد منهج علمي يتبع وتحترم خصائصه وأبعاده المحددة مسبقا والمتفق عليها علميا، حيث أن التقيد بمنهج وإطار ايستومولوجي معين والذي يمكن أن يبدو أنه تقييد لحرية الباحث وأفكاره إلا أنه يعكس ذلك تماما، وكون الايستومولوجيا هي فرع من فروع الفلسفة فمن المؤكد أنها تتفق مع تعارض الأفكار وتسمح بحرية بناء المعرفة غير أنها تتطلب تحديد الوسيلة والمنطق المعتمد عليه في ذلك، فاختيار منهج معين إذا يعطي الباحث نوع من الوضوح في اختيار طرق البحث، بناء فروضه، والخروج بنتائج مبررة تحظى بدرجة من الثقة والقبول، لطالما سمحت ايستومولوجيا التجارة بالتموقع الوضعي، التفسيري أو البنائي بانتهاج النهج الموضوعي بعيدا عن التحيز الذاتي والخروج بنتائج واقعية من منطق استنتاجي أو اختيار الذاتية والاستعانة بالإدراك الشخصي وإطلاق أحكام نسبية، بانتماء التجارة إلى العلوم الاقتصادية يجد الباحث نفسه في مفترق الطرق بين هذه النماذج نظرا لطبيعة المجتمعات المستهدفة في الدراسة، حيث يأبى الباحث تصديق النتائج الكمية البحتة دون اللجوء للاستقراء والواقعية في البحث، ويبحث في إمكانية وجود درجة حرية تسمح بالجمع بين أكثر من نموذج، ويختلف في ذلك الباحثين فهماك من يعتبر أن التقيد بنموذج واحد ضرورة حتمية وهناك من يرشح التكييف بين الموضوعية والذاتية ويرى وجود إمكانية في التوفيق بينها عن طريق ما يعرف بالذاتية(العقلانية)، والتي تقبل نموذج في وجود الثاني ويعتبر ذلك النموذج المتطور للنموذج الوضعي والذي يطلق عليه النموذج(بعد الوضعي).

6. منهجية الدراسة:

يضم البحث قسمين رئيسين، قسم نظري يهتم بالجانب الأكاديمي والفكري للدراسة، وقسم آخر يعمل على محاولة إسقاط الجانب النظري والفكري على الواقع باعتماد دراسة تطبيقية لشركة تارجت التجارية للبيع بالتجزئة.

ووفقا لطبيعة الموضوع تم الاعتماد في الجانب النظري على استخدام المنهج الوصفي التحليلي، الذي يقوم على جمع المعلومات الكافية والدقيقة ذات الصلة من المصادر العلمية الموثوقة.

أما في الجانب التطبيقي فقد تم توظيف منهج دراسة الحالة الذي يقوم على التحليل العميق لحالة واحدة أو عدة حالات واقعية لفهم ظاهرة معقدة، ومن خلال هذه المنهجية الملتزمة بأدوات البحث العلمي والموضوعية المحايدة كان لزاما على الباحث، اعتماد دراسة حالة قائمة على جمع المعلومات من التقارير والمقالات والموقع الخاص بالشركة.

وعلى هذا الأساس أتت هذه الدراسة الموسومة ب: **مساهمة الأمن السيبراني في تعزيز الاستقرار المالي (دراسة حالة شركة تارجت الأمريكية).**

7.حدود الدراسة:

للإجابة على الإشكالية والتوصل إلى نتائج دقيقة، حصرت الدراسة ضمن حدود المفاهيم المعتمدة والإطار الزمني والمكاني وذلك على النحو التالي:

أ. الحدود الزمانية: تمتد الحدود الزمنية للدراسة في الفترة (2012-2023)

ب. الحدود المكانية: يعتمد موضوع الدراسة في دراسته التطبيقية على دراسة حالة لشركة **Target** الأمريكية.

8. أهمية الدراسة:

تظهر أهمية الدراسة من أهمية الموضوع المدروس بذاته، فدراسة مساهمة الامن السيبراني في تعزيز الاستقرار المالي تعد من المواضيع الحديثة والتي لها أهمية كبيرة في عالم الأعمال اليوم، خاصة مع تزايد التطورات التكنولوجية أصبح من الضروري جدا اعتماد تقنيات حديثة وذكية كالأمن السيبراني لحماية نظام البنية التحتية للمؤسسات المالية من الاختراقات وقرصنة البيانات، أصبحت الشركات تعتمد بشكل كبير على المواقع الالكترونية للترويج لمنتجاتها وخدماتها وهذا ما جعلها أكثر عرضة لسرقة بيانات عملائها.

9.أهداف الدراسة:

يسعى هذا البحث إلى تحقيق مجموعة من الأهداف أهمها:

أ. التمكن من المضامين النظرية للأمن السيبراني وتحليل أبعاده المفاهيمية، بوصفه مدخلا تحليليا ضروريا لفهم سبل توظيفه الفعال في ضمان الاستقرار المالي والمحافظة عليه.

ب. دراسة التهديدات السيبرانية المحتملة التي تواجه المؤسسات المالية وتأثيراتها النظامية على الاستقرار المالي.

ج. التعرف على دور الأمن السيبراني في تحديد المخاطر التي قد تتعرض لها الشركة.

د. قياس التداعيات المالية والاقتصادية للانتهاكات الأمنية السيبرانية على متانة المؤسسات المالية.

ه. تقييم الآثار المالية المباشرة وغير المباشرة الناجمة عن الهجمات الإلكترونية على المؤسسات المالية.

و. استخلاص استنتاجات بحثية وتوصيات عملية قابلة للتطبيق تسهم في إثراء المعرفة الأكاديمية والتطبيقية في هذا المجال.

10. صعوبات الدراسة:

هناك العديد من الصعوبات التي واجهتنا في اعداد البحث نوضحها كالتالي:

أ. تواجه الدراسة تحديات منهجية في تجميع البيانات بسبب تباين المصادر وتضارب المعلومات بين المراجع المختلفة.

ب. قلة المصادر العلمية التي تناولت المتغير المستقل تمثل إحدى محدوديات الدراسة.

ج. صعوبة تحديد العلاقة بين المتغيرين بسبب تعقيد العوامل التي تؤثر على الاستقرار المالي.

د. صعوبة ربط المتغيرين ويعود ذلك لقلة المصادر.

11. هيكل الدراسة:

تم تقسيم هذه الدراسة إلى ثلاث فصول، بالإضافة إلى كل من المقدمة والخاتمة.

أ. الفصل الأول: ويحمل عنوان: **الإطار النظري للأمن السيبراني،** وقسم إلى ثلاث مباحث حيث تناول المبحث الأول يقدم مدخلا مفاهيميا يعرف بالأمن السيبراني، والمبحث الثاني تطرق إلى التهديدات السيبرانية، المبحث الثالث يستعرض الهجمات السيبرانية بأنماطها المختلفة، مع التركيز على آليات الوقاية منها واستراتيجيات التصدي لها.

ب. الفصل الثاني: ومعنون ب: **الإطار المفاهيمي حول الاستقرار المالي،** وقسم إلى ثلاث مباحث حيث خصص المبحث الأول لتقديم تمهيدا نظريا لمفهوم الاستقرار المالي، أما المبحث الثاني فتطرق إلى ماهية الاستقرار المالي، وفي المبحث الثالث يدرس تأثير التهديدات السيبرانية على الاستقرار المالي.

ج. الفصل الثالث: ومعنون ب: **الإطار التطبيقي للدراسة،** وقسم أيضا إلى ثلاث مباحث فالمبحث الأول تناول تقديم شركة **Target corporation**، وفي المبحث الثاني تم عرض ومناقشة الهجمات السيبرانية التي تعرضت لها الشركة، وفي المبحث الثالث تطرقنا إلى التحليل الاستراتيجي وإجراءات التعافي.

كما تم في النهاية إعداد خاتمة للدراسة التي تضمنت نتائج الفرضيات ونتائج الدراسة، متبوعة في الأخير بمجموعة من التوصيات مع صياغة آفاق الدراسة.

الفصل الأول:

الإطار النظري للأمن السيبراني

تمهيد الفصل:

يعد الأمن السيبراني ركيزة أساسية، حيث يحمي الأنظمة والشبكات والبرامج من الهجمات الإلكترونية التي تستهدف سرقة البيانات أو تعطيل الخدمات. يشمل ذلك استخدام تقنيات مثل التشفير وجدران الحماية، بالإضافة إلى تعزيز الوعي الأمني. تؤدي التشريعات الحكومية أيضا دورا مهما في مواجهة الجرائم الإلكترونية. مع تزايد التهديدات، أصبح تطوير استراتيجيات أمنية متكاملة ضروريا لضمان أمان البيانات واستمرارية الأعمال. في ظل العصر الرقمي الذي نعيشه، برزت قضية الأمن السيبراني كواحدة من أهم التحديات التي تواجه استقرار الدول والمنظمات والشركات. ومع تزايد الاعتماد على التكنولوجيا والإنترنت، ازدادت أيضا المخاطر والتهديدات السيبرانية، التي تهدف إلى سرقة البيانات والوصول غير المصرح به إلى الأنظمة والشبكات، مما يتطلب تعزيز الجهود لمواجهة هذه التهديدات وحماية الفضاء السيبراني.

المبحث الأول: مدخل للتعريف بالأمن السيبراني

تطور مفهوم الأمن التقليدي ليتجاوز الحدود المألوفة ويشمل حماية البيانات المتداولة على الإنترنت مع التسارع في التحول الرقمي، أصبح أمن المعلومات غير كاف مما أدى إلى ظهور مفهوم أوسع وهو الأمن السيبراني.

المطلب الأول: تعريف الأمن السيبراني، أهميته وأهدافه

أصبح الأمن السيبراني ضرورة حيوية لحماية المعلومات والأنظمة من التهديدات الإلكترونية المتزايدة التي تستهدف الأفراد والمؤسسات والدول. وهو مجموعة من الاستراتيجيات الهادفة إلى حماية الشبكات من الهجمات التي تهدف إلى تعطيل الخدمات.

الفرع الأول: تعريف الامن السيبراني

يعتبر الامن السيبراني ضروري للغاية من أجل ضمان استمرارية الأعمال وحماية الخصوصية والحفاظ على الاستقرار الاجتماعي والاقتصادي:

1. عرفته وزارة الدفاع الأمريكية على أنه: جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بشتى أشكالها (الإلكترونية والمادية) من مختلف الجرائم، الهجمات، التخريب، التجسس والحوادث، في حين اعتبره الإعلام الأوروبي بأنه قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث الغير متوقعة والتي تستهدف البيانات. (الحديدي، 2023، صفحة 72)

2. كما يعرف الأمن السيبراني أنه "عبارة عن مجموعة من الوسائل التقنية والإدارية التي يقوم بها لمنع الاستخدام الغير مشروع، وسوء الاستغلال للمعلومات التكنولوجية ونظم الاتصالات والمعلومات التي تحتويها. بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية." (محمد ا.، 2024، صفحة 17)

3. كما عرف بأنه هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التشغيلية ومكوناتها من عتاد وبرمجيات وما تقدمه من خدمات وما تحتويه من بينات من أي اختراق أو تعطيل أو دخول أو استخدام غير مشروع. (المطيري، 2023/2022، صفحة 994)

4. ويعرف **Richard A. Kemmerer** الأمن السيبراني بأنه" وسيلة لتقليل مخاطر الهجمات على البرامج أو أجهزة الكمبيوتر أو عناصر التحكم، بما في ذلك الوسائل والأدوات المستخدمة". (دحماني، 2023، صفحة 686)

- بناء على ما سبق ذكره، من تعريفات للأمن السيبراني يمكن استنتاج التعريف التالي:

الأمن السيبراني هو مجموعة من الإجراءات الوقائية التي تهدف لمنع الاستخدام غير المصرح به للبيانات، وحماية البنية التحتية الرقمية من الهجمات والتهديدات السيبرانية المتنوعة، مع ضمان الحفاظ على سرية المعلومات، وسلامتها، وخصوصيتها.

وتجدر الإشارة إلى وجود مصطلحات ذات صلة بالأمن السيبراني وتتمثل أبرزها فيما يلي:

1. الفضاء السيبراني:

المحيط الذي تجري فيه العمليات السيبرانية الناشئة عن أداء أنظمة الكترونية مهمتها متابعة وجمع المعلومات التي تعمل الكترونيا، وتحليلها من ثم اتخاذ إجراءات محددة لمهاجمتها عن طريق أنظمة الكترونية أخرى مخصصة لهذا الغرض. تعرفه الوكالة الفرنسية لأمن أنظمة الاعلام على أنه فضاء التواصل مشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية. (خولة، 2023، صفحة 3)

2. الجريمة السيبرانية:

"مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الانترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلمات لارتكابها أو التحقيق فيها ومقاضاة فاعليها". (الحليم، 2022، صفحة 48)

3. القوة السيبرانية:

هي القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى، وذلك عبر أدوات سيبرانية. (خولة، 2023، صفحة 4)

4. الردع السيبراني:

يعرف على أنه: " منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية". (الحليم، 2022، صفحة 48)

5. الإرهاب السيبراني:

عرفه جايمس لويس على أنه:" استخدام شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة مثل: الطاقة والنقل، أو بهدف ترهيب الحكومة والمدنيين". (لاميا، 2021، صفحة 361)

الفرع الثاني: أهمية الأمن السيبراني:

تظهر أهمية الأمن السيبراني بشكل واضح في حماية المعلومات ومصادرها بالإضافة إلى الأنظمة المتعلقة بتخزينها، ويمكن ملاحظة هذه الأهمية من خلال ما يلي: (نسيمة، 2022، صفحة 9 10)

1. السلامة أي سلامة البيانات والمعلومات وحمايتها من أي هجوم أو اختراق أو قرصنة.

2. السرية وتكون كل المعطيات والبيانات والمعلومات في مأمن وغير مرخص أ مسموح لأي كان من الولوج إليها.

3. الجاهزية فطالما آمنة ومحمية فهي متاحة وجاهزة للاستعمال حسب الطلب والإتاحة.

وكذلك لدينا: (السيد، 2022، صفحة 398)

4. التقليل من مخاطر التهديدات الأمنية والاختراقات المحتملة للبيانات الى جانب الحفاظ على سرية المعلومات.

5. يتمتع بقدرته على مواجهة التهديدات سواء كانت متعمدة أو غير متعمدة، بالإضافة إلى قدرته على الاستجابة السريعة والتعافي من آثارها.

6. ضمان الوصول المنطقي إلى الأصول المعلوماتية، وذلك من خلال منع الوصول غير المصرح به وتقييده.

7. يمتلك الأمن السيبراني القدرة على حماية الشبكات وإدارتها بشكل فعال.

الفرع الثالث: أهداف الامن السيبراني

يهدف الأمن السيبراني إلى حماية الأنظمة والشبكات والبيانات من الهجمات الإلكترونية التي قد تلحق أضرارا كبيرة بالأفراد والمؤسسات والدول: (منى عبد الله السمحان، 2023، صفحة 12)

1. تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحويه من بيانات.

2. التصدي لهجمات وحوادث امن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.

3. توفير بيئة امنة وموثوقة للتعاملات في مجتمع المعلومات.

4. توفير المتطلبات اللازمة للحد من المخاطر والجرائم الالكترونية التي تستهدف المستخدمين.

5. الحد من التجسس والتخريب الالكتروني على مستوى الحكومة والافراد.

6. سد الثغرات في أنظمة امن المعلومات.

7. يهدف الأمن السيبراني إلى حماية خمس أنواع من المعدات والأنظمة الأساسية، هي أمن البنية التحتية وأمن الشبكات وأمن السحابة وأمن إنترنت الأشياء وأمن التطبيقات. (كاظم، 2025، صفحة 01)

المطلب الثاني: أبعاد الأمن السيبراني وخصائصه

يتسم الأمن السيبراني بمجموعة من الخصائص التي تميزه عن غيره من المجالات، كما يتميز بتعدد أبعاده وتعقيدها حيث يركز على أربعة أبعاد رئيسية ونذكر منها:

الفرع الأول: أبعاد الأمن السيبراني

هناك أبعاد متنوعة ومتعددة تتعاون معا لتوفير حماية متكاملة للأنظمة الرقمية والبيانات يمكن ابرازها كالتالي:

1. البعد الاقتصادي:

يرتبط الأمن السيبراني إرتباطا وثيقا بالحفاظ على على المصالح الاقتصادية لكل دولة ، فالترابط وثيق بين الإقتصاد و المعرفة فأغلب الدول تعتمد في تعزيز اقتصادها و ازدهاره على إنتاج و تداول المعرفة و المعلومات على المستويات، مما يبرر الدور الخطير للأمن السيبراني في حماية الاقتصاد من السرقة و الملكية الفكرية. (اللقاني، 2023، صفحة 153)

2. الابعاد الاجتماعية:

تساهم شبكات التواصل الاجتماعي بشكل خاص في فتح المجال للأفراد للتعبير عن تطلعاتهم السياسية و طموحاتهم الاجتماعية بأشكالها المختلفة، كذلك تشكل مشاركة جميع شرائح المجتمع و مكوناته و سيلة لتطوير المجتمع مما يتيح الفرصة للاطلاع على الأفكار و المعلومات و بما تكونه من حاجة لدى المجتمع في الحفاظ على استقرار الفضاء الالكتروني و المجتمع الذي يرتكز اليه ، كما ان انفتاح مجتمع ما على المجتمعات الأخرى يؤسس لتبادل خبرات و أفكارو تكوين أفاق للتعاون و التكامل . (عطية، 2019، صفحة 105 106)

3. البعد السياسي:

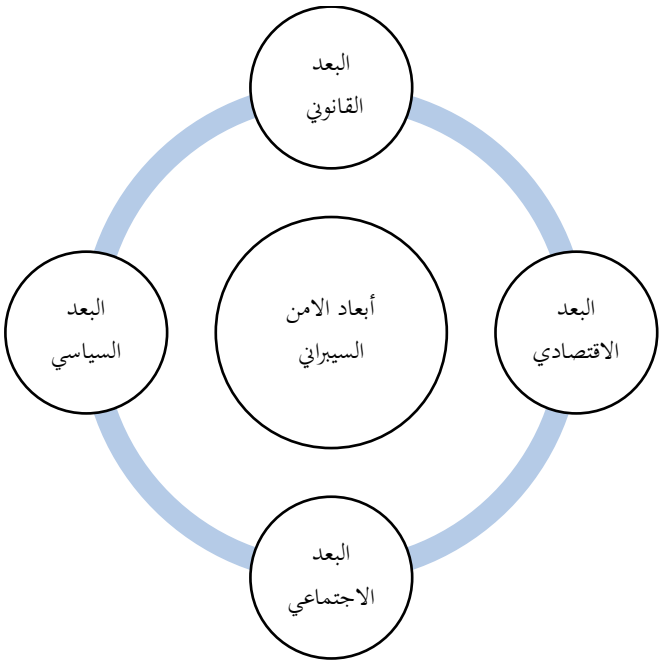
يقوم هذا الأخير على أساس حماية نظام الدولة السياسية و كيانها ، حيث يمكن أتستخدم التقنيات في بث معلومات وبيانات قد يحدث من خلالها زعزعة في لإستقرار أمن الدول و الحكومات حيث تصل بسرعة فائقة إلى أكبر عدد من المواطنين بغض النظر عن صحة البيانات و المعلومات التي تم نشرها. (اللقاني، 2023، صفحة 153)

4.البعد القانوني:

تعد العلاقة بين القانون و التكنولوجيا علاقة تبادلية فالتطورات التكنولوجية المختلفة تفرض مواكبة التشريعات القانونية لها، من خلال وضع اطر و تشريعات للاعمال القانونية و غير القانونية منها ولكن بصورة عامة تفتقر الجرائمة السيبرانية في الوقت الحالي للاطر القانونية الصارمة للتعامل معها ، ولعل ذلك يعود لعوامل مثل طبيعة الجريمة المرتبطة بتكنولوجيا المعلومات ، الى جانب ذلك فان الجرائم السيبرانية غير مقيدة بحدود الدول، الامر الذي يقتضي تفعيل التعاون الدولي المشترك لمكافتها. (عطية، 2019، صفحة 106)

و يتم تلخيص الأبعاد السالفة الذكر في الشكل التالي:

الشكل رقم(02): أبعاد الأمن السيبراني.



المصدر: من اعداد الطالبتين بالاعتماد على ما سبق.

الفرع الثاني: خصائص الامن السيبراني

الأمن السيبراني يتميز بمجموعة من الخصائص التي تميزه عن المجالات الأخرى، ومن أبرز هذه الخصائص لدينا:

1.الثقة وعدم الثقة:

تعمل جدران الحماية الخاص بنظام الأمن السيبراني كمرشح إلكتروني يتحكم في نوع وطبيعة البرامج والتقنيات المسموح بتفعيلها، بحيث يسمح بمرور البرامج الموثوقة والتي تم التحقق من أمانها سواء من قبل المستخدم أو من خلال المتجر الإلكتروني وتم حظر البرامج الخبيثة ومنعها من التطفل واستغلال الثغرات مما يعزز الحماية ويقلل من مخاطر الانتهاكات الإلكترونية. (شاهين، 2024، صفحة 88)

2. السرعة وغياب الدليل:

تتمثل صعوبات إثبات الجرائم الالكترونية في استخدام المخترقين وسائل تقنية حديثة ومتطورة باستمرار، لذلك كان من اللازم أن يأتي الأمن السيبراني بتقنيات حديثة عالية تفوق تقنياتهم وخبراتهم. (المنيع، 2022، صفحة 164)

3. الحماية من التهديدات الخارجية:

تعد الحماية من التهديدات الخارجية أحد أهم الركائز الأساسية للأمن السيبراني، حيث يتم فيها بناء جدار الحماية تعمل كخط دفاع أول قادر على تصفية المخاطر الخارجية التي يسفر عنها التعامل مع العالم الرقمي، حيث يشمل

ذلك حماية النظام من الرسائل الإلكترونية الضارة والروابط الخبيثة أو الفيروسات إضافة إلى معالجة نقاط الضعف في النظام أو الثغرات الأمنية التي قد تستغل من قبل جهات خارجية في السيطرة على النظام والتحكم فيه. (شاهين، 2024، صفحة 89)

4. ضعف الأجهزة الأمنية والقضائية في التعامل مع الجرائم السيبرانية:

وذلك بسبب نقص الخبرة الرقمية لدى الأجهزة الأمنية، مما يعزز دور الأمن السيبراني في تحقيق الأمن الرقمي للمؤسسات من أجل حماية البيانات والبنى التحتية لهذه المؤسسات. (المنيع، 2022، صفحة 164)

المطلب الثالث: أنظمة واستراتيجيات الامن السيبراني

تشكل استراتيجيات الأمن السيبراني الإطار العام الذي يحدد ملامح التخطيط وآليات التنفيذ الرامية إلى حماية البنية الرقمية من المخاطر والاختراقات الأمنية. كما تعتبر أنظمة الأمن السيبراني هي منظومة متكاملة من السياسات والتقنيات والإجراءات تهدف إلى حماية المعلومات والبنى التحتية الرقمية من التهديدات والهجمات السيبرانية، مع ضمان سرية البيانات وسلامتها وتوافرها.

الفرع الثاني: أنواع أنظمة الأمن السيبراني

تشمل مجموعة متنوعة من التقنيات التي تُصمم خصيصًا لحماية الأنظمة من الهجمات الإلكترونية. تختلف هذه الأنظمة لتلبية احتياجات أمنية متعددة. (القحطاني، 2022، صفحة 125)

1. نظام أمن التطبيقات والبرمجيات:

وهو خاص بمنع سرقة البيانات أو التعليمات البرمجية داخل التطبيق أو الاستيلاء عليها.

2. نظام أمن السحابة:

يوفر التأمين لبيئات الحوسبة السحابية ضد التهديدات الداخلية والخارجية، ويمنع من الوصول غير المصرح به، ويحافظ على البيانات والتطبيقات آمنة في السحابة.

3. نظام أمن شبكات البنية التحتية في المنظمات والشركات والمؤسسات المختلفة.

4. نظام أمن انترنت الأشياء (IOT):

لحماية شبكات الأشياء والأشخاص المتصلين بأجهزة الانترنت وشبكات الاتصال، ويشمل أجهزة الاستشعار وأجهزة التلفزيون والطابعات، وعددا لا يحصى من أجهزة الشبكات المنزلية المختلفة.

الفرع الثالث: استراتيجيات الأمن السيبراني

هناك العديد من الاستراتيجيات التي يمكن إتباعها لتعزيز الأمن السيبراني وحماية الأنظمة الإلكترونية والبيانات، ومن بينها: (المعايطة، 2024، صفحة 367 368)

1. **تطوير سياسات الأمن السيبراني**: إنشاء وتطبيق سياسات الأمن القوية والمحدثة لضمان الامتثال بالمعايير الأمنية المحددة، بما في ذلك سياسات إدارة الهوية وسياسة استخدام البيانات والتحقق من الهوية.

2. **تحسين التحقق من الهوية**: تعزيز عمليات التحقق من الهوية مثل استخدام كلمات مرور قوية والمصادقة المتعددة العوامل والتحقق البيو متري.

3. **تحقيق التدريب والتنوع**: توفير التدريب المستمر للموظفين حول مخاطر الأمن السيبراني وكيفية التصرف في حالة التعرض لها، بالإضافة وكيفية التصرف في حالة التعرض لها، بالإضافة إلى تعزيز التنوع بين المستخدمين النهائيين حول ممارسة الأمن الجيد.

4. **تحديث وصيانة البرمجيات والأجهزة**: تطبيق تحديثات الأمان وإجراءات الصيانة الدورية للبرمجيات والأجهزة لسد الثغرات الأمنية المعروفة وتحسين الحماية.

5. **تطبيق أمن الشبكات**: استخدام جدران الحماية وأنظمة اكتشاف التسلل وأجهزة الأمان الشبكي لرصد ومنع الهجمات السيبرانية.

6. **تطوير خطط استجابة الطوارئ**: إنشاء خطط استجابة الطوارئ للتصدي للاختراقات والهجمات السيبرانية بشكل فعال وتقديم الاستجابة السريعة والفعالة:

ولدينا أيضا: (القحطاني، 2022، صفحة 140 141)

7. وضع استراتيجية وطنية لحماية نظام المعلومات والاتصالات.

8. تحديد ميزانية مالية لتحقيق مستوى عالي من تجهيزات البنية التحتية الخاصة بنظام الأمن السيبراني.

9. تفعيل الاتفاقيات والمعاهدات الدولية لتنسيق الجهود المشتركة حول تحديد أنظمة الأمن السيبراني على المستوى الوطني والإقليمي والدولي.

المبحث الثاني: التهديدات السيبرانية

تعد التهديدات السيبرانية مخاطر متنامية تهدد أمن الأنظمة الرقمية، حيث تشمل هجمات إلكترونية متنوعة تهدف إلى استغلال الثغرات الأمنية لسرقة البيانات أو تعطيل الخدمات. وتستلزم هذه التهديدات تبني استراتيجيات أمنية متكاملة لمواجهتها، بما في ذلك التحليل الدقيق للمخاطر وتطوير آليات الحماية الوقائية والعلاجية.

المطلب الأول: تعريف وأنواع التهديدات السيبرانية

أصبحت حماية الأنظمة الرقمية من التهديدات السيبرانية أمر في غاية الأهمية. فالهجمات السيبرانية لا تقتصر آثارها على الخسائر المالية الكبيرة فحسب، بل تمتد لتشكل تهديدًا لسمعة المؤسسات وتؤدي إلى فقدان ثقة العملاء، بالإضافة إلى ما قد تخلفه من تداعيات أمنية واجتماعية خطيرة.

الفرع الأول: تعريف التهديدات السيبرانية

تأتي التهديدات بأشكال متعددة ويمكن أن تكون منظمة أو عشوائية. فيما يلي سنعرض بعض من التعريفات الخاصة بالتهديدات السيبرانية: (شرقي، 2023، صفحة 275)

1. يقصد بها تلك الهجمات التي تتم باستخدام آليات وشبكات الأنترنت وشبكات الحاسوب الآلي، وتهدف إلى إلحاق الضرر بالأجهزة والشبكات الإلكترونية ذات الاتصال بالأنترنت.

2. كما تعرف التهديدات السيبرانية بأنها: فعل يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف ما تمكن المهاجم من التلاعب بالنظام.

وهناك تعريفات أخرى نوضحها كالتالي: (رحيم، /20242023، صفحة 8 9)

3. هو برنامج ضار آت من الفضاء السيبراني يهدف إلى المساس بأمن الميكروكمبيوتورات والهواتف الذكية والأجهزة اللوحية والشبكات وغيرها من الأشياء المتصلة بالأنترنت. يمكن أن يكون مرتكب التهديد السيبراني شخصا أو دولة أو مجموعة قراصنة أو منظمة ذات أهداف جيوسياسية. (بوقرص، 2022، صفحة 65)

4. تعرف أيضا بأنها الهجمات الالكترونية التي يتم شنها من جهاز حاسوب على جهاز حاسوب آخر أو عدة أجهزة، وقد يكون الهدف منها الوصول إلى بيانات معينة أو اختراق شبكات أو تدمير مواقع، أو تدمير البنى التحتية مما يشكل تهديد حقيقي وفعلي على الأمن الدولي والأمن القومي.

- ومن التعريفات السابقة الذكر نستنتج أن التهديدات السيبرانية:

تشير إلى أي خطر يهدد أنظمة الحاسوب أو الشبكات أو البيانات الالكترونية بهدف سرقتها، اختراقها، أو اتلافها، يمكن أن تصدر هذه التهديدات عن أفراد، مجموعات أو حتى دول تسعى لتحقيق أهداف محددة مثل الوصول إلى معلومات سرية أو تعطيل الخدمات أو إلحاق الضرر بالبنية التحتية الرقمية.

الفرع الثاني: أنواع التهديدات السيبرانية

تعرف التهديدات السيبرانية بأنها مجموعة من الأنشطة الضارة التي تستهدف الأنظمة والشبكات الرقمية، بهدف إلحاق الضرر بالبنية التحتية الرقمية. يتم ذلك إما عن طريق تعطيل العمليات الرقمية أو إتلاف البيانات، أو التلاعب بالمعلومات الحساسة، ومن أبرز هذه التهديدات ما يلي:

1. هجوم الحرمان من الخدمة (DOS):

هو هجوم يهدف إلى تعطيل قدرة الهدف على تقديم الخدمات المعتادة، ويتم استخدام هذه الطريقة ضد مواقع الأنترنت أو البنوك أو المؤسسات بمختلف أصنافها للتأثير عليها. (شرقي، 2023، صفحة 278)

2. هجمات رفض أداء الخدمة(DDOS):

تستخدم لزيادة التحميل على الانترنت مما يؤدي للضغط على الشبكات ويمنع المستخدمين من الوصول للمنتجات والخدمات. (بونيف، 2019، صفحة 125)

3. إتلاف المعلومات أو تعديلها:

ويقصد به الوصول إلى معلومات الضحية عبر شبكة الأنترنت أو الشبكة الخاصة، والقيام بعملية تعديل البيانات الهامة دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة قد تؤدي إلى نتائج كارثية خاصة إذا كانت خطط عسكرية أو مواعيد أو خرائط سرية. (شرقي، 2023، صفحة 278)

4. تدمير المعلومات:

من خلال تدمير كامل لأصول المعلومات والبيانات ويسمى هذا الفعل بتهديد سلامة المحتوى. (زروقة، 2019، صفحة 23 10)

5 . برامج الفدية:

وتستهدف تغيير الملفات المستخدمة وتغيير بيانات الوصول إليها والمتمثلة في التشفير والقيام بطلب فدية ويسمى هجوم بيتا كريبتو. (المطاع، 2025، صفحة 77)

وأيضا تعمل على تشفير البيانات على النظام المستهدف ويطلب من خلاله الفدية مقابل السماح للمستخدم بالوصول إلى البيانات مرة أخرى، وتتراوح حدة هذه الهجمات من الازعاج المنخفض المستوى إلى الحوادث الخطيرة،

حيث أصبح هذا النوع من الهجمات أكثر انتشارا ويمثل تهديد كبير للشركات والأفراد نظرا لطابع الابتزاز. (توفيق، 2024، صفحة 706)

6. هجمات التصيد الاحتيالي:

هو نوع من الهجمات السيبرانية، حيث يشكل المهاجم كيانا أو شركة مرموقة من أجل خداع الأشخاص وجمع معلوماتهم الحساسة كبيانات بطاقة الائتمان، وأسماء المستخدمين، وكلمات المرور وما إلى ذلك. تستخدم هجمات التصيد رسائل الكترونية مزيفة تقنع المستخدم بإدخال معلومات حساسة في موقع ويب مزيف. وعادة ما تطلب هذه الرسائل من المستخدم إعادة تعيين كلمة المرور الخاصة به أو تأكيد بيانات بطاقات الائتمان ثم تأخذه إلى موقع ويب مزيف يشبه جدا الموقع الأصلي. (زواوي، 2023، صفحة 151)

7. سرقة كلمات المرور والتسلسل للنظام:

وتتمثل في التخمين والخداع والبرمجيات الخبيثة والنفاذ لملف تخزين كلمات مرور. (بونيف، 2019، صفحة 124)

8. التجسس المعلوماتي:

وذلك عن طريق التجسس والتنصت على أجهزة الحواسيب واعتراض المراسلات الالكترونية، وغالبا ما يتم ذلك عبر تثبيت برامج التجسس المعرفة على أنها برامج مصممة لجمع البيانات من حاسوب أو جهاز آخر وإعادة توجيهها إلى طرف آخر من دون موافقة المستخدم. وتنقسم برامج التجسس بوجه عام إلى أربع فئات أساسية: أحصنة طروادة في المقام الأول، وبرامج الإعلانات المتسللة في المقام الثاني، وملفات تعريف الارتباط للتعقب في المقام الثالث، وفي الأخير برامج مراقبة النظام. (زواوي، 2023، صفحة 151)

المطلب الثاني: مخاطر التهديدات السيبرانية ومجالاتها

تشكل التهديدات السيبرانية خطرا جسيما يهدد أمن البيانات وسلامة البنى التحتية الرقمية ولا يقتصر على الجانب التقني فحسب بل يمتد ليهدد كافة مجالات الحياة العصرية.

الفرع الأول: مخاطر التهديدات السيبرانية

للتهديدات السيبرانية مخاطر كثيرة ومتعددة نذكر منها ما يلي: (منى، 2017) منقولا عن مذكرة الماستر (دحمان، 2017-2018، صفحة 33)

1. التلاعب بالمعلومات الموجود في نظام معين، وتشويهها أو اتلافها، سواء عبر الاختراق او نشر الفيروسات.
2. الجرائم التي تندرج في إطار الجريمة المنظمة، والتي تهدد أمن الافراد والدول، كتبييض الأموال والإرهاب ...الخ.
3. الدخول الى الأنظمة والملفات دون إذن، وهذا يعتبر اعتداء على الحريات والحقوق الشخصية.
4. الجرائم العادية التي تستخدم الانترنيت، كسرقة الهويات، والاعتداء على الملكية الفكرية.

وهناك أيضا مخاطر أخرى تكمن في: (ساعد بوقرص، 2022، صفحة 66)

5. التأثير السلبي على الرأي العام.

6.التجسس والابتزاز.

7.اعتراض البيانات وتخريبها.

الفرع الثاني: المجالات التي تقع عليها التهديدات السيبرانية.

لقد توسع نطاق التهديدات السيبرانية بشكل كبير ليشمل جميع جوانب حياة الأفراد والمجتمعات، مما يهدد أمنهم وسلامتهم على مستويات متعددة. لم تعد هذه الجرائم مقتصرة على نطاق ضيق، بل أصبحت متشعبة وخطيرة، حيث تمتد تأثيراتها من الحياة الشخصية إلى الأمن القومي ونذكر من بين هذه المجالات ما يلي: (محمد, العيداني، 2024، صفحة 22)

1. تهديدات سيبرانية تمس الأموال:

مع تزايد المعاملات المالية عبر الشبكات الإلكترونية، تطورت وسائل الدفاع الإلكتروني، الأمر الذي أدى لتطور الجرائم الإلكترونية مثل اختراق بطاقات الائتمان والتحويلات المالية إلى التطور أيضًا لسرقة الأموال بأقل تكلفة ممكنة.

2. التهديدات السيبرانية تلحق بأمن الدولة:

يعتبر الأمن القومي للدولة خط أحمر لا يُمس، إذ أن المساس به يعني زوال مؤسساتها وكيانها. وتُعد جرائم مثل الإرهاب والجوسسة المضادة من الجرائم السيبرانية المنظمة التي تهدد أمن الدولة واستقرارها.

3. التهديدات السيبرانية تمس بحياة الأفراد الخاصة.

يسن المشرع القوانين لحماية الأفراد من أي اعتداء، ومع ظهور العالم الإلكتروني أصبحت خصوصيات الأشخاص مهددة بسبب إمكانية اختراق بياناتهم واستغلالها في أعمال كالتهديد والمضايقة وانتحال الشخصية.

المطلب الثالث: تحديات الامن السيبراني والحلول اللازمة

هناك تحديات كبيرة حماية الأنظمة والشبكات والبيانات عملية معقدة ومستمرة. هذه التحديات ناتجة عن التطور التكنولوجي السريع، ولكن لكل مشكلة حل فقد خصصت بعض التدابير من أجل مواجهة هذه التحديات.

الفرع الأول: التحديات التي تواجه الأمن السيبراني

يواجه الأمن السيبراني مجموعة من التحديات التي تعد من أكبر المشكلات التي يتعامل معها العالم الرقمي اليوم، حيث غالبا ما تتسبب هذه التحديات في خسائر كبيرة يصعب التعافي منها. يمكن رصد أبرز هذه التحديات كالتالي: (بوقرص، 2022، صفحة 73 74)

1. ظهور تقنيات جديدة وبالتالي نقاط ضعف جديدة وباستمرار وحتى للشركات التي لديها موارد لا بأس بها.

2. توسع وتطور رقعة الهجومات السيبرانية وذلك راجع إلى الارتفاع المذهل لعدد الأشياء المتصلة بالأنترنت **(IOT).**

3. المرونة السيبرانية باعتبارها ميزة الشركات التي تتمتع بالقدرة على الاستعداد والتكيف مع التهديدات المتطورة وكذلك استرداد قدراتها بسرعة من الهجمات السيبرانية. في هذا الإطار يلاحظ عدم إقامة تدريبات حل الأزمات لعدد كبير من الشركات.

ويمكن ابراز تحديات أخرى: (الخبيزي، 2023، صفحة 246)

4. سرعة حدوث الجرائم والهجمات السيبرانية.

5. كون الجرائم والهجمات السيبرانية عابرة للحدود ولا تعترف بالحواجز الجغرافية.

6. مخاطر صعوبة تحديد الكيان المنفذ للهجمات السيبرانية في الكثير من الحالات.

7. ارتفاع الخسائر الناجمة عن الجرائم والهجمات السيبرانية مقارنة بالجرائم التقليدية.

8. عدم وجود اختصاص قضائي خاص بهذه النوعية من الجرائم والهجمات.

9. الاعتماد الكبير على الأجهزة والبرامج المستوردة، إذ تعتمد عديد من الدول على استيراد التقنيات الحديثة والتكنولوجيات الحاسوبية من دول متقدمة بهذا المجال مثل الصين وأمريكا، وتستخدمها في قطاعاتها الحيوية مثل الدفاع والأمن والمؤسسات المالية الاقتصادية والحكومية، وبالتالي فإن هذه التبعية تشكل تهديدا خطيرا للأمن القومي لهذه الدولة.

الفرع الثاني: التدابير اللازمة لتحقيق الأمن السيبراني

تم تصنيفها وتوضيحها في مجموعة من النقاط نبرزها كما يلي: (لخضر، 2023، صفحة 515)

1. استعمال البرمجيات المضادة للاعتداءات الالكترونية والتي تعمل على البحث وتحطيم البرامج الخبيثة.

2. تطوير وسائل الدفع المالي كالبطاقة الائتمانية التي تعتبر من أكثر الوسائل أمانا.

3. حماية البرمجيات وذلك بإعداد كلمات مرور قوية والتحديث المستمر لهذه البرمجيات.

4. التوقيع الالكتروني وهو طريقة للتحقق من أن صاحب المعاملة هو نفس الشخص الذي قام بإرسالها أو تنفيذها، كما يطلق عليه بالبصمة الالكترونية، ويتم تشفير التوقيع الالكتروني باستخدام نظام التشفير عن طريق المفتاح العام المزدوج.

5. التحكم بدخول المستخدمين باستخدام الجدار الناري أو جدار الحماية(**Fire-wall**) وهذا لمقاومة أخطار المتطفلين وتوفير الحماية للمنظمات.

المبحث الثالث: الهجمات السيبرانية وسبل الوقاية منها

أصبحت الهجمات السيبرانية سلاحا خطيرا تستخدمه جهات مختلفة لتحقيق أهداف محددة، حيث تعتمد على اختراق الأنظمة التكنولوجية، مما يهدد أمن وخصوصية البيانات. كما يكمن الفرق بين التهديدات السيبرانية والهجمات هو ان التهديدات السيبرانية هي مخاطر محتملة قد تسبب ضررا أو استغلالا لأنظمة المعلومات، أما الهجمات السيبرانية فهي تنفيذ فعلي لهذه التهديدات، حيث يتم استغلال الثغرات لإلحاق الضرر أو الاختراق.

المطلب الأول: مفهوم الهجمات السيبرانية

تطورت التهديدات الإلكترونية لتفوق النطاق التقليدي للاختراقات، حيث لم تعد تقتصر على مجرد سرقة البيانات، مع تسارع الاعتماد على الفضاء الرقمي، برزت الهجمات السيبرانية كخطر استراتيجي متعدد الأشكال، تتراوح بين البرمجيات الخبيثة والتصيد الإلكتروني وصولاً إلى الحروب السيبرانية.

سنقدم جملة من التعريفات حول الهجمات السيبرانية التي قدمها بعض العلماء الاقتصاديين لتوضيح مفهومها كما يلي:

1.عرفها مايكل شيمت على أنها: " مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة". (العزيز، 2023، صفحة 474)

2. كما عرفت أيضا على بأنها:" تصرف يدور في عالم افتراضي قائم على استخدام بيانات رقمية، ووسائل اتصالات جراء اختراق مواقع الكترونية حساسة". (عارفان، 2024، صفحة 474)

3. استخدام البيانات والأكواد الضارة أو الخبيثة لتغيير بيانات وأكواد الحواسيب، مما يؤدي إلى عواقب وخيمة تتراوح ما بين تعريض سلامة هذه البيانات للخطر أو سرقة المعلومات والبيانات الشخصية والهويات. (رضوان، 2025، صفحة 1755)

– نستنتج أن الهجمات السيبرانية هي: جريمة يعاقب عليها القانون، حيث يقوم بها أفراد أو مجموعات يتمتعون بخبرات تقنية عالية تمكنهم من تنفيذ هذه العمليات بسهولة وسرعة، باستخدام برامج وأدوات متخصصة تهدف إلى سرقة البيانات أو الأموال أو المعلومات الحساسة التابعة لأفراد أو مؤسسات أو حتى دول.

المطلب الثاني: خصائص الهجمات السيبرانية وأسباب انتشارها

تتميز الهجمات السيبرانية بعدد من الخصائص التي تجعلها تهديدا معقدا ومتطورا، كما تتنوع أسبابها التي ترتبط بشكل عام بمدى قدرة الأنظمة الأمنية على حماية البيانات والتكنولوجيات المستخدمة.

الفرع الأول: خصائص الهجمات السيبرانية

تمثل الهجمات السيبرانية أحد أخطر التهديدات التي تواجه المؤسسات والحكومات، حيث تتميز بعدة خصائص من أبرزها: (صيام، 2024، صفحة 46 47)

1. **جرائم يصعب اكتشافها:** بسبب سرعة تدمير الأدلة من طرف منفذ الهجوم السيبراني وبسبب خبرتهم التي تفوق خبرة السلطات في الدول المختلفة، وأيضا طريقة التنفيذ الآلية تكون بدون ترك آثار ويصعب بشكل كبير اكتشافها.
2. **صعوبة الاثبات:** الأدوات المستعملة في هذا النوع من الجرائم معقدة ويصعب اثبات القيام بالهجمات السيبرانية.
3. جرائم مغرية للمجرمين فهي تتسم بسرعة التنفيذ وبسرعة الربح خلال مدة زمنية قد تصل لبضع ثواني.

وأيضا: (عرفان، 2024، صفحة 2991)

4. التغلب على العامل الجغرافي حيث يختفي معها ولا يؤثر على اختبار الجهة المستهدف الهجوم عليها.
5. التحديث والتطوير بوتيرة سريعة وبصفة دائمة مما يترتب عليه زيادة فاعليتها وقدرتها التدميرية.
6. صعوبة تحديد هوية مرتكبيها، وأيضا صعوبة استشعارها لعدم وجود مؤشر للتنبؤ بحدوثها.
7. القدرة على اختراق أكثر الأنظمة حماية، وإصابة أنواع مختلفة من الأجهزة الالكترونية مثل الحاسب الآلي أو الخوادم الالكترونية، وذلك على سبيل المثال وليس الحصر.

الفرع الثاني: أسباب انتشار الهجمات السيبرانية

ترتبط الهجمات السيبرانية عموما بمدى قدرة الانظمة المنية على حماية البيانات ومختلف التكنولوجيات المستخدمة في ذات الإطار وعليه نجد: (عزالدين، 2022، صفحة 115)

1. عدم صلابة بنية الشبكات المعلوماتية مما يسهل عملية اختراقها.
2. بقاء هوية المهاجم مجهولة مما يساعد على توسيع نطاق الهجمة.
3. الاعتماد المتزايد للدول على الفضاء السيبراني.

4. سهولة الوصول للمعدات المساعدة على الهجوم.

المطلب الثالث: سبل مواجهة الهجمات السيبرانية

تتعدد الطرق المستخدمة في مواجهة الهجمات السيبرانية، والتي تسعى إلى منع هذه الهجمات وتجنب المخاطر التي تترتب عليها، ويمكن تلخيص أبرز هذه السبل في النقاط التالية:

الفرع الأول: سبل مواجهة الهجمات السيبرانية

في ظل تزايد التهديدات السيبرانية أصبح من الضروري اعداد استراتيجيات وطرق من أجل الحماية وسنوضح أبرز السبل في النقاط التالية:

1. التطبيقات المضادة للفيروسات:

هو برنامج يتم استخدامه لاكتشاف البرمجيات الضارة ومنعها من إلحاق الضرر بالحاسوب أو سرقة البيانات الشخصية، وذلك عن طريق إزالتها أو إجراء التعديلات عليها وإصلاحها، بحيث يمكن لهذا البرنامج أن يتصدى لبرنامج التجسس، وبرنامج أحصنة طروادة، والتي هي عبارة عن شيفرات صغيرة تقوم ببعض المهام الخفية وغالبا ما تتركز على إضفاء قوى الدفاع واختراق جهاز الحاسوب وسرقة بياناته. (كاوجة، 2022، صفحة 115)

2. الاستراتيجية الهجومية:

وهي تلك الطرق التي يتم استخدامها ضد أطراف معينة قد تشكل خطرا مستقبلي على بياناتها، وتعتمد بالأساس على عملية إطلاق ديدان الكترونية أو فيروسات أو أي نوع آخر من الهجمات السيبرانية، ولعل أشهرها ما يسمى حصان طروادة التي تعتمد على حزمة الفيروسات الخفية التي تهاجم الخصم بشكل فجائي أو طريقة الأبواب الخلفية المعتمدة على استغلال ثغرات نظام العدو واستراتيجية حجب الخدمة، وتهدف كلها شل طرف معين أو زعزعة قدراته الهجومية. (بونيف، 2019، صفحة 128)

3. أنظمة كشف التسلل: تتألف أنظمة التسلل من عدة مكونات هي جهاز استشعار ينبه على وقوع الأحداث، ولوحة تحكم لمراقبة الأحداث والتنبيهات والتحكم بأجهزة الاستشعار، ومحرك يقوم بتسجيل إدخالات الأحداث المتلقات من خلال أجهزة الاستشعار في قاعدة البيانات. وتكون أنظمة التسلل مصنفة بالاعتماد على نوع وموقع أجهزة الاستشعار والمنهجيات المستخدمة على المحرك. (كاوجة، 2022، صفحة 116)

4. الاستراتيجيات الدفاعية: وتتمثل في مجموعة الإجراءات الدفاعية التي تتمثل في تطوير الذات وتقوية القدرات لمواجهة الأخطار الممكنة، وتتركز أغلبها في تجهيز مجموعة من الأنظمة ذات أبعاد مختلفة تتمثل في: (بونيف، 2019، صفحة 128)

أ. **البعد العسكري:** وهي عملية الحماية الأمنية للمعلومات من خلال بلورة أنظمة الدفاع السيبراني.

ب. **البعد السياسي:** وهو امتلاك الدولة الحق في حماية نظامها السياسي ومصالحها ومصالح مواطنيها، وذلك من خلال اعتماد استراتيجيات داخلية متمثلة في إجراءات محلية أو خارجية من خلال العمل على التوافق الدولي لحماية الأمن السيبراني.

5. جدران الحماية:

تعد من أقوى السبل الوقائية لمثل هذه الهجمات الحادة و الخطرة التي تمس أنظمة الكمبيوتر و الشبكات ، و التي تعرف أيضا بتسمية "الجدران النارية" ، أما عن بداية هذه التقنية فقد ظهرت أواخر عقد الثمانينات من القرن الماضي ، و ذلك استجابة لعدد من الاختراقات لشبكة الانترنت المستجدة حينذاك وقد ظهر منها عدة أجيال الجيل الأول يعرف بمرشحات العبور، يقوم مبدأ عمله على فلترة (تشريح) العبور و التي تمثل الوحدة الأساسية المخصصة لنقل البيانات بين الحواسيب على الانترنت .فإذا كانت العبوة تطابق مجموعة من شروط الجدار فإنه يسمح بمرور العبوة أو يرفضها و يتخلص منها و يقوم بإرسال إشارة أرو للمصدر ، في حال لم تكن مطابقة. (كاوجة، 2022، صفحة 116)

الفرع الثاني: الجهود الدولية المبذولة لمواجهة الهجمات السيبرانية

إن الاهتمام المتزايد بمواجهة الهجمات السيبرانية ساهم في ظهور العديد من المنظمات والاتفاقيات والمعاهدات التي قدمت حلولا ونصت على قوانين ملزمة وسوف نبين أبرز هذه الجهود من خلال ما يلي:

1. جهود منظمة الأمم المتحدة:

تباشر منظمة الأمم المتحدة دورا هاما في الحد من انتشار الجرائم السيبرانية، ومواجهة الآثار المترتبة عليها، ومن أجل تحقيق ذلك نظمت العديد من المؤتمرات نذكر منها المؤتمر السابع في ميلانو 1985 حتى المؤتمر الثاني عشر في 2010 بالإضافة إلى المؤتمر الخامس عشر للجمعية الدولية. وهكذا أصدرت منظمة الأمم المتحدة عدة قرارات وتوصيات بشأن العمليات السيبرانية، كما أنشأت فرقا من الخبراء الحكوميين المعنيين بهذه العمليات، وناقشت هيئاتها أمن الفضاء السيبراني. (عرفان، 2024، صفحة 3002)

2. مبادرات منظمة شنغهاي للتعاون (SCO): (حمدان، 2021، صفحة 26 27)

تم صدور اعلان ***"يكاترينبورغ"*** وذلك في قمة منظمة شنغهاي للتعاون التي عقدت في روسيا وقد أظهرت المنظمة من خلاله التعاون والالتزام بهدف منع الحروب والهجمات السيبرانية، والحاجة الملحة للرد على التهديدات السيبرانية واعتبر أمن المعلومات على نفس أهمية السيادة الوطنية، والأمن الوطني، والاستقرار الاجتماعي والاقتصادي.

-في عام 2011 تقدمت دول منظمة شنغهاي للتعاون بمشروع قرار للجمعية العامة للأمم المتحدة بشأن أمن المعلومات.

3. الاتفاقيات الدولية في مجال مكافحة الهجوم السيبراني:

تعد الاتفاقيات والمعاهدات الدولية من أهم صور التعاون الدولي بصفة عامة، وفي مجال مكافحة الجرائم الناتجة عن الهجوم السيبراني بصفة خاصة ومن بين المعاهدات والاتفاقيات التي تعمل على مكافحة الجرائم السيبرانية معاهدة بودابست لمكافحة جرائم الانترنت، وتوصيات المجلس الأوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات. (عرفان، 2024، صفحة 3002)

4. حلف شمال الأطلسي(الناتو): (حمدان، 2021، صفحة 24)

أدت تداعيات الهجمات السيبرانية التي استهدفت البنية التحتية الرقمية لإستونيا عام 2007 وأيضا الهجمات السيبرانية ضد جورجيا خلال نزاعها المسلح مع روسيا عام 2008 إلى سعي حلف شمال الأطلسي للتصدي للهجمات السيبرانية، فقد عمد إلى إنشاء مركز الدفاع الالكتروني التعاوني للتميز. وفي الفترة ما بين 2009و 2012، وبطلب من هذا المركز قامت مجموعة من الخبراء والباحثين القانونيين بتقييم إمكانية تطبيق المبادئ القانونية على الهجمات السيبرانية، وتم تتويج هذه الجهود بنشر دليل يعرف باسم " دليل تالين"**(Manual de tallin)** وهو عبارة عن وثيقة قانونية غير ملزمة، تنظم قواعد الاشتباك عبر الانترنت. وقد تم صدور اصدارين له.

أ. الإصدار الأول عام 2013 يركز على أهم وأشد الهجمات السيبرانية خطورة أي تلك التي تنتهك حضر استخدام القوة في العلاقات الدولية.

ب. الإصدار الثاني عام 2017 ويركز على أنواع القرصنة والهجمات السيبرانية الأخرى.

خلاصة الفصل:

تطرقنا في هذا الفصل إلى مفهوم الأمن السيبراني باعتباره ضرورة من ضروريات العالم، بالإضافة إلى المصطلحات التي لها علاقة به ، ثم بينا مدى أهميته في حماية المعلومات والأنظمة ومساهمته في الحفاظ على أمنها، كما تناولنا أهدافه التي يسعى لتحقيقها، وعرضنا كذلك أهم أبعاده المختلفة مثل البعد الاقتصادي والاجتماعي وغيرهم، كما تناولنا استراتيجيات الأمن السيبراني ومختلف أنظمته ومن بينها أمن انترنت الأشياء وأمن السحابية....إلخ، وكذلك تحدثنا عن مختلف خصائصه التي تميزه عن المجالات الأخرى كالثقة وعدم الثقة وما إلى كذلك، كما قدمنا لمحة عن أهم أنواع التهديدات السيبرانية منها التجسس المعلوماتي والتصيد الاحتيالي وغيرها ، وأيضا تطرقنا لمخاطر التهديدات السيبرانية ومجالات التهديدات، وأيضا أهم التحديات والعراقيل التي تواجهه، وكذلك خصائص الهجمات السيبرانية و أسباب الهجمات المتنوعة وأيضا سبل مواجهتها والجهود المبذولة موضحة في جملة من النقاط.

الفصل الثاني:

الإطار المفاهيمي للاستقرار المالي

تمهيد الفصل:

في ظل التغيرات السريعة التي تشهدها العولمة في شتى المجالات شهد القطاع المصرفي والمالي تطورات كبيرة. تمثلت في التحرر الاقتصادي، الذي أصبح من الضروري أن يصاحبه التأكيد على الاستقرار المالي. ويعتبر من بين الأهداف الرئيسية لأي اقتصاد، وزاد الاهتمام به بشكل كبير بعد حدوث الأزمات المالية. لذلك، أصبح من الضروري تعزيز الاستقرار المالي من خلال السياسات والتشريعات المناسبة، بهدف الحفاظ على استقرار الأسواق المالية وتعزيز النمو الاقتصادي المستدام. حيث تنوعت الأدبيات الاقتصادية في تعريفه، إلا أن جميع هذه التعريفات تتفق على أهميته. لهذا السبب، تم تشكيل لجان الاستقرار المالي بهدف الحفاظ عليه وتجنب الوقوع في أزمات مالية قد تأثر سلبا على الاقتصادات العالمية.

المبحث الأول: مدخل للتعريف بالاستقرار المالي

الاستقرار المالي هو أحد المكونات الأساسية وأداة مهمة للحفاظ على سلامة النظام المالي وتجنب الاضطرابات وضمان استمراريته، حيث أصبح من بين الاهتمامات التي تشغل الجهات المعنية على المستوى العالمي.

المطلب الأول: تعريف الاستقرار المالي وأهميته

يمثل الاستقرار المالي حجر الزاوية في بناء اقتصاد قوي ومتين لأي دولة، حيث يشير إلى قدرة النظام المالي على الصمود أمام التحديات والصدمات الاقتصادية المفاجئة.

الفرع الأول: تعريف الاستقرار المالي

الاستقرار المالي مصطلح متعدد الأوجه وقد تم اللجوء إلى تعريف عدم الاستقرار المالي ومن خلاله يتم توضيحه، سنقدم جملة من التعريفات كالتالي:

1. يرى "**R. Fergusson**" أنه تكون هناك حالة عدم الاستقرار المالي، عندما تبرز العوامل الخارجية للسوق وتؤثر سلبا على الاقتصاد الحقيقي. العوامل الخارجية هي القرارات التي اتخذت من قبل المتعاملين الماليين والاقتصاديين التي تؤثر سلبا على أنشطة باقي المتعاملين. (أحمد، 2020، صفحة 22)

2. من أهم المحاولات لتقديم تعريف للاستقرار المالي تلك الأبحاث التي قام بها غاري شينازي **Schinasi 2004** " يكون النظام المالي في صنف الاستقرار كلما كان قادرا على تسهيل وليس إعاقة أداء الاقتصاد وقادر على تشتيت الاختلالات المالية التي تتطور داخليا أو تنتج من أحداث سلبية مهمة وغير متوقعة." (بوبكر، 2015/2014، صفحة 49)

3. كما عرفه أيضا (**Das.u. quintyn and chenardk**)" من المدخل التحليلي الذي يتوافق إلى حد ما مع تحليل السلامة المالية الكلية، والتي تعرف بأنها القدرة على مقاومة الأزمات واستيعاب الصدمات والتعافي السريع منها، وتتميز بأنها أكثر قابلية للقياس، وقياس الاستقرار المالي يعتمد كذلك على مؤشرات قياسية، إضافة إلى أن السلامة المالية تشكل عنصرا رئيسيا في المفهوم الكلي للاستقرار. (أمال بن الدين، 2020/2019، صفحة 6)

4. ويشير**(andrew crochett)** الى ضرورة التفرقة بين مفهومين للاستقرار المالي وهما استقرار الأسواق. وحيث تعتبر البنوك في مقدمة المؤسسات المكونة للقطاع المالي، فان استقرار القطاع يتحقق عندما تزيد الثقة في أداء المؤسسات المصرفية، والتي تعد من وجهة نظره الركيزة الأساسية التي يعول عليها في نجاح القطاع المالي والقيام بدور الوساطة المالية. وعليه، فان حدوث تراجع الثقة بالجهاز المصرفي يعني ليس فقط حدوث اضطراب بأحد المكونات

الرئيسية للنظام المالي، بل قد يمتد أثر هذا الاضطراب لينعكس في انهيار قطاع الشركات والأسواق في ذات الوقت. (أحمد شفيق الشاذلي، 2014، صفحة 13)

5. ان مفهوم الاستقرار المالي لا يتعلق فقط بغياب الأزمات المالية ولكن أيضا بقدرة النظام المالي على الحد من ظهور الاختلالات واحتوائها والتعامل معها قبل أن تشكل خطرا على الشركة أو على الاقتصاد، وبالتالي فإن الاستقرار المالي ينطوي على أبعاد وقائية وعلاجية إذ يتميز الاستقرار المالي بأنه يتجاوز الحدود الحرجة، ليصل إلى مرحلة الأمان مما يؤدي إلى منع حدوث أزمة نظامية، لذلك فإن الاستقرار المالي مهم بشكل خاص لأي شركة. (التميمي، 2023، صفحة 474 475)

- نستنتج مما سبق بأن الاستقرار المالي هو:

-قدرة الدولة على إدارة مواردها المالية بشكل مستدام.

-الحد من الاختلالات والاضطرابات ومواجهة الأزمات التي تقع على القطاع المالي من أجل الحفاظ على توازن المؤسسات المالية والبنى التحتية، الأسواق المالية.

الفرع الثاني: أهمية الاستقرار المالي

يعتبر الاستقرار المالي أحد أهم الأهداف الأساسية التي يسعى صندوق النقد والبنك الدوليين الى تحقيقها للدول الأعضاء وذلك للحفاظ على توازن الاقتصاد العالمي. ويمكن توضيح أهمية الاستقرار المالي من خلال النقاط التالية:

1. ان الاضطرابات المالية تأتي في قمة المخاطر التي تهدد استقرار الاقتصاد العالمي. فقد أشار تقرير منتدى الاقتصاد العالمي الذي صدر عام 2008 بعنوان "المخاطر العالمية 2008" الى أن النظم المالية المضطربة، وخاصة أزمة الرهن العقاري التي تفاقمت في أمريكا في منتصف وأواخر عام2007، تمثل تحديا كبيرا يؤثر على استقرار الاقتصاد العالمي. لهذا فقد طالب التقرير بزيادة التدخل في أسواق المال لتقليل حدة المخاطر وتحسين حوكمة النظام المالي العالمي من خلال شبكة مسؤولين لإدارة المخاطر. وأكد التقرير على أن التركيز المتزايد على الأسواق المالية المضطربة والتوترات السياسية المتفاقمة في عام 2008 قد يدفعان الحكومات والشركات الى تجاهل المخاطر الأقل الحاحا مثل التغيرات المناخية، وهذا من شأنه أن يزيد في صعوبة التعامل مستقبلا مع هذه القضايا الحرجة بعيدة المدى. (أحمد، 2020، صفحة 36)

وللاستقرار المالي أهمية متزايدة أيضا نوضحها كالتالي: (سلطان، 2024، صفحة 649)

2. الاستقرار المالي عنصر أساسي لتحقيق النمو الاقتصادي، حيث بإمكان النظام المالي المستقر من امتصاص الصدمات المالية وبالتالي التقليل من انتقال آثار الأحداث السلبية للاقتصاد الحقيقي، فضلا عن تهيئة البيئة الملائمة

لتخصيص الموارد وتوجيهها إلى الاستخدامات المثلى أو الاستثمارات المنتجة والحد من المخاطر المعنوية ومخاطر عدم الامتثال والتقليل من حالات التضخم المفرط وكلها آثار مدمرة للنظام المالي.

3. تعد الاضطرابات المالية من أهم المخاطر التي تهدد استقرار الاقتصاد العالمي، لذلك فإن النظم المالية الغير المستقرة تأثر على استقرار الاقتصاد لهذه الدولة، لهذا تطالب المؤسسات المالية الدولية بالتدخل في أسواق المال وتحسين حوكمة النظام المالي العالمي والتقليل من حدة المخاطر.

4. إن استقرار القطاع المصرفي كأهم مكونات النظام المالي والذي يعد الممول والمحرك لجميع القطاعات الاقتصادية الأخرى، يعد عاملا محوريا لاستقطاب رؤوس الأموال الأجنبية والحفاظ عليها وتساهم في تحقيق التنمية الاقتصادية والاجتماعية الشاملة.

5. تكون الأزمات المالية أكثر خطورة عندما تكون نتيجة أثر تقلبات الدورات الاقتصادية المرتبطة بعملية الائتمان. (معوشي، 2022، صفحة 176)

المطلب الثاني: أهداف الاستقرار المالي، خصائصه وأسسه

يعد الاستقرار المالي غاية استراتيجية تهدف إلى حماية النظام المالي والتخفيف من آثار الصدمات الاقتصادية والتقلبات المفاجئة. كما يرتكز على منهجية متكاملة تجمع بين الأسس النظرية والتطبيقات العملية، سعيا لتحقيق التوازن الأمثل بين تحفيز النمو الاقتصادي وفرض ضوابط فعّالة لإدارة المخاطر المالية.

الفرع الأول: أهداف الاستقرار المالي

تتركز أهدافه الرئيسية على تحقيق التوازن بين متطلبات النمو الاقتصادي وضرورات الحماية من الأزمات أبرزها ما يلي: (الرفيعي، 2022، صفحة 105)

1. العمل على تشجيع واعتماد سياسة وقائية واستباقية وعلاجية في نفس الوقت.

2. تعزيز الاستقرار على مستوى النظام المالي بشكل كامل، وليس على مستوى المؤسسات الفردية فقط.

3. الحد من المشكلات التي تحدث في النظام المالي، وينبغي ألا تأثر في عناصر القطاع الحقيقي، والمشكلات التي تنشأ في المؤسسات المالية الفردية وألا تؤثر في النظام المالي بأكمله.

4. تعزيز قدرة النظام المالي في تحمل الصدمات وأداء دور مؤثر في عملية النمو الاقتصادي عن طريق دراسة وتحليل أهم العوامل والقطاعات التي تؤثر في استقرار النظام المالي، مثل سلامة المراكز المالية للمؤسسات المالية غير المصرفية، وسلامة المراكز المالية لقطاع الشركات وملائمة نمو الائتمان المصرفي مع حجم النشاط الاقتصادي.

ويمكن توضيح أهداف أخرى: (سعيد، 2022، صفحة 6)

5. استخدام الخدمات والمنتجات المالية من قبل الأفراد والشركات خاصة الفئات المستهدفة بحيث تكون رخيصة ومستدامة ومريحة لمجهزي الخدمات مع شرط عدم وجود تأثير مضاد في الاستقرار المالي والحماية المالية للمستهلك

6. الوصول إلى قطاع مالي فعال يساهم في تحقيق النمو الاقتصادي المرتفع والمستدام وتتناسب مؤشرات الأداء به مع المؤشرات الاقتصادية الكلية، وتعمل فيه الأسواق المالية بكفاءة مع الالتزام بالقواعد الاحترازية لتعاملات المؤسسات المالية بها، وتتحقق من خلاله الرقابة الفعالة على المؤسسات المالية، ويتمتع ببنية تحتية ذات كفاءة عالية تحظى بثقة المتعاملين.

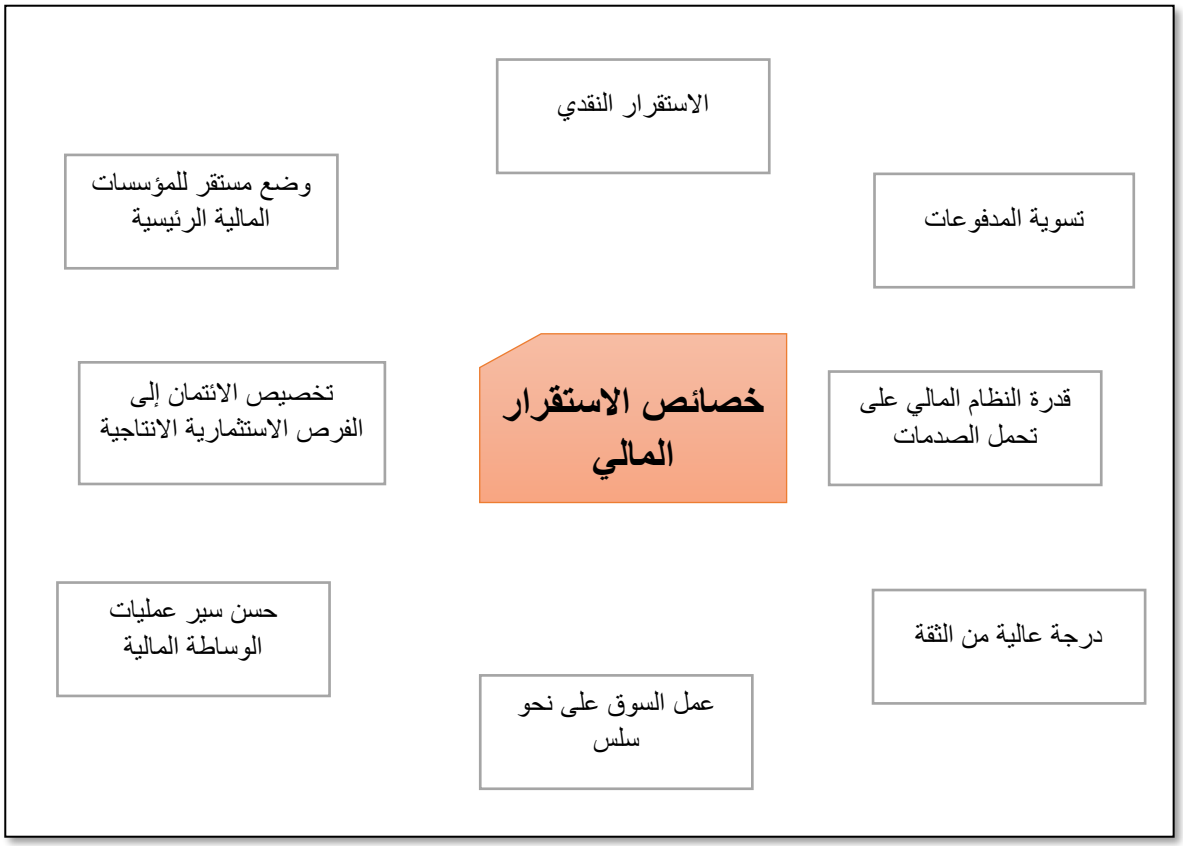
الفرع الثاني: خصائص الاستقرار المالي

بالرغم من التنوع الكبير في التعريفات المقدمة سابقا حول الاستقرار المالي، إلا أنه يتركز حول مجموعة من الميزات التي يتميز بها يمكننا تقديمها كالتالي: (ابراهيم، 2023/2022، صفحة 13)

قدرة النظام المالي على تسوية المدفوعات أو تخصيص الائتمان لفرص الاستثمار المنتج، والقدرة على تعزيز النشاط الاقتصادي مع حسن سير عمليات الوساطة المالية، وعمل السوق على نحو سلس وتوافر الائتمان، واتصاف المؤسسات الرئيسية في النظام المالي بالوضع المستقر، مع وجود درجة عالية من الثقة في قدرتها على الوفاء بالتزاماتها التعاقدية، والقضاء على تحركات الأسعار نسبيا للأصول الحقيقية أو المالية، الاستقرار النقدي والقدرة الداخلية للنظام المالي على الصمود أمام الصدمات.

نلخص أهم هذه الخصائص في الشكل الموالي:

الشكل رقم (03): خصائص الاستقرار المالي



المصدر: من اعداد الطالبتين بالاعتماد (ابراهيم، 2023/2022، صفحة 13)

الفرع الثالث: أسس الاستقرار المالي

يعتمد تحقيق الاستقرار المالي على منظومة متكاملة من الأسس الحيوية التي تضمن قوة النظام المالي وقدرته على الصمود، يمكن توضيحها كالتالي: (الشربيني، 2018، صفحة 308 309)

1. الثقة حيث عادة ما تكون مؤسسات النظام المالي مستقرة إذا توافرت لديها درجة عالية من الثقة في قدرتها على الوفاء بالتزاماتها باستمرار ودون مساعدات خارجية.
2. تجنب الاضطرابات حيث أن الهدف من الحفاظ على استقرار النظام المالي هو تجنب حدوث اضطرابات فيه، والتي من شأنها أن تؤدي الى التسبب في تعرض الاقتصاد الحقيقي لأضرار وتكاليف كبيرة.
3. حدوث استقرار نقدي والذي يتمثل في انخفاض معدل التضخم، واستقرار أسعار الصرف.
4. توفر الثقة في المؤسسات والأسواق المالية العاملة في الاقتصاد.
5. عدم وجود تقلبات حادة في أسعار الأصول المالية أو الحقيقية في الاقتصاد دون دواعي موضوعية.

المطلب الثالث: محددات الاستقرار المالي ومظاهره

يخضع تحقيق الاستقرار المالي لمجموعة من العوامل الحاسمة والتي يمكن تصنيفها إلى جملة من المحددات وبعض المظاهر التي تساهم في بناءه:

الفرع الأول: محددات الاستقرار المالي

هناك بعض الدعائم التي ساهمت في شرح مختلف هذه المحددات موضحة كالتالي: (مخلوف، 2016/2015، صفحة 172 173)

1. الشروط الرقابية والقانونية (Regulatory and Supervisory condition)

أ. ضبط ومراقبة النظام المالي على المستوى الجزئي والكلي وذلك بهدف تسيير وإدارة المخاطر.

ب. إدارة الأزمات المالية والمصرفية بفاعلية: وجود إطار فعال للتعامل مع الأزمات ومعالجة اثارها لتقليل أثرها على الاستقرار المالي وذلك من خلال إجراء مراجعة لدور جميع الجهات ذات العلاقة لتحديد دور كلا من المؤسسات في التعامل مع هذه الأزمات المصرفية.

ج. مع الأخذ بالاعتبار السياسة النقدية والسياسة المالية والسياسات الأخرى (مثل حماية الزبائن والتنافسية والمعايير المحاسبية) والاقتصاد المحلي والإقليمي والعالمي.

2. الشروط المتعلقة بالسوق وبالبنية التحتية (infrastructure Market and conditions)

أ. البنية التحتية القانونية للتمويل بما في ذلك نظام الاعسار وحقوق الدائن وشبكات الأمان المالية.

ب. نظام البنية التحتية للسيولة بما في ذلك العمليات النقدية والصرف المدفوعات ونظم تسوية الأوراق المالية والتبادل وأسواق رأس الأوراق المالية.

ج. الشفافية، الحوكمة والبنية التحتية للمعلومات، بما في ذلك شفافية السياسة المالية والنقدية، حوكمة الشركات، إطار المحاسبة والتدقيق، تقارير نظام الائتمان.

الفرع الثاني: مظاهر الاستقرار المالي

يمكن رصد مختلف مظاهره الأساسية التي تعكس متانة وكفاءة النظام المالي: (مصطفى، 2022، صفحة 209)

1. تسيير كفاءة توزيع الموارد الاقتصادية، حسب المناطق الجغرافية ومع مرور الوقت، إلى جانب العمليات المالية والاقتصادية الأخرى (كالادخار والاستثمار، والاقراض والاقتراض، وخلق السيولة وتوزيعها، وتحديد أسعار الأصول، وأخيرا تراكم الثروة ونمو الناتج).

2. تقييم المخاطر المالية وتسعيرها وتحديدها وإدارتها.

3. استمرار القدرة على أداء هذه الوظائف الأساسية حتى مع التعرض للصدمات الخارجية أو في حال تراكم الاختلالات.

4. الذعر المالي ويقصد به تلك الظاهرة التي ينتج عنها حدوث التهافت على سحب الودائع من البنك.

5. الانهيار المالي وهو ما يتعلق بانهيار الأسواق المالية.

6. عدم استقرار الأسعار والذي يمكن أن يأخذ شكلين وهما التضخم والانعكاس في الأسعار. (ساعد، 2014/2013، صفحة 91)

المبحث الثاني: ماهية الاستقرار المالي

يعتبر تحقيق الاستقرار المالي مسؤولية تشاركية بين الحكومات والمؤسسات المالية والجهات الرقابية من خلال تعزيز الأطر التنظيمية والرقابية واعتماد أفضل الممارسات العالمية.

المطلب الأول: أسباب اللااستقرار المالي وإجراءات الحفاظ عليه

يشكل عدم الاستقرار المالي تحديا كبيرا حيث يظهر من خلال التقلبات التي تضعف القدرة على إدارة الموارد المالية بكفاءة. ومع ذلك، يمكن مواجهة هذه التحديات من خلال مجموعة من الإجراءات الوقائية والتصحيحية التي تعمل على تعزيز الاستقرار المالي وحماية الاقتصاد من الآثار السلبية المحتمل.

الفرع الأول: أسباب اللااستقرار المالي

لتفسير أسباب عدم الاستقرار المالي يمكن الرجوع إلى عدة نظريات، نذكر منها: الهشاشة المالية النقدية، عدم اليقين، الصناعة المالية سيتم تناول أهم نظرية وهي الهشاشة المالية لمينسكي سنوضحها كما يلي: (ريمة، 2012-2013، صفحة 26 27)

1. قدم مينسكي طرحا مغايرا للطرح السائد في الأدبيات المالية فوفقا لنظريته فإن القطاع المالي في الاقتصاد الرأسمالي عامة يتسم بالهشاشة وتختلف درجة هشاشته باختلاف المرحلة التي يمر بها الاقتصاد من مراحل الدورات الاقتصادية، ومن ثم تزيد خطورة حدوث أزمة في ذلك القطاع على الاقتصاد ككل.

توصل مينسكي إلى فرضية عن عدم الاستقرار المالي قام بصياغتها في شقين:

أ. الشق الأول يتمثل في أن الاقتصاد الرأسمالي عبارة عن أنظمة تمويل تساهم في استقراره وأخرى تعمل على عكس ذلك، أي في عدم استقراره.

ب. أما الشق الثاني فانه يتمثل في لأن طول فترة الرخاء والازدهار يؤدي بالاقتصاد إلى أن ينتقل من العلاقات الاقتصادية المستقرة إلى العلاقات المالية الغير مستقرة.

2. ويمكن تلخيص أسباب عدم الاستقرار المالي في أربع فئات رئيسية وهي العوامل الداخلية للمؤسسة التي تشمل تباين المعلومات بصرف النظر عن مصادرها، العوامل المؤسسية التي تؤثر بدورها في الاقتصاد الكلي والموازنة العامة، العوامل الخارجية التي تتمثل في بنية الأسواق المالية الدولية التي قد ينتج عنها أزمات أسعار الصرف وأخيرا وجود سياسات غير مستقرة وضعف قواعد الحوكمة. (رميس، 2015، صفحة 4 5)

الفرع الثاني: إجراءات الحفاظ على الاستقرار المالي

من أجل تحقيق الاستقرار المالي وضمان استقرار الاقتصاد الكلي يتم اتخاذ مجموعة من الإجراءات على صعيد السياسات لبناء نظام مالي قادر على التكيف مع التحديات والحماية من الأزمات وهي كالتالي:

1. السياسة الوقائية :

تعتبر السياسة الملائمة له بغية مواصلة الاستقرار من خلال الاعتماد على الانضباط وفق شروط السوق وأعمال الإشراف والرقابة الرسمية. وتتمثل الأدوات الوقائية الرئيسية في النظام المالي السليم تلك التي تساهم في عدم تراكم الاختلالات التي يمكن أن تؤدي إلى وقوع أزمة، وترتبط بتعزيز درجة الانضباط في الأسواق، ومراجعة عمليات التنظيم والرقابة والاتصال الرسمية. وقد يتطلب الأمر إجراء تعديلات في أسلوب تقدير مواطن الضعف والأدوات والسياسات التي من شهادة التأثير على النظام المالي. (الشاذلي، 2014، صفحة 48)

2. السياسة التصحيحية:

تكون هناك اختلالات داخل القطاع المالي ويكون هناك تخوف من انتقال تداعياتها للقطاع الحقيقي، فتتخذ السلطات المعنية إجراءات لتؤثر على حجم هذه الاختلالات وذلك من خلال القيام بمراجعة التنظيم والرقابة وإدارة الأزمات وهي ما تعرف بالإجراءات التصحيحية أو العلاجية وتخص إجراءات التدخل المتعلقة بالمؤسسات المالية دور المقرض الأخير، وهنا يجب أن نميز بين دعم السيولة ودعم الملاءة. (مطاي، 2019، صفحة 93)

أ. دعم السيولة:

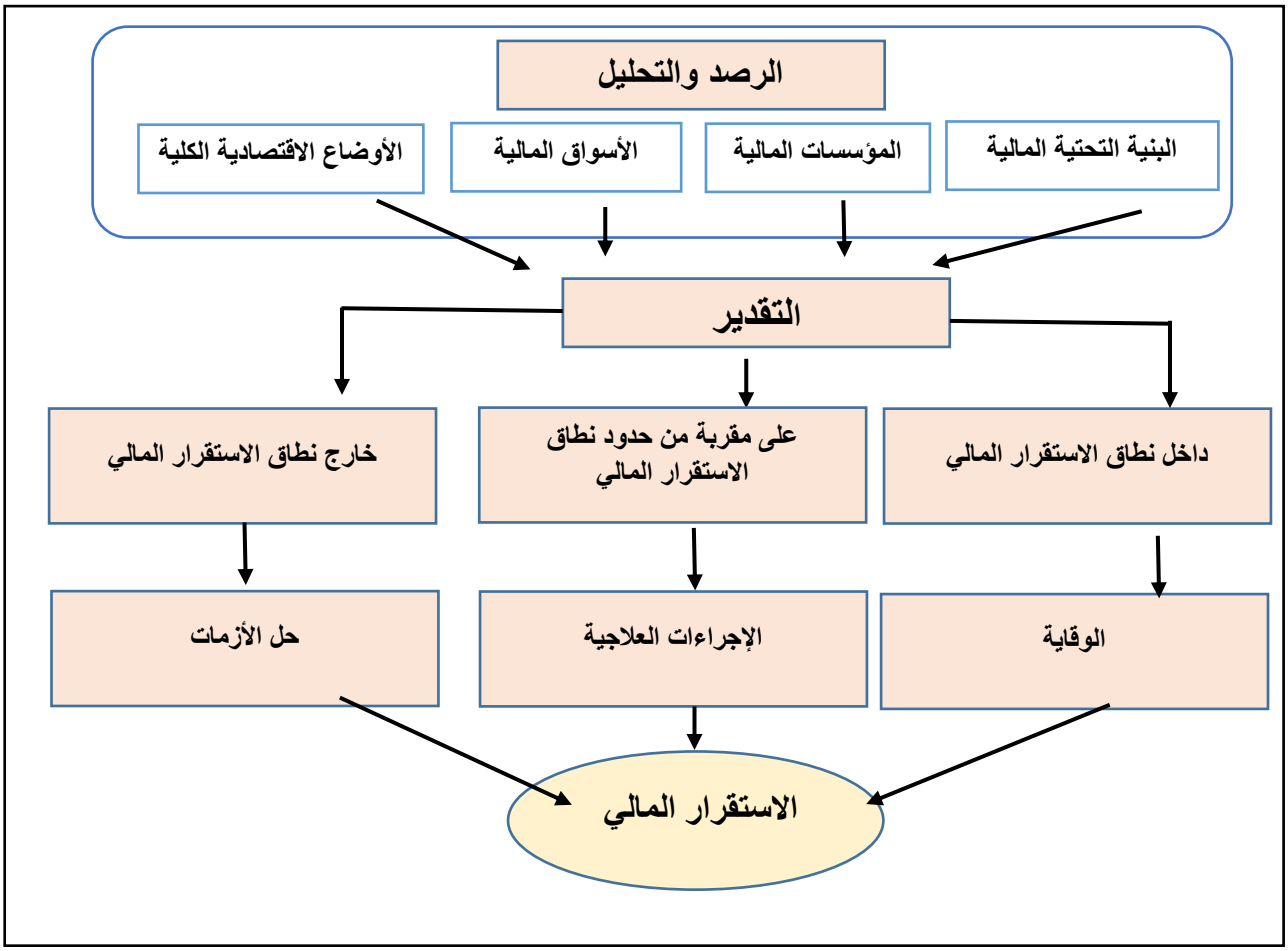
يتم اللجوء إلى هذا الاجراء في حالة عدم عمل نظام ال (**IT** أنظمة رقابة قائمة على تقنيات الاعلام الالي والتكنولوجيا الحديثة) لبنك ما بشكل صحيح، حيث تقود العمليات الكلاسيكية للمقرض الأخير إلى ضخ السيولة في البنوك التجارية، ولكن ما نلاحظه هو أن الدول التي تتبع نظام **Currencyboard** تسجل صعوبات في القيام بدور المقرض الأخير.

ب. دعم الملاءة:

يكون المشكل أكثر خطورة وتهديدا إذا فقدت إحدى المؤسسات مالية كانت أو غير مالية ملاءتها، ويجب على هذه الحكومة في هذه الحالة أن تقرر ما إذا كان من الضروري أن تمنح هذه المؤسسة مساعدة فورية، وتقوم الحكومة بمساعدة هذه المؤسسات من أجل تجنب تشوه النشاط الاقتصادي وحماية الدائنين والقضاء على خطر العدوى. (قلادي، 2017، صفحة 323)

ويمكننا توضيح آلية العمل لتحقيق الاستقرار المالي من خلال المخطط التوضيحي التالي:

الشكل رقم (04): آلية العمل لتحقيق الاستقرار المالي



المصدر: (طيبي، 2023، صفحة 223)

المطلب الثاني: المخاطر التي تواجه الاستقرار المالي ومتطلباته

يواجه في عالم اليوم مجموعة متشابكة من التهديدات والمخاطر التي تتطلب آليات متكاملة للتعامل معها تتنوع هذه المخاطر بين ما هو مألوف وما هو تقليدي وما هو مستجد.

الفرع الأول: المخاطر التي تواجه الاستقرار المالي

يواجه الاستقرار المالي مجموعة من المخاطر التي قد تتسبب في حدوث الاختلالات، لذلك فإن إدارة هذه المخاطر بشكل فعال يتطلب تعزيز آليات الرقابة المالية من أجل حماية الاقتصاد من الاضطرابات المحتملة وتنقسم هذه المخاطر إلى قسمين: (بودیار، 2023/2022، صفحة 52)

1.مخاطر داخلية:

قد تنشأ هذه المخاطر في أي من عناصر النظام المالي الأساسية الثلاثة وهي المؤسسات، الأسواق والبنية التحتية حيث:

أ. المؤسسات:

قد تنشأ المشاكل في مؤسسة مالية معينة وتنتشر لاحقا إلى قطاعات أخرى من النظام المالي، أو تتأثر بها عدة مؤسسات أخرى على نحو متزامن نظرا لتعرضها لمخاطر مماثلة.

ب. الأسواق:

عادة ما تكون الأسواق معرضة لمخاطر الطرف المقابل، عدم اتساق أسعار الأصول، موجات السحب، والعدوى.

ج. البنية التحتية:

قد يترتب عن المشاكل الناشئة في المؤسسات المالية (مثل حالات توقف النظم التشغيلية، تركز المخاطر وسلسلة الاثار التعاقبية) حدوث مشاكل في البنية التحتية المالية في نظامي المقاصة والتسوية، على سبيل المثال وينجم عنها مضاعفات أكبر على النظام المالي. وفي المقابل، فإن مواطن الضعف الناشئة من البنية التحتية في الجهازين القانوني والمحاسبي مثلا قد يترتب عليها حالات من التوقف عن العمل.

2. مخاطر خارجية:

ومصدرها الاضطرابات على مستوى الاقتصاد الكلي، أو أحداث أخرى مثل الكوارث الطبيعية أو الأحداث السياسية، التي تؤثر في أداء النظام المالي، والنظام المالي المستقر، حسب التعريف، يجب أن يكون قادرا على مواجهة هذه المخاطر، بتشتيت الاختلالات الناجمة عنها لتخفيف اثارها. (نجاة، 2023، صفحة 100)

3. مخاطر نظامية:

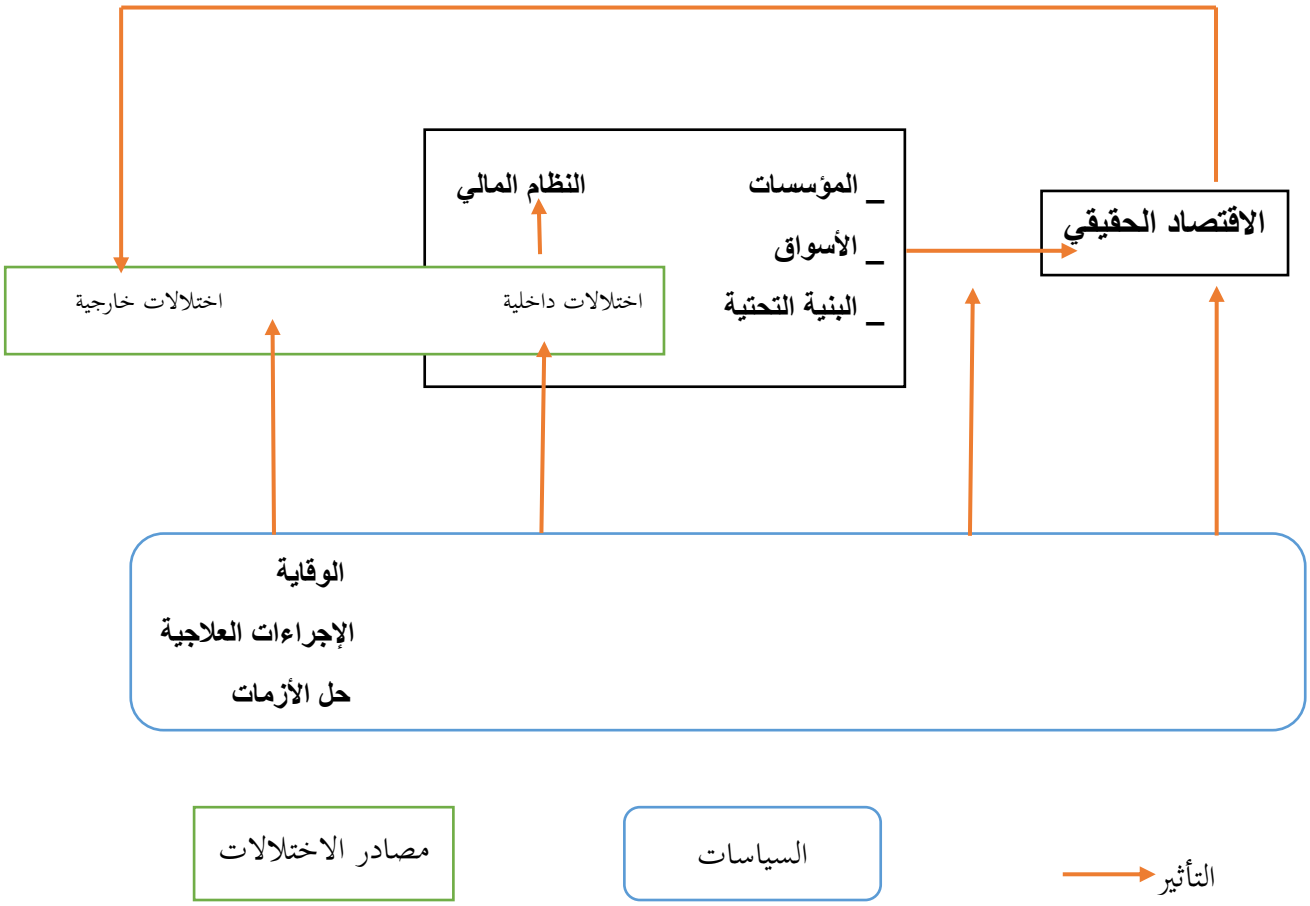
تشير إلى أي نوع من المخاطر التي قد تحدث للنظام المالي ولكن لا تؤثر هذه المخاطر على قطاع معين بل يمتد آثارها إلى باقي القطاعات الاقتصادية الأخرى، وتمثل المخاطر النظامية جميع الأحداث الخارجية التي تحدث نتيجة

التغيرات الاقتصادية أو السياسية، وتؤثر على الشركات في القطاعات الاقتصادية المختلفة. وتكون في نفس الوقت خارجة عن السيطرة.

وتعتبر من أهم التحديات التي تواجه البنوك من حيث كيفية تحديدها وقياسها وادارتها والسيطرة عليها لما لها تأثير على الاقتصاد ككل ولا ينحصر تأثيرها على قطاع معين. (صقر، 2024، صفحة 426)

ويمكن أن نبين أهم العوامل المؤثرة في أداء النظام المالي حسب شيناسي من خلال الشكل الموالي:

الشكل رقم (05): العوامل المؤثرة في أداء النظام المالي.



(شيناسي، 2005، صفحة 05)

الفرع الثاني: متطلبات تحقيق الاستقرار المالي

يتطلب تحقيق الاستقرار المالي والحد من عدم اليقين السائد توفر عدة متطلبات مهمة وأساسية أهمها:

1. توفر قطاع مالي كفأ:

يتطلب تحقيق الاستقرار الاقتصادي المستدام بالضرورة وجود قطاع مالي متطور ومستقر وقادر على توجيه المدخرات لتمويل فرص الاستثمار المنتجة القادرة على توفير المزيد فرص العمل، ورفع مستويات الإنتاجية للمستويات

القصوى الممكنة. ومن ثم فإن تحقيق الاستقرار في القطاع المالي يمكن اعتباره نقطة الانطلاق نحو تحقيق الاستقرار الاقتصادي، وتنعكس سلامة القطاع المالي وقدرته على امتصاص الصدمات والحد من تداعياتها على الاقتصاد الحقيقي. (بوديار، 2023/2022، صفحة 53)

2. توفر استقرار نقدي:

يتطلب الاستقرار المالي استقرارا نقديا يتمثل في قدرة القطاع النقدي على تحقيق استقرار المستوى العام للأسعار عند المستويات المستهدفة، ووجود هيكل واضح لأسعار الفائدة ينسجم مع التطورات الاقتصادية المحلية والدولية، يستطيع بدرجة مناسبة من الكفاءة تنظيم كمية وأسعار وشروط الائتمان بشكل يدعم النمو الاقتصادي ويحول دون تركز وتراكم مخاطره خاصة فيما يتعلق بالقطاعات الأكثر عرضة للتقلبات. (محمد، 2023، صفحة 425)

المطلب الثالث: التحديات التي تواجه تحقيق الاستقرار المالي والجهود المبذولة في مواجهتها

هناك مجموعة من التحديات التي تهدد وتقف أمام تحقيق الاستقرار المالي يتوجب التصدي لها وذلك من خلال تطبيق الجهود المبذولة سنقوم بإبرازها كما يلي:

الفرع الأول: التحديات التي تواجه تحقيق الاستقرار المالي

هناك مجموعة من التحديات والعراقيل التي تعتبر بمثابة تهديد كبير يجب التصدي له بشتى الطرق موضحة كما يلي:

1. تراجع الشفافية:

دعونا ننظر في مثال يتناول حالة بنك استثماري في هونغ كونغ يشتري حصة من أسهم رأس المال في شركة صينية ثم يقوم بتقسيم التدفقات النقدية، وقيمة الزيادة في رأسمال الاستثمار، ومخاطر الطرف المقابل، بحيث يبيع هذه الحصص الجزئية منفصلة لمستثمرين في بلدان مختلفة وعادة ما تؤدي أي معاملة مالية من هذا القبيل في زيادة فرص جمع الأموال والاستثمار وتوزيع المخاطر على من هم أكثر قدرة على تحملها غير أن المعلومات المتعلقة بكثير من الأنشطة لا تكون متاحة للمستثمرين وجهات الرقابة المصرفية نظرا لأنها مقيدة خارج الميزانية العمومية. (غاري شيناسي، 2005، صفحة 3 4)

2. المخاطر المعنوية:

تنجم عن مشاكل خارج النظام المالي فالاستقرار المالي حساس للصدمات الخارجية مثل الكوارث الطبيعية، والتغيرات في الميزان التجاري للبلد، والأحداث السياسية، وتقلبات أسعار النفط، والابتكارات التكنولوجية، والتحولات المفاجئة في معنويات السوق، أو توقف دولة مجاورة على سداد الديون السيادية. قد تؤدي أحداث الاقتصاد الكلي إلى إضعاف ثقة السوق وخلق اختلالات في النظام بأكمله. (طيبي ب.، 2023، صفحة 225)

3. ديناميكية الأسواق:

لقد أدت عولمة التمويل وتزايد اعتماد كثير من الشركات على أسواق الأوراق المالية بدلا من البنوك للحصول على الأموال اللازمة للتمويل إلى إحداث تغيرات حادة في ديناميكية السوق، فقد انخفضت تكاليف المعاملات إلى الحد الأدنى، وأصبح بالإمكان إجراء قدر هائل من المعاملات في وقت وجيز للغاية كما أدت عمليات البيع أو الشراء الضخمة والمتواصلة، على غرار ما يحدث فيما يسمى "سلوك القطيع" إلى تفاقم حركات الأسعار، كما يترتب على اثره أيضا انتشار المشاكل من السوق المضطربة إلى السوق التي لم تسرب إليها الاضطرابات بعد، وذلك لما يعتقد المستثمرون أن ثمة أوجه تشابه بين السوقين. (عبد الرحمان بن ساعد، 2013 2014، صفحة 94)

4. زيادة درجة التوسع والتعقيد بالنظام المالي:

أدت إلى صعوبة مواكبة التطورات في أسعار الأصول المالية المتداولة، وخاصة في ظل التوسع الكبير في حجم هذه الأصول في العديد من الاقتصادات المتقدمة ليشكل أكثر من ضعف إجمالي الناتج المحلي السنوي في بعض الأحيان.

5. الفجوة التكنولوجية والمعرفية:

قد توجد فجوة تكنولوجية ومعرفية بين المؤسسات أو الشركات أو الأسواق وبين الجهات الرقابية والاشرافية. فالاستثمارات الخارجية غالبا ما تترافق مع تطور هائل للتكنولوجيا الحديثة والوسائل المعرفية فمواكبة التكنولوجيا أمر مهم للغاية ويشكل تحديا كبيرا لارتفاع تكاليفه. (الشاذلي، 2014، صفحة 21)

الفرع الثاني: الجهود المبذولة لمواجهة التحديات

تعمل الحكومات والمؤسسات المالية الدولية على تعزيز الاستقرار المالي من خلال مجموعة من الجهود والسياسات الاستباقية وتشمل: (الشاذلي، 2014، صفحة 24)

1. تعزيز الشفافية والافصاح والتي تساهم في انضباط الأسواق وذلك من خلال توفير المعلومات اللازمة والموثوقة من أجل اتخاذ القرارات الاستثمارية السليمة من طرف المتعاملين بالأسواق المالية. وعدم شفافية هذه البيانات المالية من أسباب حدوث الأزمات المالية.

2. تسليط الضوء على قضايا تحرير حساب رأس المال خصوصا فيما يتعلق بانفتاح الأسواق المالية بالدول النامية سواء من حيث المبدأ أو من حيث الكيفية.

وهناك أيضا: (السن، 2015، صفحة 31)

3. يجب على الدولة أن تأخذ في الحسبان طبيعة ظروف السوق المالي بحيث تقوم بالقضاء على المضاربات المالية الضارة بالسوق مع العمل على القضاء علة الأسواق السوداء التي تظهر من حين لآخر، ولكي تقوم بذلك يجب عليها انتهاج سياسة سعر الصرف مرنة، مما يجعل دائما السوق المالي صحيا، وجاذبا ومشجعا للاستثمار.

4. تقوية ودعم القطاع المالي والمصرفي وذلك من خلال اصدار أسس للرقابة المصرفية الفعالة، تتضمن الصلاحيات الممنوحة للسلطات الرقابية، والدور المتوقع من البنوك لمواكبتها، فضلا عن وضع منهجيات تطبيق هذه الأسس، وذلك بمشاركة السلطات الرقابية بالدول الأعضاء لضمان الالتزام بتطبيقها.

5. أكد صندوق النقد الدولي على تعزيز الانضباط في الأسواق المالية المحلية والدولية فيتمثل في حث الدول على استحداث وتطوير البنية التحتية للقطاع المالي. (الشاذلي، 2014، صفحة 25)

المبحث الثالث: تهديدات الهجمات السيبرانية على الاستقرار المالي

تعد الهجمات السيبرانية أحد التهديدات التي تواجه الأنظمة المالية والاستقرار المالي وأحد المخاوف التي تعتبر عائقا بالنسبة للدول وتعرض البيانات الحساسة والموارد المالية للخطر.

المطلب الأول: مؤشرات الاستقرار المالي والمخاطر السيبرانية

تلعب المخاطر السيبرانية دورا متزايدا في تهديد الاستقرار المالي ومن خلال هذه المخاطر يتم الاستعانة بمجموعة من المؤشرات لقياس مستواه ومدى التعرض للمخاطر الالكترونية.

الفرع الأول: مؤشرات الاستقرار المالي

هناك العديد من المؤشرات الرقابية التي تستخدم من أجل اكتشاف أوجه الخلل في أداء المصارف في وقت مبكر وقبل حدوث الحدث حتى لا تتعرض لمشاكل مالية تؤدي الى انهيارها وذلك لاتخاذ ما يلزم من الإجراءات اللازمة وفيما يلي سنعرض مختلف هذه المؤشرات:

1. الإنذار المبكر (EXW)

هناك عدة مؤشرات رقابية للإنذار المبكر بالأزمات المالية تستخدم لقياس مدى سلامة الأداء المصرفي، إذ تستخدم كمؤشرات لتقييم أداء المصارف ثم تصنيفها واكتشاف أوجه الخلل المالي في أدائها قبل وقت مبكر حتى لا تتعرض لمشاكل مالية تؤدي إلى انهيارها، وتقوم هذه المؤشرات بالتعريف باحتمالات الحدوث في وقت مبكر قبل وقوع الحدث لاتخاذ ما يلزم من سياسات وإجراءات وقائية أو مانعة من وقوع الأزمات، ومن أهم هذه المؤشرات

التي تستخدم في هذا المجال مؤشرات الحيطة الكلية. وتنبع أهمية مؤشرات الإنذار المبكر بالأزمات من كونها مؤشرات تدل على مدى سلامة واستقرار النظام المالي وتساعد على تقييم مدى قابلية القطاع المالي للتأثر بالأزمات المالية والاقتصادية، وهي أيضا تعمل كأداة للإنذار المبكر في حالة تعرض الجهاز المصرفي المالي للخطر. (علي، 2015، صفحة 3)

2. مؤشر الحيطة الكلية

هي مؤشرات رقابية تستخدم في تقييم مدى تأثر النظام المصرفي بالصدمات والأزمات الاقتصادية الكلية من خلال رصد التقلبات المفاجئة في التغيرات الاقتصادية الكلية واتخاذ الإجراءات الكفيلة بالتخفيف عن تأثير هذه التغيرات في النشاط المصرفي. (بلعيد سمية و بوراس أحمد، 2022، صفحة 555)

وتنقسم مؤشرات الحيطة الكلية إلى قسمين:

أ. الحيطة الجزئية:

تعتبر من أهم المؤشرات المعتمدة في تحديد المخاطر المصرفية التي تشكل نقاط الضعف في العمليات المالية والتشغيلية والإدارية للمصرف، والتي تتطلب عناية رقابية خاصة لتقييم السلامة الكلية لأداء القطاع المصرفي كاملا، وهي تعتمد على مؤشرات تجميعية أساسية تعرف ب **CAMELS** وهي ست عناصر رئيسة: (الحموي، 2016، صفحة 42)

c. كفاية رأس المال.

A. جودة الأصول.

M. سلامة الإدارة.

E. الربحية.

L. السيولة.

S. حساسية السوق.

ب. الاقتصاد الكلي:

يعتمد الجهاز المالي على مجمل النشاطات الاقتصادية، وهو كذلك يتأثر بالتغيرات الاقتصادية التي تصيب الاقتصاد ككل. وقد أشارت بعض الدراسات الحديثة أن بعض التطورات الاقتصادية الكلية تسبق الأزمات المالية، مما يتطلب مراقبة بعض المتغيرات على الاقتصاد ككل وخصوصا تلك التي تتعلق بهروب رأس المال. (قطاف، 2020/2019، صفحة 53)

3. مؤشرات السلامة المالية (Financial safety)

يشار لمفهوم السلامة المالية على أنه قدرة المصرف على إدارة عملياته الخاصة بالوفاء بديونه في ظروف اقتصادية غير متوازنة بالاعتماد على رأس المال والاحتياطات التي بحوزته.

ويعرف أيضا على أنه الحالة التي يخصص فيها النظام المالي موارده المالية بشكل فعال بين مختلف الأنشطة بما يضمن إدارة وتشخيص الأزمات المالية بهدف استيعاب الصدمات لتحقيق الاستقرار المالي. (خربص، 2023، صفحة 197)

أ. مؤشرات السلامة المالية المتعلقة بالسيولة والملاءة: (لعور، 2022، صفحة 40 41)

تختلف مؤشرات السيولة المحسوبة على حسب الغرض منها، ونظرا لكون معظم الأزمات يرجع سببها لنقص في السيولة لدى المؤسسات المصرفية، زاد الاهتمام بمراقبة سيولة تلك المؤسسات بالاعتماد أساسا على بعض نسب السيولة أهمها نسبة السيولة القانونية والتي تساعد على تحديد قدرة البنك على الوفاء بالتزاماته الجارية ولدينا أيضا نسب الأصول السائلة ونسب جودة الأصول، أما فيما يخص الملاءة فتعرف على أنها قدرة الفرد أو المؤسسة على الوفاء بالتزاماتها.

ب. مؤشرات السلامة المالية المتعلقة بالربحية:

تعرف على أنها: " قدرة البنك على تحقيق الربح، فهي تحدد على أساس نسب مالية مأخوذة من الميزانية وحسابات النتائج الخاصة بالبنك".

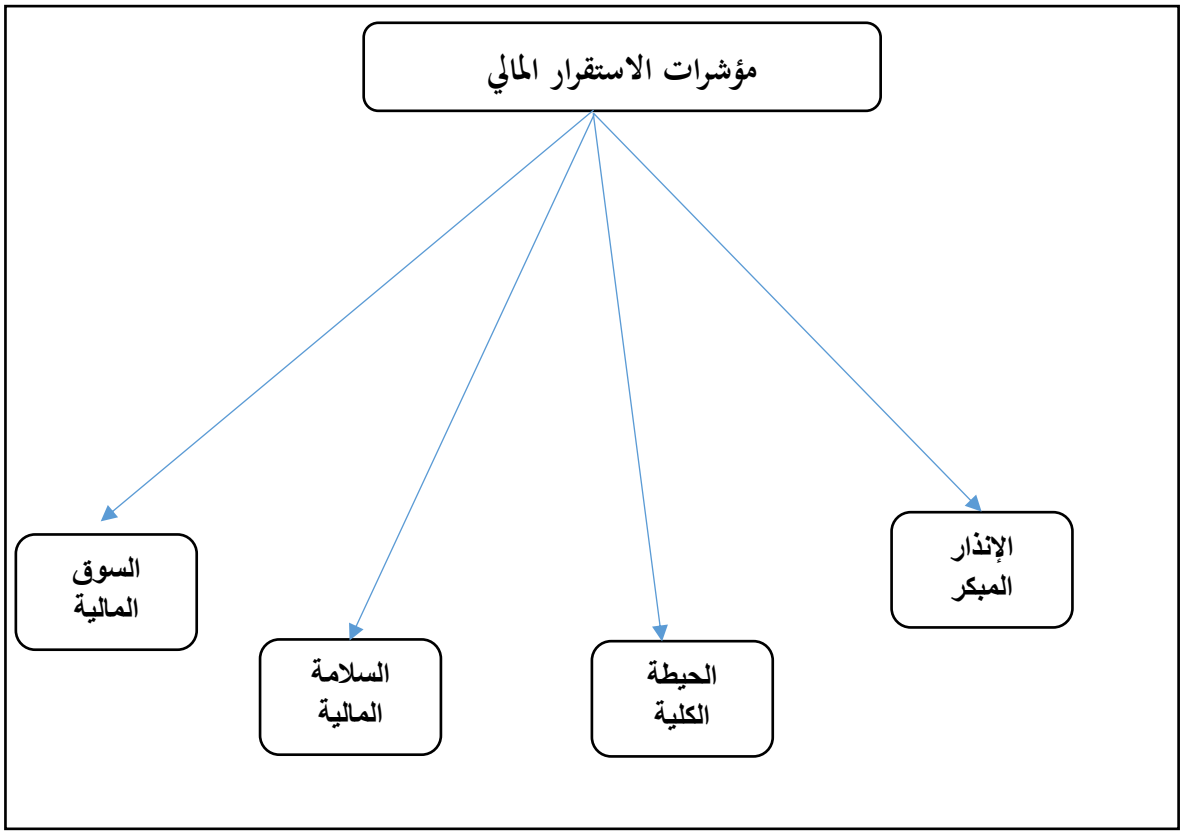
تسمح هذه المؤشرات بقياس مدى كفاءة إدارة المصرف على تحقيق الربح على الموجودات أو الأصول وعلى حقوق الملكية، فهي تمثل العائد على الأموال المستثمرة من قبل المساهمين.

4. مؤشر الأسواق المالية (آمنة، 2021/2020، صفحة 49 50 51)

يقيس مؤشر السوق المالي مستوى الأسعار في السوق، حيث يقوم على عينة من الشركات المدرجة في السوق المنظمة أو غير المنظمة، ويتم اختيار العينة بعناية ما يسمح للمؤشر بأن يعكس حالة السوق. فهو عبارة عن قيمة رقمية مطلقة بصورة متوسطات أو أرقام قياسية تصلح لعمليات المقارنة، الملاحظة، التتبع والقياس، للتغيرات الزمنية أو التغيرات المقطعية بين الشركات والصناعات والأسواق والأقاليم ودول العالم في مستوى زمني معين، والحاصلة في سوق رأس المال وبشكل رئيسي سوق الأسهم، سواء كانت سوق منظمة أو غير منظمة.

ويمكن تلخيص أهم هذه المؤشرات من خلال الشكل التالي:

الشكل رقم(06): مؤشرات الاستقرار المالي



المصدر: من اعداد الطالبتين اعتمادا على ما سبق.

الفرع الثاني: تعريف المخاطر السيبرانية وأثرها على المؤسسات المالية

تعتبر المخاطر السيبرانية الناتجة عن التحول الرقمي والتطور التكنولوجي من بين التهديدات التي تؤثر على القطاع المالي والمصرفي وتعتبر إشكالية كبيرة تتطلب المراقبة بالنسبة للمصارف والمؤسسات المالية.

1. تعريف المخاطر السيبرانية:

أ. عرفها بنك التسويات الدولية على "أنها الخسارة المالية أو الاضطراب أو الإضرار بسمعة المؤسسة نتيجة عطل في أنظمة تكنولوجيا المعلومات الخاصة بها".

ب. كما تعتبر المخاطر الالكترونية مشكلة تجارية ذات أبعاد تقنية، حيث يؤثر على كل مجالات المؤسسة ويتأثر بها من جانب احتواء المخاطر أو تضخيمها. (حشمان، 2024، صفحة 62)

ج. ويقصد بها أيضا أنها مخاطر تشغيلية على أصول المعلومات والتكنولوجيا التي لها عواقب تؤثر على سرية أو توفر أو سلامة المعلومات أو نظم المعلومات مقارنة بفئات المخاطر التي يغطيها التأمين. فإن المخاطر السيبرانية تتفق من حيث الخصائص والمسؤولية، مع مخاطر كل من الممتلكات والخصوم، وكذلك المخاطر الكارثية والتشغيلية. (البغدادي، 2021، صفحة 146)

2. أثر المخاطر السيبرانية على المؤسسات المالية

تتعرض المؤسسات المالية للمخاطر السيبرانية بشكل خاص بسبب اعتمادها الكبير على البنية التحتية الحرجة، تعتبر هذه البنية نقطة فشل واحدة، حيث أن أي هجوم ناجح قد يترتب عليه عواقب واسعة النطاق. فإذا تعطلت البنية الأساسية للأسواق المالية أو مجموعة من المؤسسات الكبرى، فإن تأثير ذلك سيكون كبيراً بسبب تركيز المخاطر ونقص البدائل.

وسنقدم بعض الأمثلة حول مؤسسات مالية تعرضت لمخاطر جعلتها تفقد جزء من مصداقيتها وثقتها:

أ. الشركات التجارية (ارامكو)

تمثل الهجمات الالكترونية مشكلة كبيرة للشركات حيث أفاد البنتاغون أنهم يتلقون حوالي 10 ملايين هجوم الكتروني يوميا، تعد شركة أرامكو السعودية واحدة من شركات الطاقة التي تأثرت بالهجمات الالكترونية. ففي عام 2012 اعرضت أرامكو لهجمات الكترونية من فيروس خبيث يسمى شمعون وقد قامت شركة الطاقة بمعالجة الوضع وحل المشكلة بعد الضرر.

كان يوم 15 أغسطس 2012 هو اليوم الأكثر تضررا من هجمات شركة أرامكو حيث وقعت الهجمات على الساعة 11:08 صباحا، دمر الفيروس وعطل أكثر من 30 ألف جهاز حاسوب و2000 خادم صمم هذا الفيروس خصيصا للتجسس الالكتروني في قطاع الطاقة كانت الشركة محظوظة لأن يوم الهجوم صادف عطلة رسمية، وكان العديد من موظفيها في إجازة وكانت أجهزة الكمبيوتر الخاصة بيهم معطلة وإلا كان الضرر أكبر وكان تأثيره أقل فعالية. (alsaeed, 2021, p. 25 26)

و في عام 2021 تعرضت الشركة ذاتها لهجوم سيبراني اخر حيث تم تسريب البيانات الخاصة بالشركة و الموظفين و العملاء و كشوف المرتبات ومواقع مصافي النقل على يد احد المتعاقدين و تم طلب فدية 50 مليون دولار من العملات المشفرة مقابل حذف البيانات المسربة مما دفع شركة أرامكو الى توقيع اتفاقية لتعزيز الأمن السيبراني مع شركة إلكترونيات المتقدمة التابعة للشركة السعودية للصناعة العسكرية ، لاستخدام تقنية (صمام البيانات) المصممة و المصنعة داخل المملكة لتفادي تأثيرات الهجمات السيبرانية المتكررة على سمعة الشركة واستعادة ثقة العملاء و الموردين و الشركاء التجاريين. (الخفاجي، 2024، صفحة 39)

ب. البنوك المركزية:

كما تعرضت البنوك المركزية في الاقتصادات الناشئة والمتقدمة لمجموعة من الهجمات السيبرانية. ففي الاقتصادات المتقدمة كانت الهجمات إما خروقات للبيانات (الولايات المتحدة الامريكية وإيطاليا) أو تعطيل للأعمال (النرويج

والسويد)، بينما الاقتصادات الناشئة كانت معظم الهجمات مرتبطة بالاحتيال مما أسفر على خسائر بلغت 117 مليون دولار أمريكي ومن خلال الجدول التالي سوف نبرز الهجمات السيبرانية الأخير على البنوك المركزية. (Bouveret, 2018, p. 8)

الجدول رقم (01): أبرز الهجمات السيبرانية على البنوك المركزية

المؤسسات	التاريخ	نوع الهجوم	تفاصيل
الاحتياطي الفيدرالي بنك كليفلاند	2010	خرق البيانات	سرقة 122 ألف بطاقة ائتمانية
الاحتياطي الفيدرالي نيويورك	2012	خرق البيانات	سرقة أكواد برمجية خاصة بقيمة 9.5 مليون دولار أمريكي.
البنك المركزي السويدي	2012	عمل خلل	أدى هجوم رفض الخدمة الموزع (ddos)الى ترك المواقع الالكترونية غير متصلة لمدة 5ساعات.
بنك سنترال ديل الاكوادور	2013	احتيال	سرقة 13.3 مليون دولار من حساب مدينة ريوبامبافي البنك المركزي
الاحتياطي الفيدرالي بنك سانت لويس	2013	خرق البيانات	نشر أوراق اعتماد 4000 من المسؤولين التنفيذيين في البنوك الأمريكية (مجهول)
البنك المركزي سوازيلاند	2014	احتيال	سرقت 688 ألف دولار أمريكي
البنك المركزي الأوروبي	2014	خرق البيانات	20 ألف عنوان بريد إلكتروني ومعلومات اتصال معرضة للخطر
بنك النرويج	2014	عمل خلل	هجوم ddos على سبع مؤسسات مالية كبيرة، مما أدى الى تعليق الخدمات خلال يوم واحد
البنك المركزي أذربيجان	2015	خرق البيانات	سرقة بيانات ألاف العملاء المصرفيين
بنك بنجلاديش	2016	احتيال	تم اعتماد بيانات swiftللبنك المركزي في بنجلادش تستخدم لتحويل 81 مليون دولار أمريكي من حسابها في البنك الاحتياطي الفيدرالي في نيويورك. محاولات القرصنة سرقة 951مليون دولار امريكي.
بنك روسيا	2016	احتيال	21 هجوم الكتروني بهدف سرقة 50 مليون دولار أمريكي من حساب البنوك المراسلة في البنك المركزي مما أدي إلى خسارة قدرها22 مليون دولار أمريكي
بنك إيطاليا	2017	خرق البيانات	اختراق حسابات البريد الإلكتروني لإثنين من المسؤولين التنفيذيين السابقين.

المصدر: من اعداد الطالبتين اعتمادا على (Bouveret, 2018, p. 9)

المطلب الثاني: استراتيجيات مواجهة المخاطر وآثار التهديدات على الاستقرار المالي

تتبلور جملة من الاستراتيجيات والآليات الفاعلة لمعالجة التهديدات السيبرانية، بهدف تعزيز الصمود المالي والتخفيف من الآثار السلبية الناشئة عن الحوادث الإلكترونية، مما يُسهم في تحقيق التوازن المالي ورفع درجة المرونة النظامية في القطاعات المالية والاقتصادية.

الفرع الأول: استراتيجيات إدارة مخاطر الأمن السيبراني

هددت التهديدات السيبرانية النظام المالي بشكل حاد على مر السنين. ولهذا السبب، فإن دمج نهج شامل على مستوى المؤسسة للمرونة السيبرانية أمر بالغ الأهمية للمؤسسات المالية. (lyons, 2024)

1. استخدام تقنيات الخداع بجذب وتحليل المهاجمين السيبرانيين في بيئة آمنة مما يسمح بجمع المعلومات حول أساليبهم، وتشمل عادة على نظام اشعار لتسجيل نشاط المهاجم.

2. تعطيل سلسلة القتل السيبراني المصممة لفهم المراحل المختلفة للهجوم، الاستطلاع، التسلح، التسليم، الاستغلال، التثبيت، القيادة، السيطرة والعمل على الهدف وأخيرا تحقيق الربح.

3. تبني إطار عمل للمرونة السيبرانية لتوجيه أنشطة إدارة المخاطر وتحسين الاستعداد التام.

4. تنفيذ برامج مكافأة اكتشاف الثغرات لتحفيز القراصنة الأخلاقيين على تحديد والإبلاغ عن الثغرات في أنظمة البرمجيات.

الفرع الثاني: تأثير التهديدات السيبرانية على القطاع المالي

برزت الحوادث الإلكترونية كأحد أبرز التحديات التي تواجه المنظومة المالية العالمية، فأمام الاعتماد المتزايد على الحلول الرقمية في القطاع المالي تعددت الثغرات الأمنية التي قد تستهدفها الجماعات الإجرامية لتعريض الاستقرار المالي للخطر. ومن خلال هذا المطلب سنوضح تأثير الحوادث على المؤسسات: (sontheim, 2024)

1. من شأن الحوادث التي يتعرض لها القطاع المالي أن تهدد الاستقرار المالي والاقتصادي، إذا ما أدت إلى تآكل الثقة في النظام المالي أو تعطيل الخدمات الضرورية أو انتقال التداعيات إلى مؤسسة أخرى.

2. يؤدي حادث سيبراني تتعرض له احدى المؤسسات المالية إلى تفويض الثقة وربما تنشأ عنه موجة بيع عارمة في الأسواق أو سحب جماعي للودائع المصرفية في الحالات القصوى.

3. يمكن أن تؤثر الحوادث الالكترونية إلى تعطيل نظام المدفوعات وبالتالي توقف المعاملات في البنوك المحلية.

4. نظرا لقوة الروابط المالية والتكنولوجية المتبادلة، فإن أي هجمة ناجحة على مؤسسة مالية كبرى يمكن أن تنتشر تداعياتها سريعا في النظام المالي مما يؤدي إلى اضطراب واسع الانتشار يتسبب في العديد من الأزمات كأن يطالب المستثمرون والمودعون بأموالهم ويحاولون الغاء حساباتهم. (Jenkinson, 2020)

5. فقدان الثقة:

إذا أدى هجوم واسع النطاق إلى شلل العمليات الحيوية لفترة طويلة، فقد يؤدي في النهاية إلى فقدان ثقة العملاء والمشاركين في السوق بالنظام المالي مما يجعلهم يترددون في تقديم السيولة أو الائتمان مما يتسبب في مزيد من الضرر. قد تؤدي الهجمات وانقطاعات الخدمة التي تؤثر على شركة واحدة الى استنتاج أن الشركات الأخرى معرضة للخطر على نحو مماثل. مثل ما حدث في نيوزلندا سنة 2020 حيث تم تعطيل بورصة الأوراق المالية بسبب سلسلة من الهجمات لإلكترونية إلى فقدان الثقة، وظل نظام التداول يعمل من الناحية الفنية ولكن كان لابد من إيقاف التداول بسبب المخاوف بشأن نزاهة السوق. (elliote, 2020, p. 10)

6. الاعتماد الكبير على البيانات:

يجعل أي تأثير على سرية البيانات أو سلامتها أو توفرها عرضة لعواقب واسعة النطاق في النظام، على سبيل المثال قد يؤدي عدم توفر أسعار التداول أو التلاعب بها إلى توقف السوق عن العمل. (luque, 2021, p. 191)

7. عدم القدرة على الاستبدال:

في العديد من الأنظمة المالية قد تقدم مؤسسة أو اثنتان كبيرتان خدمات حيوية مثل خدمات الحفظ أو المقاصة، قد تشكل المؤسسات الكبيرة التي تهيمن على أسواق ما بين البنوك أو المؤسسات التي تقدم خدمات متخصصة والبنوك المراسلة في الاقتصادات النامية مخاطر تتعلق بقابلية الاستبدال. على سبيل المثال قد يؤدي انقطاع في أنظمة البنية التحتية الرئيسية للأسواق المالية، مثل أنظمة الدفع إلى تعطيل معالجة المعاملات مع تأثير متسلسل على مستوى النظام. (elliote, 2020, p. 11)

8. درجة عالية من الترابط:

يمكن أن تأتي التبعيات بين مكونات النظام المختلفة على سبيل المثال بين المؤسسات المالية والبنية التحتية للسوق، ولكن أيضا بين مكونات النظام ومكونات من خارج النظام على سبيل المثال مزودي خدمات البرمجيات أو الاتصالات. إن الحادث الالكتروني في مكون معين قد ينتشر إلى مكونات أخرى تعتمد عليه بغض النظر عما إذا كانت جزءا من النظام المالي أم لا. (luque, 2021, p. 191)

– يمكن أن تؤثر الهجمات الالكترونية على الشركات من خلال الجوانب الرئيسية الثلاث لأمن المعلومات: (Bouveret, 2018, p. 4)

أ. السرية:

تنشأ مشكلات السرية عند الكشف عن معلومات خاصة داخل الشركة لأطراف ثالثة، كما هو الحال في خروقات البيانات.

ب. النزاهة:

تتعلق مشكلات النزاهة بإساءة استخدام الأنظمة كما هو الحال في الاحتيال.

ج. التوافر:

ترتبط مشكلات التوافر بانقطاعات الأعمال. وللأنواع الثلاثة من الهجمات الإلكترونية تأثيرات مباشرة مختلفة على الجهات المستهدفة، فاضطرابات الأعمال تمنع الشركات من العمل مما يؤدي إلى خسارة في الإيرادات ويؤدي الاحتيال إلى خسائر مالية مباشرة بينما تستغرق آثار اختراقات البيانات وقتا أطول لتظهر من خلال الآثار التي تلحق بالسمعة بالإضافة إلى تكاليف التقاضي.

المطلب الثالث: دور الأمن السيبراني في الحفاظ على الاستقرار المالي

يعتبر الأمن السيبراني موقعا استراتيجيا في الحفاظ على الاستقرار المالي، حيث يشكل منظومة دفاعية متكاملة لمواجهة المخاطر السيبرانية التي تهدد سلامة البنية التحتية المالية، كما يضمن استدامة العمليات المالية وثبات تقديم الخدمات المصرفية والمالية في بيئة تتسم بدرجة عالية من الاعتماد الرقمي.

الفرع الأول: استراتيجيات تعزيز الأمن السيبراني العالمي

التهديدات السيبرانية تجاوزت الحدود الجغرافية مما يستدعي تضافر جهود الدول والمؤسسات المالية لمواجهتها، وفيما يلي سنسلط الضوء على ست استراتيجيات من شأنها أن تساعد على تحسين بيئة الأمن السيبراني العالمية وهي كالتالي: (jain, 2023, p. 4)

1. يجب فهم الترابطات بين مكونات النظام المالي العالمي بشكل أفضل من خلال تحديد الترابطات التشغيلية والتكنولوجية الرئيسية، بما في ذلك الترابطات المتعلقة بالبنية التحتية الحيوية. إن دمج المخاطر السيبرانية بشكل أفضل في تحليل الاستقرار المالي سيحسن القدرة على فهم المخاطر على مستوى النظام والتخفيف من حدتها.

2. ينبغي وضع إطار عمل مشترك للأمن السيبراني يحدد أفضل الممارسات والمعايير التي ينبغي على المؤسسات المالية اتباعها. وهذا من شأنه أن يساعد على ضمان اتخاذ جميع المؤسسات للتدابير اللازمة لحماية نفسها من التهديدات السيبرانية.

3. في حدود ما تسمح به القوانين المحلية يمكن للدول تبادل المعلومات والاستخبارات حول التهديدات والهجمات الإلكترونية، وهذا من شأنه أن يساعد في تحديد التهديدات ونقاط الضعف الناشئة ويمكن المؤسسات المالية من اتخاذ تدابير استباقية لمنع الهجمات.

ويمكن توضيح استراتيجيات أخرى: (chiu, 2021, p. 14 16)

4. مساهمة الحكومات في نشر سياسات وارشادات حول الأمن السيبراني بانتظام واستقطاب الكفاءات في هذا المجال والمشاركة في منظمات عالمية وإقليمية لتعزيز تبادل المعلومات.

5. تعزيز الوعي بالمرونة السيبرانية بين الأفراد والمؤسسات.

6. تطوير القوى العاملة السيبرانية المستقبلية وتحفيز الشركات القادمة هذه السياسة منتهجة من طرف الولايات المتحدة.

الفرع الثاني: مزايا الأمن السيبراني في القطاع المالي

يساهم الأمن السيبراني في الحفاظ على استمرارية الخدمات المالية ويدعم التطور التكنولوجي والابتكار، ما يجعل المؤسسات المالية أكثر تنافسية ومرونة في عصر الرقمنة. كما أنه يقدم عدة فوائد نذكر منها:(عبده، 2024)

1. حماية المعلومات الحساسة للحفاظ على سرية وسلامة المعلومات.

2. ضمان استمرارية الخدمات بتقديم ضمانات تكنولوجية وإدارية لضمان قدرة الأنظمة والتطبيقات المالية على العمل بسلاسة ودون انقطاع.

3. الامتثال للتشريعات أي التقيد باللوائح والقوانين المحلية والدولية المتعلقة بأمن المعلومات لحماية البيانات والمعلومات المالية.

4. تعزيز الابتكار حيث يساهم الامن السيبراني في تطوير تقنيات دفع آمنة وتقديم خدمات مالية رقمية وتحسين تجربة المستخدم، يمكن للقطاع المالي أن يحقق توازنا بين التقدم التكنولوجي وضمان الأمان والثقة في الخدمات المالية المقدمة.

5. مخاطر تتعلق بقابلية الاستبدال. على سبيل المثال قد يؤدي انقطاع في أنظمة البنية التحتية الرئيسية للأسواق المالية، مثل أنظمة الدفع إلى تعطيل معالجة المعاملات مع تأثير متسلسل على مستوى النظام. (elliote, 2020, p. 11)

خلاصة الفصل:

قد تطرقنا في هذا الفصل إلى تقديم مفهوم الاستقرار المالي وأهم الأهداف التي يسعى إليها ومختلف خصائصه التي يتميز بها، كما تعرفنا على أسسه التي يرتكز عليها وتمثلت في الثقة وتجنب الاضطرابات وغيرها، وأيضا تناولنا محدداته والتي تنقسم بدورها إلى الشروط الرقابية والقانونية وشروط السوق والبنية التحتية وكذلك ذكرنا أهم مظاهره وأسباب عدم الاستقرار المالي والتي قمنا بتلخيصها في مجموعتين رئيسيتين العوامل الداخلية والخارجية وأيضا تطرقنا لفرضية منسكي، كما ذكرنا أهم إجراءات الحفاظ على الاستقرار المالي والتي قسمناها إلى اجراءات وقائية وأخرى تصحيحية وكذلك قمنا بتوضيح المخاطر التي قسمناها إلى مخاطر داخلية وخارجية ونظامية ومتطلبات تحقيقه التي تمثلت في توفر قطاع مالي كفأ وتوفر استقرار نقدي ،كما قدمنا لمحة عن أهم التحديات التي تعرقل تحقيق الاستقرار المالي والجهود المبذولة لمواجهتها وأيضا أهم مؤشراته وفي الأخير تطرقنا إلى دراسة العلاقة بين الأمن السيبراني والاستقرار المالي.

الفصل الثالث:

الإطار التطبيقي للدراسة

تمهيد الفصل:

بعد الإحاطة بمختلف جوانب موضوع الدراسة من الناحية النظرية وباعتبار أن أي دراسة نظرية يجب أن تعقبها دراسة تطبيقية لمحاولة إسقاط أو معرفة مدى التطبيق في الواقع العملي. تم اختيار شركة **"target"** كدراسة حالة، نظرا لموقعها البارز في القطاع التجاري العالمي حيث تعد من بين أكبر متاجر التجزئة في الولايات المتحدة الأمريكية من حيث القيمة السوقية والحجم التشغيلي. تعتمد الشركة بشكل مكثف على التحول الرقمي وتقنيات الذكاء الاصطناعي مما يجعلها عرضة لمخاطر أمن المعلومات السيبرانية مثل انتهاكات البيانات أو الاختراقات الإلكترونية مما أثر سلبا على سمعتها المالية والتجارية وأدى إلى خسائر فادحة تقدر بمئات الملايين من الدولارات. من هنا تكتسب دراسة هذه الحالة أهمية خاصة في تحليل فجوة الممارسات الأمنية بين الجانب النظري والتطبيقي وكيفية تأثير هذه الثغرات على ثقة العملاء واستقرار العلامة التجارية في بيئة الأعمال الرقمية سريعة التطور.

المبحث الأول: تقديم شركة Target corporation

تعد شركة تارجت الأمريكية من أبرز الشركات التجارية العالمية في قطاع التجزئة، حيث تميزت بجمعها بين عناصر الجودة العالية والأسعار التنافسية. وقد استطاعت أن تبرز هويتها المتفردة في سوق تجزئة تنافسي محققة تميزا واضحا بين الشركات الأخرة مثل وول مارت وأمازون.

المطلب الأول: مفهوم شركة Target corporation

سنقوم بتقسيم عناصر هذا المطلب إلى فرعين، في الفرع الأول سنقوم بتعريف الشركة ونشأتها، وفي الفرع الثاني سوف نتعرف على الهيكل التنظيمي للمؤسسة.

الفرع الأول: التعريف بالشركة ونشأتها وخدماتها

1. التعريف بشركة Target

شركة تارجت هي شركة تجزئة للبضائع العامة عبر متاجرها التقليدية ومنصاتها الرقمية الأخرى تشمل هذه المنتجات تشكيلة واسعة من البضائع العامة والأغذية. (Pan, 2022, p. 167)

2. نشأة شركة Target

تعتبر شركة تارجت **(Tgt)** اليوم ثاني أكبر متاجر التجزئة للتخفيضات في الولايات المتحدة الأمريكية. أسسها جورج دايتون عام 1902 في مينيا بوليس، مينيسوتا، تحت اسم **(good fellow dry goods)** ثم عدل اسمها عدة مرات لتصبح **(target corporation)** عام 2000، تأسس أول متجر تارجت للخصومات عام 1962 كشركة تابعة لشركة **(dry goods)**. وقد اختير اسم تارجت لتمييز متاجر الخصومات عن المتاجر الكبرى. اعتبارا من 2015 تدير شركة تارجت أكثر من 1790 متجرا في جميع أنحاء الولايات المتحدة، ويعمل بها ما يقارب من 347 ألف موظف بدوام كامل وجزئي. في يناير 2011 بدأت تارجت بالتوسع دوليا في كندا من خلال شراء عقود إيجار ل 220 متجرا من سلسلة متاجر التجزئة الكندية **(zillers)**، إلا أن خطة التوسع إلى كندا لم تكتب لها النجاح بسبب عدة مشاكل منها مشاكل في سلسلة التوريد ونتيجة لذلك تكبدت الشركة خسائر صافية من المتجر الكندي منذ ذلك الحين حتى أغلقت جميع متاجرها في كندا بحلول أبريل 2015. (ebrahim, 2016, p. 29)

والجدول الموالي يوضح عدد المتاجر لشركة تارجت وأعضاء الفريق:

الجدول رقم (02): اجمالي عدد متاجر تارجت خلال الفترة (2020–2024)

السنوات	2020	2021	2022	2023	2024
متاجر الو.م.أ	1897	1926	1948	1956	1978
أعضاء الفريق	409000	450000	440000	415000	440000

المصدر: من اعداد الطالبتين اعتمادا على (corporate, s.d.)

3.الخدمات التي تقدمها شركة Target

تقدم الشركة مجموعة من الخدمات لعملائها والتي سنبرزها كما يلي:(corporate, s.d.)

أ. التسوق من تطبيق **ios**و **android** الحائز على جوائز لنظامي التشغيل في أي مكان وفي أي وقت.

ب. الطلب عبر تطبيق **drive up** والقيادة إلى مواقف السيارات الخاصة بالشركة للتوصيل داخل السيارة.

ج. استخدام الواقع المعزز لمعرفة مدى ملائمة منتج كبير مثل الأريكة لمنزلك باستخدام تطبيق **see it in your space**.

د. استخدام بطاقة **wallet** للدفع والتوفير باستخدام القسائم في مسح ضوئي واحد **target circle**.

الفرع الثاني: التنظيم الإداري لشركة تارجت

على الرغم من حجمها الضخم تدار شركة تارجت بواسطة فريق قيادي صغير نسبيا، يتولى رئاسة مجلس الإدارة الرئيس التنفيذي ويدعمه عدد من نواب الرئيس التنفيذيين الذين يشرفون على العمليات ويتحملون مسؤولية مجموعة مختارة من المجالات داخل الشركة. ويوضح الشكل العام لهيكل الشركة كما يلي:(organimi, s.d.)

1. فريق القيادة التنفيذية: يتألف من كبار المسؤولين التنفيذيين الذين يشرفون على التوجه الاستراتيجي العام للشركة واتخاذ القرارات اللازمة، يضم هذا الفريق الرئيس التنفيذي ونائبي الرئيس التنفيذيين بالإضافة إلى مناصب إدارية عليا، مثل المدير المالي والمدير التنفيذي للتسويق، والمدير التنفيذي للموارد البشرية، وغيرهم من كبار المسؤولين التنفيذيين وهم يوفرون القيادة والتوجيه للأقسام والوظائف.

2. الوظائف: هناك أقسام وظيفية تقدم الدعم والخبرة في جميع أنحاء المؤسسة تشمل الأقسام المالية، والتسويق، والموارد البشرية، وتكنولوجيا المعلومات، وسلسلة التوريد، وعمليات المتاجر، وغيرها. يرأس كل قسم رئيس قسم يشرف على عمليات القسم ويقدم تقاريره إلى فريق القيادة التنفيذية.

3. الأقسام: تعمل تارجت من خلال أقسام مختلفة كل منها مسؤول عن خط أعمال أو فئة منتجات محددة، من أمثلة الأقسام لدينا الملابس والإكسسوار، مستحضرات التجميل والعناية بالصحة، والأدوات المنزلية، الالكترونيات وغيرها، يرأس كل قسم قائد يشرف على عملياته وأدائه.

المطلب الثاني: تحليل الأداء المالي خلال الفترة (2022–2024)

تتم عملية تحليل الأداء المالي لشركة **Target** بالاعتماد على مجموعة من الإحصائيات الفعلية التي تعكس نشاط الشركة خلال السنوات الثلاث الماضية، الممتدة من عام 2022 وحتى عام 2024. ويستخدم في هذا التحليل منهج الأرقام القياسية بهدف دراسة التغيرات النسبية في بيانات الشركة، مما يتيح فهما أدق لأهم التطورات التي شهدتها خلال هذه الفترة.

الفرع الأول: تحليل الأداء وفق تطور إيرادات الشركة

تعتبر الإيرادات من أبرز المؤشرات المالية التي تعكس درجة الاستقرار المالي للمؤسسة وتعبر عن كفاءتها في توليد العوائد من أنشطتها التشغيلية. ويعد تحليل تطورها خلال الفترة 2022–2024 أداة أساسية لتقييم الأداء المالي العام وقياس مدى فعالية السياسات والاستراتيجيات المتبعة. ويوضح الجدول التالي مسار تطور إيرادات شركة Target خلال هذه الفترة.

جدول رقم (03): تطور إيرادات شركة Target للفترة(2022–2024)

الوحدة: مليون دولار

السنوات	2022	2023	2024
الإيرادات	109,120	107,412	106,566
الأرقام القياسية	%103	%98.43	%99.21

المصدر: من اعداد الطالبتين بالاعتماد على التقرير السنوي 2024،2023،2022.

شهدت إيرادات شركة **Target** نموا ملحوظا خلال عام 2022، حيث ارتفعت لتسجل ما يعادل 103% مقارنة بسنة الأساس، مما يعكس أداء قويا في تلك الفترة. إلا أن هذا الاتجاه التصاعدي لم يستمر، إذ تراجعت الإيرادات في عام 2023 إلى 98.43%، مما يشير إلى انخفاض في الأداء العام للشركة. وفي عام 2024، بدأت الإيرادات بالتحسن النسبي، لتصل إلى 99.21%. وعلى الرغم من هذا التحسن، فإن الإيرادات لا تزال دون مستوى سنة الأساس (2022)، مما يدل على أن الشركة لم تستعد بعد كامل أدائها المالي السابق.

الفرع الثاني: تحليل الأداء وفق تطور مبيعات الشركة

تعد المبيعات من المؤشرات المالية الأساسية التي تعبر عن النشاط التشغيلي للشركة، إذ يسهم تطورها في تقييم الكفاءة السوقية واتجاهات الطلب على منتجات الشركة. ويعرض الجدول التالي تطور مبيعات شركة Target خلال الفترة 2022–2024.

جدول رقم (04): تطور مبيعات شركة Target (2022–2024)

الوحدة: مليون دولار

السنوات	2022	2023	2024
المبيعات	107,588	105,803	104,820
الأرقام القياسية	%103	%98.34	%97.23

المصدر: من اعداد الطالبتين بالاعتماد على التقرير السنوي 2024،2023،2022

شهدت الشركة ارتفاعا ملحوظا في مبيعاتها خلال عام 2022، حيث بلغت ذروتها مسجلةً نسبة 103%، مما يعكس أداء إيجابيا في ذلك العام. إلا أن هذا الأداء لم يستمر، حيث دخلت الشركة في مرحلة تراجع تدريجي في المبيعات خلال عامي 2023 و2024. ورغم أن الانخفاض المسجل لم يكن حادا من حيث النسبة، إلا أن استمراريته تشير إلى تحدي للشركة.

الفرع الثالث: تحليل الأداء وفق تطور أرباح الشركة

تعتبر صافي الأرباح أحد المقاييس المالية التي يعتمد عليها في تحليل وتقييم أداء الشركة، والجدول التالي يوضح تطور الأرباح لشركة **Target** خلال الفترة 2022-2024.

جدول رقم (05): تطور أرباح شركة Target (2022–2024)

الوحدة: مليون دولار

السنوات	2022	2023	2024
صافي الأرباح	2,780	4,138	4,091
الأرقام القياسية	%40.02	%149	%99

المصدر: من اعداد الطالبتين بالاعتماد على التقرير السنوي 2024،2023،2022

شهد صافي الأرباح الشركة خلال الفترة من 2022 إلى 2024 تذبذبا ملحوظا في أدائها المالي. ففي عام 2022، سجل صافي الأرباح تراجعا حادا بلغ 40.02% ما يعكس ضعفا في الكفاءة المالية خلال تلك السنة. إلا أن الشركة تمكنت في عام 2023 من تحقيق انتعاش، حيث ارتفعت الأرباح إلى 149%، متجاوزة بذلك صافي

الأرباح عام 2022 بفارق كبير، وهو ما يشير إلى تحسن كبير في الأداء المالي. وفي عام 2024، استقرت الأرباح عند مستوى قريب من سنة 2023، حيث بلغت 99%، مع تسجيل انخفاض طفيف مقارنة بعام 2023.

المطلب الثالث: استراتيجيات الشركة ومعوقاتها

في ظل البيئة التجارية شديدة التنافسية والتي تتسم بالتغير المستمر، تسعى شركة تارجت إلى تعزيز موقعها التنافسي من خلال تبني استراتيجيات نمو مدروسة قائمة على أسس علمية. وعلى الرغم من مواجهتها لتحديات هيكلية وعملية تعيق مسيرة نموها، إلا أن الشركة قد استطاعت التغلب عليها بنجاح.

الفرع الأول: الاستراتيجيات التي تتبعها تارجت للنمو

اتبعت الشركة مجموعة من الاستراتيجيات الأساسية لتعزيز مكانتها في السوق ودفع نمو الإيرادات والربحية تمثلت فيما يلي: (ebrahim, 2016, p. 32)

1. تقديم عن منافسيها منتجات عالية الجودة وعصرية بهامش ربح منخفض.

2. التعامل مع العملاء على أنهم ضيوفا من أجل إظهار أولوية قصوى لهم وإظهار الالتزام بإقامة علاقة مفيدة معهم.

3. التركيز على تصميم المتاجر لضمان تجربة تسوق ممتعة وجذابة من خلال التركيز على جوانب معينة كالنظافة والتجهيز الجيد وأجواء تسوق ممتعة ووقت انتظار قصير للدفع.

4. تعتمد تارجت على وظيفتين أساسيتين في بناء هويتها التجارية وهما شراكة التصميم والإعلان الإبداعي.

وتتمثل أيضا الاستراتيجيات في: (corporate, s.d.)

5. تحويل سلسلة التوريد الخاصة لتحسين الكفاءة والسرعة والقدرة والموثوقية عبر شبكتنا.

6. افتتاح متاجر جديدة وتحديث المتاجر الحالية وتعزيز تجربتنا الرقمية للوصول إلى المزيد من المستهلكين وتوفير تجربة تسوق مريحة وسهلة وملهمة بشكل موثوق.

الفرع الثاني: التحديات التي تواجه شركة تارجت

تواجه شركة تارجت العديد من التحديات التي تعرقل نموها وتوازنها سنبرزها في النقاط التالية:(Lino, 2024)

1. منافسة شديدة من تحار التجزئة التقليديين وعمالقة التجارة الالكترونية.

2. التكيف مع تفضيلات المستهلكين وعادات التسوق المتغيرة بسرعة.

3. موازنة عمليات المتجر الفعلي مع نمو المبيعات الرقمية.

4. إدارة اضطرابات سلسلة التوريد وارتفع التكاليف.

5. التعامل مع حالة عدم اليقين الاقتصادي والانخفاضات المحتملة في السوق.

6. الحفاظ على ثقة العملاء وأمن البيانات في ظل المشهد الرقمي المتزايد.

المبحث الثاني: الهجمات السيبرانية التي تعرضت لها الشركة

شهد العقد الأخير تطورا نوعيا في طبيعة الهجمات السيبرانية، حيث اتسمت بدرجة متزايدة من التعقيد والتخصص في استهداف البنى التحتية المعلوماتية الحيوية للكيانات الاقتصادية الكبرى.

المطلب الأول: آلية تنفيذ الهجمة الالكترونية

تتميز الهجمات الإلكترونية المعاصرة باتباعها منهجية متسلسلة تبدأ بمرحلة جمع المعلومات إلى أن يصل المهاجمين إلى مرحلة الاختراق وسرقة البيانات.

الفرع الأول: البرنامج المستعمل في الهجوم السيبراني على الشركة

في السنوات الأخيرة تزايدت بشكل ملحوظ الهجمات السيبرانية التي تركز على الأنظمة الحساسة وباستعمال أحدث التطبيقات والبرامج عالية الدقة، ومن أبرز هذه البرامج الخبيثة **Blackpos** الذي استعمل لسرقة بيانات الشركة:

يعد برنامج **BlackPOS**من البرمجيات الخبيثة التي استخدمت في الهجوم السيبراني الذي استهدف نقاط البيع الخاصة بشركة **Target**، التي تعمل بنظام **Windows** اعتمد البرنامج في انتشاره على استغلال ثغرات أمنية والتسلل ليقوم بعد ذلك بتثبيت نفسه كخدمة **Windows** تعرف باسم **PosWDS**، حيث يقوم **BlackPOS** بالتقاط بيانات بطاقات الائتمان مباشرة أثناء تمريرها عبر أجهزة نقاط البيع، وذلك قبل أن يتم تشفيرها، مما مكّنه من سرقة كميات هائلة من المعلومات المالية الحساسة. (tian, 2023, p. 04)

الفرع الثاني: كيفية تنفيذ الهجمة الالكترونية على الشركة

استغل المهاجمون ضعف تجزئة شبكة شركة**Target** ، حيث أدى الترابط الوثيق بين الأجهزة إلى تسهيل الانتشار داخل الشبكة. بدأ الهجوم من خلال اختراق شركة**Fazio** ، المقاول المتعامل مع**Target** ، عبر رسالة بريد إلكتروني خبيثة تضمنت برنامج**Citadel** ، الذي يُستخدم لسرقة بيانات تسجيل الدخول من متصفح الإنترنت. (terry, 2021, p. 02)

أعلنت شركة **Fazio** التي قدمت خدمات التدفئة والتهوية وتكييف الهواء لشركة تارجت، أنها استخدمت لاختراق نظام الدفع الخاص بالشركة وأفادت التقارير أن جهاز كمبيوتر تابعا لشركة فازيو مصرح له بتقديم معلومات فواتير العقود وإدارة المشاريع إلى تارجت قد تعرض للاختراق من قبل متسللين. (weiss, 2015, p. 03)

لاحقا، استغل المهاجمون ثغرة في تطبيق الويب التابع لـ**Target** ، حيث اكتشفوا ملفًا باسم **xmlrpd.php** يرجح أنه استخدم لتحميل مستندات رسمية مثل الفواتير، ولم تقم الشركة بمنع هذا النوع من التحميل. عن طريق رفع واجهة ويب خبيثة على هيئة ملف شرعي، تمكنوا من تنفيذ أوامر على النظام وتحديد خوادم الشركة التي تحتوي على بيانات حساسة، مثل أرقام بطاقات الائتمان. (ORATO labs, 2014, p. 8)

مع ذلك، لم يعثروا على معلومات بطاقات في البداية بسبب التزام الشركة بمعايير **PCI** التي تمنع تخزين بيانات البطاقات بعد الشراء. لذا، لجأ المهاجمون إلى تثبيت برنامج **Kaptoxa** الخبيث على نحو 40,000 جهاز من أجهزة نقاط البيع، حيث قام بجمع معلومات العملاء أثناء المعاملات وسرّب بيانات بطاقات ائتمان نحو 40 مليون عميل إلى خادم تابع لهم. (terry, 2021, p. 03)

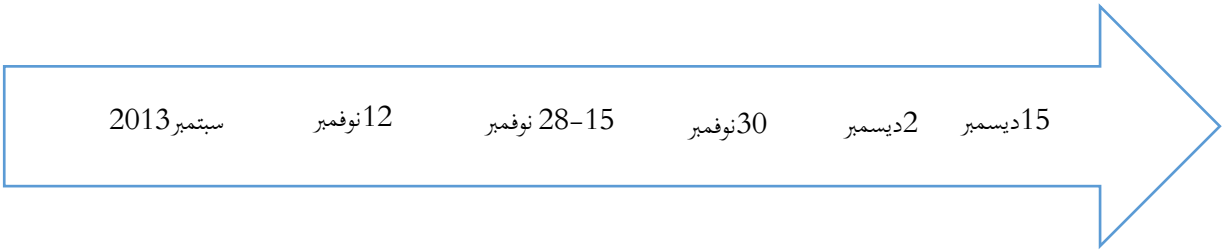
المطلب الثاني: الإطار الزمني وآثار الاختراق على الشركة

يمثل الإطار الزمني لاختراق الشركة حالة دراسية نموذجية للهجمات الإلكترونية المستهدفة طويلة الأمد حيث اتسمت العملية بامتدادها الزمني عبر مراحل متعاقبة ومترابطة. مما خلقت بعض الآثار السلبية التي تهدد استقرار ونمو الشركة.

الفرع الأول: الهيكل الزمني للاختراق

1. أولا، يتم توضيح الخطوات التي اتبعها المهاجمون لسرقة بيانات الشركة:

الشكل رقم (07): خطوات المهاجمين لسرقة البيانات.



المصدر: من إعداد الطالبتين بالاعتماد على (tian, 2023, p. 02)

ومن خلال الشكل الموالي يمكننا تقديم شرح مفصل حول كيفية تنفيذ المهاجمين الاختراق في وقت زمني معين: (بدون كاتب، 2014)

أ. في سبتمبر 2013 تمكن المهاجمون من سرقة بيانات الدخول (أوراق الاعتماد) الخاصة بشركة **FAZIO** للتهوية وهي إحدى الشركات المتعاقدة مع تارجت.

ب. في 12 نوفمبر باستخدام بيانات الدخول المسروقة نجح المهاجمون في اختراق الشركة.

ج. من 15 إلى 28 نوفمبر في متاجر بدأ المهاجمون بتجربة برامج ضارة مصممة لاستهداف أنظمة نقاط البيع.

د. في 30 نوفمبر اكتمل تثبيت البرنامج الضار (**Blackpos**) على أنظمة نقاط البيع.

هـ. في 2 ديسمبر تم تطوير البرامج الضارة لتصبح أكثر تقدما، وبدا المهاجمون في استخدام بيانات بطاقات العملاء بشكل مكثف.

و. في 15 ديسمبر بسبب اكتشاف الخرق وإجراءات أمنية قامت بها الشركة فقد المهاجمون السيطرة على الشبكة.

الشكل رقم (08): رد فعل الشركة على الهجوم.

المصدر: من إعداد الطالبتين بالاعتماد على(tian, 2023, p. 02)

2. في هذا الشكل سنوضح رد فعل الشركة على كل هجمة كان يقوم بها المهاجمين والتي لم تكن كافية لحماية نظامها من الاختراق: (بدون كاتب، 2014)

أ. في سبتمبر 2013 الهدف معتمد ومتوافق مع معيار أمان بيانات صناعة بطاقة الدفع.

ب. في 30 نوفمبر تم تشغيل الإنذارات أول **Fire eye** وقام برنامج **Simantic** بتحديد النشاط الخبيث.

ج. في 2 ديسمبر تم تشغيل المزيد من التنبيهات **Fire eye**.

د. في 15 ديسمبر الهدف يؤكد الاختراق ويزيل البرامج الضارة.

هـ. في 19 ديسمبر أعلنت الشركة علنا عن سرقة 40 مليون بطاقة ائتمان وخصم وأيضا تم سرقة السجلات.

ولتقديم شرح أكثر دقة حول كيفية تنفيذ الهجمة الالكترونية يمكن العودة للملحق رقم (01).

الفرع الثاني: الاثار المترتبة على الاختراق

واجهت شركة **Target** واحدة من أكبر وأخطر حوادث اختراق البيانات، مما خلف تأثيرا واسع النطاق لم يقتصر على الجانب المالي فحسب بل امتد ليشمل سمعة الشركة وثقة العملاء. وفيما يلي نظرة عامة على أهم الآثار التي ترتبت على هذا الاختراق (Sun, 2025, p. 4 5)

1. بلغ صافي النفقات المتعلقة بخرق البيانات في عام 2013 بأكمله 17 مليون دولار، وهو ما يعكس 61 مليون دولار من النفقات الاجمالية التي تم تعويضها جزئيا من خلال الاعتراف بمبلغ 44 مليون دولار مستحقات التأمين.

2. انخفضت الأرباح في عام 2013 بنسبة 46بالمئة مقارنة بالفترة نفسها من العام السابق وذكرت الشركة انها انفقت خلال تلك الفترة 61 مليون دولار على النفقات المتعلقة بالاختراق.

3. توصلت شركة **target** الى اتفاق بقيمة 67 مليون دولار مع **Asiv** بشأن الاختراق الضخم لبيانات الدفع الخاصة بالعملاء والذي شوه سمعتها وأثار تساؤلات خطيرة حول أنظمة امن البيانات الخاصة بالشركة.

وهناك أيضا بعض الآثار الأخرى: (Yanthan, 2024)

4. أثر الاختراق على ولاء العملاء للعلامة التجارية وإيرادات الشركة على المدى الطويل.

5. أدت التحقيقات وتحديثات النظام الى تعطيل العمليات اليومية للشركة.

6. أثار الاختراق اهتمام تنظيما كبيرا مما أدى الى فرض متطلبات امتثال أكثر صرامة على الشركة.

المطلب الثالث: النتائج المالية لشركةTarget بعد التعرض للهجمات 2014-2013

في ظل تصاعد التهديدات السيبرانية في بيئة الأعمال الحديثة، باتت هذه الهجمات تشكل عاملا مؤثرا في استقرار الشركات وأدائها المالي، لا سيما في قطاع التجزئة المعتمد على النظم الرقمية. وتعد شركة **Target** نموذجا واضحا لتأثير الأزمات الأمنية على المؤشرات المالية والتشغيلية. لذا، يعد تحليل نتائجها المالية بين عامي 2012 و2014 ضروريا لتقييم تداعيات تلك الهجمات.

الفرع الأول: تحليل تطور إيرادات الشركة قبل وبعد حدوث الهجمات السيبرانية

الإيرادات من المؤشرات المالية الجوهرية التي تعكس كفاءة الأداء المالي للشركات، وتخضع هذه الإيرادات لتأثيرات متعددة ناتجة عن عوامل داخلية وخارجية. ويبرز الجدول الموالي مسار تطور إيرادات شركة **Target** قبل وبعد حدوث الهجمات السيبرانية.

جدول رقم (06): تطور ايرادات شركة Target للفترة (2012-2014)

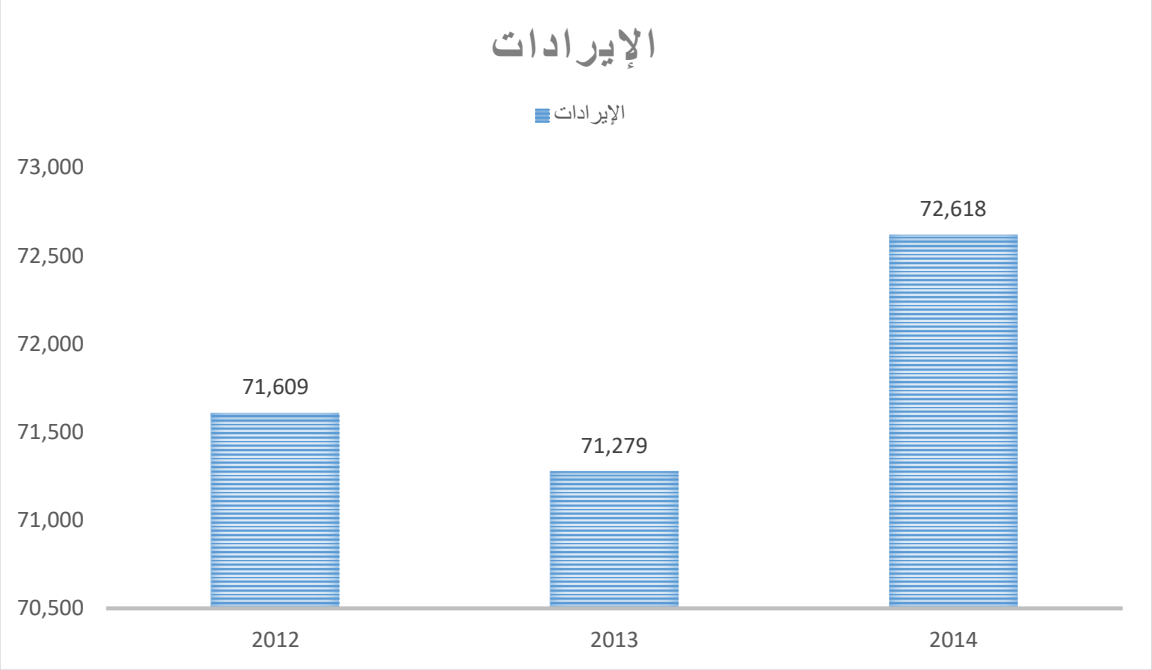
الوحدة: مليار دولار

السنوات	2012	2013	2014
الإيرادات	71, 609	71,279	72,618

المصدر: من اعداد الطالبتين بالاعتماد على التقرير السنوي (2012-2014).

وتعرض بيانات الجدول رقم (**06**) في التمثيل البياني التالي:

الشكل رقم (09): التمثيل البياني لتطور إيرادات شركةTarget للفترة (2012-2014)



المصدر: من اعداد الطالبتين بالاعتماد على الجدول رقم (06)

من خلال تحليل الاعمدة البيانية الخاصة بإيرادات شركة **Target** خلال الفترة الممتدة بين عامي 2012 و2014، يتبين أن الشركة شهدت تغيرات محدودة في أدائها المالي، تعكس في مجملها تفاعلا مع تطورات خارجية، لا سيما في سياق التحديات الأمنية. ففي عام 2012، سجلت Target إيرادات بلغت نحو 71.609 مليار دولار، وهو ما يعكس حالة من الاستقرار النسبي في الطلب على منتجاتها وخدماتها، ويدل على توازن بين الأداء التشغيلي ورضا العملاء في تلك المرحلة، غير أن هذا الاستقرار لم يستمر إذ تراجعت الإيرادات في عام 2013 إلى نحو 71.279 مليار دولار، بانخفاض طفيف نسبته حوالي 0.46% مقارنة بالعام السابق. ويحتمل أن هذا التراجع الطفيف يعكس بوادر ضعف في ثقة العملاء، ربما نتيجة لتسريبات أولية أو مؤشرات غير رسمية سبقت الإعلان العلني عن حادثة الهجوم السيبراني.

أما في عام 2014، وهو العام الذي أعقب الكشف عن الهجمات السيبرانية، شهدت الشركة تحسنا طفيفا في أدائها المالي فقد سجلت الإيرادات ارتفاعا لتصل إلى 72.618 مليار دولار، محققة نموا بنسبة تقدر بنحو 1.88% مقارنة بعام 2013. ويشير هذا التحسن إلى إمكانية حدوث تعاف نسبي في ثقة العملاء، كما قد يعكس أثر الإجراءات التصحيحية التي اتخذتها الشركة للتعامل مع تداعيات الهجوم، سواء من خلال تعزيز البنية التحتية للأمن السيبراني أو عبر تفعيل استراتيجيات فعالة في مجال التسويق واستعادة ثقة السوق. ويأتي هذا التحسن بالرغم من استمرار التحديات التشغيلية والمالية الناتجة عن الهجمات.

الفرع الثاني: تحليل تطور المبيعات الشركة قبل وبعد حدوث الهجمات السيبرانية

تعتبر دراسة المبيعات أداة تحليلية لفهم ديناميكيات السوق وأداء الشركات في بيئات العمل المتغيرة، حيث تمثل الهجمات السيبرانية تهديدا كبيرا قد يؤثر بشكل بالغ على استمرارية العمليات التجارية، مما ينعكس سلبا على ثقة العملاء والمداخيل المالية. في هذا السياق، يعرض الجدول التالي تطور مبيعات شركة **Target** قبل وبعد وقوع الهجمات السيبرانية.

جدول رقم (07): تطور المبيعات شركة Target للفترة (2012–2014)

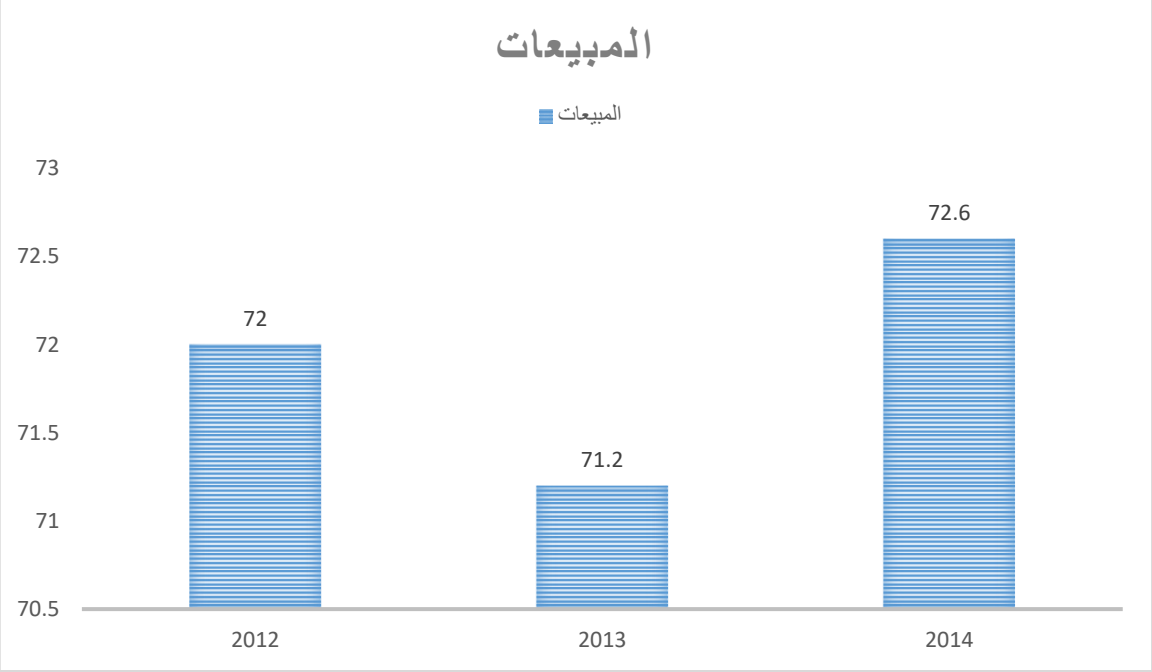
الوحدة: مليار دولار

السنوات	2012	2013	2014
المبيعات	72.0	71.2	72.6

المصدر: من اعداد الطالبتين بالاعتماد على التقرير السنوي 2014،2013،2012.

ونوضح بيانات الجدول رقم (**07**) في الشكل البياني التالي:

الشكل رقم (10): التمثيل البياني لتطور مبيعات شركة Target للفترة (2012-2014)



المصدر: من اعداد الطالبتين بالاعتماد على الجدول رقم (07)

بالاعتماد على تحليل الاعمدة البيانية للفترة الممتدة بين 2012 و2014، اتضح أن شركة**Target** شهدت تقلبات محدودة في أدائها التجاري، وهو ما يمكن ربطه جزئيا بالهجمات السيبرانية التي تعرضت لها في نهاية عام 2013.

ففي عام 2012، بلغت مبيعات الشركة نحو 72.0 مليار دولار، ما يعكس أداء تجاريا مستقرا نسبيا في ظل ظروف سوقية اعتيادية، إلا أن هذا الاستقرار لم يستمر حيث تراجعت المبيعات في عام 2013 بشكل طفيف لتصل إلى نحو 71.2 مليار دولار، مسجلة انخفاضا بنسبة تقارب 1.11% مقارنة بالعام السابق. ويحتمل أن هذا التراجع يعكس تأثر المبيعات سلبا بالاضطرابات الأمنية، ولا سيما تلك المرتبطة بالهجمات السيبرانية، التي ربما بدأت تؤثر على ثقة العملاء وسلوكهم الشرائي حتى قبل الإعلان الرسمي عنها.

واما عام 2014، أظهرت البيانات تحسنا طفيفا في الأداء التجاري للشركة، حيث ارتفعت المبيعات إلى حوالي 72.6 مليار دولار، محققة نموًا بنسبة تقدر بنحو 1.97% مقارنة بعام 2013، ويمكن تفسير هذا النمو بعودة تدريجية في ثقة المستهلكين، بالإضافة إلى فعالية الإجراءات التصحيحية التي يرجح أن الشركة قد اتخذتها للتعامل مع تداعيات الأزمة، سواء من خلال تعزيز البنية التحتية الأمنية أو عبر تنفيذ استراتيجيات استهدفت استعادة صورتها السوقية.

بالتالي، تعكس بيانات المبيعات خلال هذه الفترة حالة من عدم الاستقرار النسبي أعقبتها بوادر تعاف تدريجي، مما يبرز بوضوح حساسية الأداء التجاري للشركة تجاه التهديدات الأمنية، ويؤكد في الوقت ذاته أهمية السياسات التصحيحية والاستباقية في احتواء الأزمات واستعادة وتيرة النمو.

الفرع الثالث: تحليل تطور صافي أرباح الشركة قبل وبعد حدوث الهجمات السيبرانية

صافي الأرباح يعد من المؤشرات المالية الرئيسية التي تعكس أداء الشركة وكفاءتها في تحقيق العوائد بعد خصم كافة التكاليف والمصروفات. تتأثر هذه الأرباح بعدد من العوامل الاقتصادية، بما في ذلك الحوادث الطارئة مثل الهجمات السيبرانية التي قد تؤثر سلبا على سير العمل والأداء المالي، في هذا الإطار يعرض الجدول التالي تطور مبيعات شركة **Target**قبل وبعد وقوع الحادث.

جدول رقم (08): تطور صافي الأرباح لشركة Target للفترة (2012–2014)

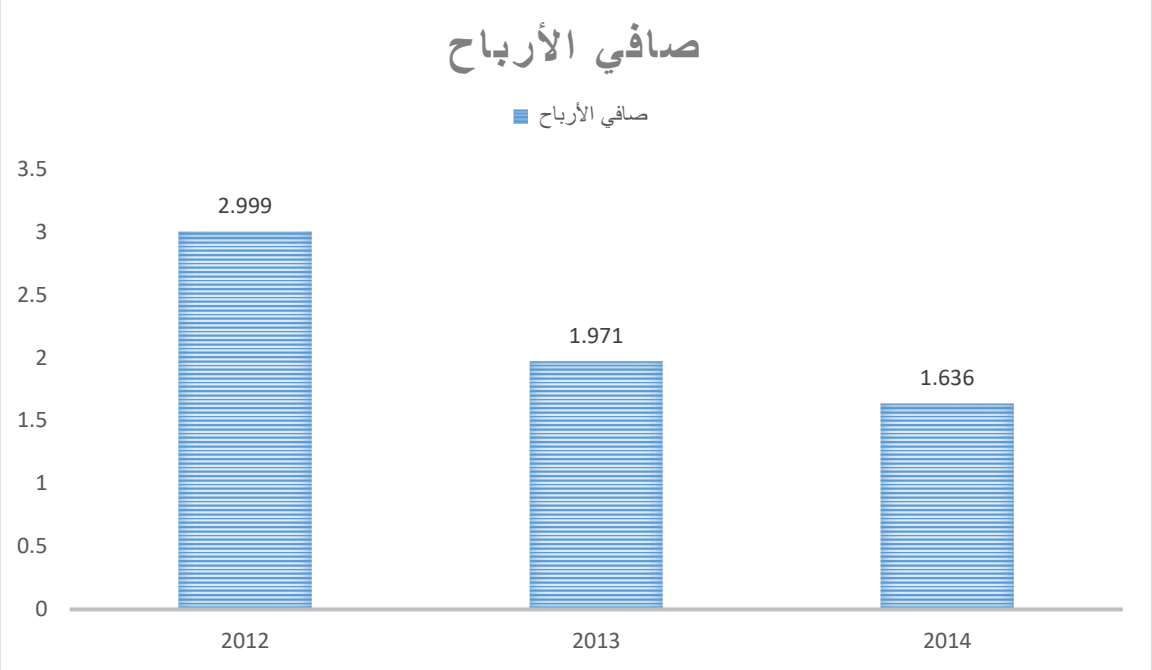
الوحدة: مليار دولار

السنوات	2012	2013	2014
صافي الأرباح	2,999	1,971	1,636

المصدر: من اعداد الطالبتين بالاعتماد على التقرير السنوي 2014،2013،2012.

وفي المنحنى البياني الموالي سيتم توضيح البيانات الواردة في الجدول رقم (08)

الشكل رقم (11): التمثيل البياني لتطور صافي أرباح شركة Target للفترة (2012–2014)



المصدر: من اعداد الطالبتين بالاعتماد على الجدول رقم (08)

استنادا إلى تحليل المؤشرات البيانية للفترة الممتدة بين عامي 2012 و2014، يتضح أن شركة **Target**واجهت تراجعا تدريجيا في صافي أرباحها. ففي عام 2012، سجلت الشركة أداء ماليا قويا حيث بلغ صافي أرباحها ما يقارب 2.999مليار دولار، وهو ما يعد مؤشرا إيجابيا على استقرار الشركة وقدرتها التشغيلية، في ظل غياب تأثيرات سلبية خارجية ذات شأن على نتائجها المالية. غير أن هذا الوضع شهد تحولا جذريا في عام 2013، حيث انخفض صافي الأرباح بشكل حاد ليصل إلى 1.971مليار دولار، ما يمثل تراجعا بنسبة تقدر بحوالي 34.28% مقارنة بالعام السابق. ويعزى هذا الانخفاض الكبير إلى احتمالية تكبد الشركة نفقات إضافية تتعلق بمواجهة تداعيات الهجوم السيبراني، بما في ذلك التكاليف القانونية وتلك الخاصة بتعزيز الإجراءات الأمنية، إلى جانب تراجع ثقة العملاء، وهو ما انعكس سلبا على الأداء المالي العام. وفي عام 2014، استمر هذا الاتجاه التراجعي، حيث تراجع صافي الأرباح إلى 1.636مليار دولار، مسجلا انخفاضا إضافيا نسبته نحو 17.0%مقارنة بعام 2013. ويرتبط هذا التراجع على الأرجح باستمرار التأثيرات السلبية المترتبة على الهجمات السيبرانية، بما في ذلك ارتفاع النفقات المرتبطة بتقوية البنية التحتية الأمنية، والتكاليف القانونية الناتجة عن التسويات المحتملة أو جهود استرجاع بيانات العملاء، فضلًا عن ضعف نسبي في المبيعات وانخفاض الكفاءة التشغيلية.

المبحث الثالث: التحليل الاستراتيجي وإجراءات التعافي

يشكل التحليل الاستراتيجي للهجمات الالكترونية واجراءات التعافي منها اطارا منهجيا حيويا لفهم ديناميكيات الاستجابة للحوادث الامنية.

المطلب الأول: تحليل سووت وبورتر لشركة تارجت

يركز المطلب الحالي على استعراض منهجيتين تحليليتين محوريتين في تقييم الأداء الاستراتيجي تتمثلان في تحليل سووت وتحليل بورتر للقوى الخمس لشركة تارجت في قطاع التجزئة.

الفرع الأول: تحليل سووت لشركة تارجت

يقدم هذا التحليل رؤية متكاملة تجمع بين المحددات الداخلية نقاط الضعف والقوة وبين المتغيرات الخارجية الفرص والتهديدات التي تؤثر على الأداء الاستراتيجي.

1. تعريف سووت (SWOOT):

هو تقنية فعالة لتحليل أبحاث السوق يستخدم عادة لتقييم أداء المنظمة في السوق والمساعدة في تطوير استراتيجيات أعمال فعالة، وتكمن أهميته في دعم التخطيط الاستراتيجي، تحقيق الميزة التنافسية، مواءمة الموارد، تقييم المخاطر، اتخاذ القرارات، وأخيرا تعزيز التواصل والتعاون. وكلمة (**swoot**) هي اختصار يشير إلى:(ragaa, 2025)

-نقاط القوة (**strengths**)

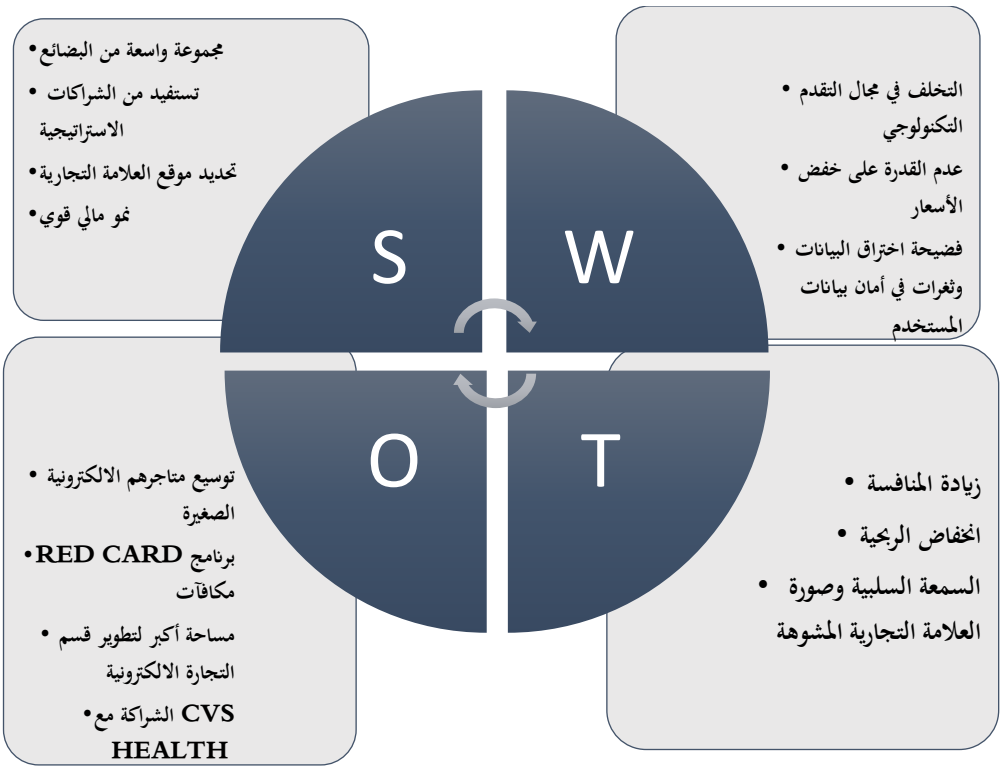
-نقاط الضعف (**weaknesses**)

-الفرص (**opportunities**)

-التهديدات (**threats**)

والشكل الموالي يوضح أهم العوامل الداخلية والخارجية المتكون منها تحليل سووت:

الشكل رقم (12): تحليل سووت لشركة تارجت للتجزئة



المصدر: من اعداد الطالبتين.

2. تحليل سووت لشركة تارجت:

وينقسم إلى مجموعة من العوامل التي تحدد أداء الشركة وهي كما يلي:

أ. نقاط القوة:

يركز هذا التحليل على العناصر الأساسية التي تمنح الشركة تفوقا تنافسيا في سوقها تنقسم كالتالي:

-مجموعة واسعة من البضائع:

لقد رسخت تارجت مكانتها كمتجر شامل يقدم كل شيئ من البضائع المختلفة حتى خلال الجائحة مارس 2020 عندما ازداد الشراء بدافع الهلع اثبتت مجموعة منتجات تارجت المتنوعة قدرتها على التكيف. في حين انخفضت مبيعات السلع الغير الأساسية كالملابس والاكسسوارات، ارتفعت مبيعات السلع الضرورية في المتاجر بنفسها بنسبة 50 يجسد هذا التنوع استراتيجية تارجت التسويقية القوية.(Bhasin, 2025)

-تستفيد من الشراكات الاستراتيجية:

تعتبر من احدى الطرق التي ساعدت الشركة على تحقيق إيرادات مبيعاتها هي توظيف شراكات فعالة مع شركات عملاقة. على سبيل المثال تفاوضت تارجت على صفقة بقيمة 1.9 مليار دولار أمريكي مع صيدلية سي في إس مما يسمح لشركة الأدوية بالاستحواذ على جميع الصيدليات والعيادات الصغيرة التابعة لها في جميع أنحاء البلاد. (Pereira, 2024)

-تحديد موقع العلامة التجارية:

تجمع استراتيجية علامة تارجت التجارية بمهارة بين الجودة والأسعار المعقولة تلبية جميع احتياجات العائلات من ذوي الدخل المتوسط والعالي حيث يبلغ متوسط دخل الأسرة 80.000 دولار أمريكي سنويا وقد مكنها موقعها كمتجر التجزئة المفضل للسلع الضرورية بأسعار معقولة من ترسيخ مكانة فريدة في سوق تنافسية واستقطاب قاعدة عملاء متنوعة مولعة بالأناقة ومخلصة.

-نمو مالي قوي:

النمو الكبير في مبيعات التجارة الالكترونية وايراداتها البالغة 31.9 مليار دولار أمريكي، فالنمو المتتالي في مبيعات الشركة من فبراير 2024 يوضح الأساس المالي القوي ومسار التطور المحتمل.(Bhasin, 2025)

ب. نقاط الضعف:

يبرز تقييم نقاط الضعف في فهم التحديات التي تواجه نمو الشركة واستقرارها تبرز فيما يلي:

-التخلف في مجال التطور التكنولوجي:

تشكل التكنولوجيا أساس الكفاءة التشغيلية ورضا العملاء في قطاع التجزئة الذي يشهد منافسة متزايدة ورغم استثمارات شركة تارجت في توسيع نطاق حضورها التقني إلا أنها لا تزال متأخرة عن منافسيها، حيث يستخدم

منافسو شركة تارجت أحدث التقنيات مثل الذكاء الاصطناعي للخدمات اللوجستية والتحليلات التنبؤية لعادات الشراء لدى العملاء وهو ما يسلط الضوء على الحاجة إلى تسريع نمو تارجت التكنولوجي. (Bhasin, 2025)

–عدم قدرتها على خفض الأسعار:

وذلك من أجل التنافس بكفاءة أكبر مع بعض منافسيها المقربين مثل وول مارت حيث تؤكد الشركة على أهمية توفير منتجات قيمة ذات جودة عالية تمنح العملاء أفضل قيمة مقابل المال. ومع ذلك هذا أيضا يعني فرض أسعار أعلى بشكل عام بما في ذلك منتجات من نفس موردي وول مارت، هذا يحد من المجالات التي يمكن للشركة أن تتوسع فيها. (ajmal, 2019, p. 15)

–ثغرات في بيانات المستخدم:

بعد مواجهة الشركة لفضيحة القرصنة وسرقت بيانات العملاء سارعت إلى اصدار بيان وتحذير العملاء من المخاطر المحتملة، إلا أنها اضطرت إلى دفع تسوية بقيمة 18.5 مليون دولار ومع ذلك لم يكن هذا سوى غيض من فيض إذ أنها لا تزال الشركة تعاني من الضرر الذي لحق بسمعة الشركة مما تسبب في انخفاض الأرباح بنسبة 46 بالمئة لعد الهجوم. (Pereira, 2024)

–فضيحة اختراق البيانات:

تعتمد ثقة العملاء وسمعتهم على إدارة الشركة لبياناتها سرق قراصنة ما يصل إلى 40 مليون بطاقة ائتمان وخصم من متسوقي تارجت خلال موسم أعياد 2013 بعد تحقيق شامل وتسوية، قامت تارجت بتسوية 47 مطالبة من الولايات المتحدة، ألحقت هذه الجريمة ضررا طويل الأمد بعلامة تارجت التجارية ومن الصعب استعادة ثقة العملاء بعد هذه الحادثة مما يبرز نقاط ضعف ممارسات أمن البيانات في تارجت. (Bhasin, 2025)

ج. الفرص:

تبرز الفرص مختلف العوامل الإيجابية التي يمكن للشركة استثمارها لتعزيز موقعها التنافسي.

–توسيع متاجرهم الالكترونية الصغيرة:

من عيوب أسلوب متاجر التجزئة الكبيرة في معظم فروع تارجت ضيق المساحة المتاحة لمثل هذه المتاجر في المراكز الحضرية المكتظة بالسكان كالمدن. ونتيجة لذلك يفتقر المتجر إلى حضور ملحوظ في هذه المناطق ومع ذلك مع افتتاح متاجر صغيرة جديدة يمكن لتارجت التوسع في مراكز المدن الكبرى وتلبية احتياجات قاعدة عملاء أوسع. (Bhasin, 2025)

-برنامج مكافآت (RED CARD):

يعزز ولاء العملاء من خلال الخصومات والمكافآت وأيضا يوفر لتارجت معلومات مهمة حول عادات الشراء لدى عملائها وتفضيلاتهم والتي يمكن استخدامها لتوجيه اختيار المنتجات، واستراتيجيات التسويق، والعروض الترويجية المستهدفة ومن شأن تحسين هذا البرنامج أن يعزز بشكل كبير من استبقاء العملاء واكتسابهم. (Bhasin, 2025)

-مساحة أكبر لتطوير التجارة الالكترونية:

على الرغم من أن المنصة كانت في وقت مبكر من تبني خدمة التجارة الالكترونية المخصصة وشهدت نمو كبير في هذا القسم في عام 2020، لم تتجاوز حصة مبيعاتهم عبر قنوات البيع الالكترونية 20 بالمئة، مما أتاح لهم مجالا كبيرا للنمو وقد سجلت خدمات التوصيل في نفس اليوم نسبة استيفاء 80 بالمئة لذا يعد تحسين هذه الإحصائية بداية ممتازة من خلال تعزيز الاستفادة من خدمة توصيل البقالة في نفس اليوم "شيبت"، بالإضافة إلى إضافة خدمات **Drive app** لمراكز استلام البقالة. (Pereira, 2024)

-الشراكة مع cvs health:

بدأ هذا التحالف في ديسمبر 2015 عندما استحوذت الشركة ما يقارب من 1.9 مليار دولار أمريكي مما مثل فرصة استراتيجية ذ، وقد دمجت هذه الاتفاقية خدمات الرعاية الصحية التي تحمل علامة مما زاد من راحة العملاء من خلال توفير وجهة واحدة لتلبية احتياجات التجزئة والأدوية ويجذب هذا التعاون عملاء جدد ويعزز صورة تارجت التجارية. (Bhasin, 2025)

د. التهديدات:

توضح التهديدات مختلف المخاطر المحتملة التي تعيق مسيرة الشركة ويساهم فهم هذه التهديدات في بناء استراتيجيات قادرة على التخفيف منها.

-زيادة المنافسة:

على الرغم من النمو المطرد لشركة تارجت خلال السنوات القليلة الماضية إلا أنها لا تزال تواجه منافسة شرسة من الشركات القديمة والجديدة في قطاع تجارة التجزئة في المتاجر الكبرى والسوبرماركت. وهذا يزيد من حدة المنافسة عبى حصة السوق في قطاع منخفض الهامش مثل قطاع التجزئة مما يضع الشركة في مواجهة شركات عملاقة مثل وول مارت وأمازون وكوستكو وكروجر وغيرها، وهذا أمر مثير للقلق نظرا لانخفاض عوائق الدخول إلى قطاع الفيديو عبر الانترنت. (Pereira, 2024)

-انخفاض الربحية:

بسبب زيادة المنافسة من طرف الشركات الأخرى مثل أمازون وكوستكو وغيرها ومع ظهور التسوق عبر الانترنت ازداد نمط الشراء لدى المزيد والمزيد من العملاء وأيضا أن شركة تارجت لم تواكب مع الاتجاهات المتغيرة في الاقتصاد قد تجد نفسها تحت ضغط على إيراداتها والربحية. (ajmal, 2019, p. 16)

-السمعة السلبية وصورة العلامة التجارية المشوهة:

لطالما كانت تارجت علامة تجارية رائدة في القضايا الاجتماعية وبالرغم من ذلك لا يظهر هذا صمود المنصة أمام بعض الجدل والانتقادات المحيطة بهذه المواضيع وقد واجهت الشركة نصيبها من الفضائح بما يتعلق ببيانات العملاء، تجربة العملاء، التوجهات السياسية، ولوائح السلامة. (Pereira, 2024)

3. التوصيات الاستراتيجية للشركة:

هناك بعض التوصيات الاستراتيجية لشركة تارجت مبنية على تحليل سووت يمكن اتباعها من أجل تحقيق ما هو أفضل للشركة وتجاوز بعض التحديات التي تعرقل نموها وهي كالتالي: (Lino, 2024)

أ. تعزيز التوجه الرقمي من خلال مواصلة الاستثمار في إمكانيات التجارة الالكترونية ودمج تجارب البيع بالتجزئة الرقمية والتقليدية.

ب. توسيع نطاق المتاجر الصغيرة وذلك بتسريع طرح المتاجر الصغيرة وفي المناطق الحضرية وبالقرب من الحرم الجامعي للاستحواذ على قطاعات سوقية جديدة والتنافس بشكل أكثر فعالية مع متاجر التجزئة وتجار التجزئة عبر الانترنت.

ج. الابتكار في العلامات التجارية الخاصة من خلال تطوير علامات تجارية خاصة جديدة أو توسيع نطاق العلامات التجارية الحالية لتشمل فئات منتجات جديدة.

د. استكشاف شراكات استراتيجية جديدة يمكنها تعزيز القيمة المقترحة للشركة.

هـ. تحسين سلسلة التوريد لتحسين الكفاءة وخفض التكاليف وتعزيز المرونة.

الفرع الثاني: تحليل بورتر لشركة تارجت

يعد نموذج بورتر للقوى الخمس إطارا تحليليا أساسيا، حيث يقدم منهجية نظامية تتفاعل مع بعضها بشكل ديناميكي.

1. تعريف بورتر للقوى الخمس (porters five forces analysis)

هو إطار تحليلي يستخدم لتقييم جاذبية صناعة معينة ومستوى التنافس فيها وهو يعتبر أداة هامة في مجال التخطيط الاستراتيجي واتخاذ القرارات التجارية وتطوير الاستراتيجيات اللازمة للتنافسية والذي يساعد الشركات على فهم بيئة السوق التي يعملون فيها وتحديد الفرص والتحديات التي تواجههم.

ويتكون تحليل بورتر للقوى من خمس عوامل تتمثل فيما يلي: (بكه، 2025)

-قوة التهديد من المنافسين الحاليين **(threat of existing competitors)**

-قوة التهديد من المنافسين الجدد **(threat of new entrants)**

-قوة قدرة المشترين **(power of buyers)**

-قوة قدرة الموردين **(power of suppliers)**

2. تحليل بورتر لشركة تارجت:

يعد نموذج بورتر من بين أكثر الأدوات الاستراتيجية فعالية في تشخيص العوامل المؤثرة على قدرة الشركة في تحقيق الأرباح.

أ. قوة التهديد من المنافسين الحاليين:

تعمل شركة تارجت في بيئة تجزئة شديدة التنافسية، هناك العديد من المنافسين الكبار لها مثل وول مارت، وكوستكو، وكروجر، وهول فودز ماركت مستوى المنافسة مرتفع للغاية مما قد يؤدي إلى انخفاض الأسعار ويهدد ربحية الشركة، ورغم أن تارجت تقدم منتجات عالية الجودة بتكلفة أقل إلا أن تكاليف تغيير العلامة التجارية لا تصنف مرتفعة نظرا للمنافسة الشرسة وهذا العامل يجعل المنافسة تشكل تهديدا كبيرا. (الرحمنوف، 2019، صفحة 02)

ب. قوة التهديد من المنافسين الجدد:

تقدم الشركات الجديدة منتجات وخدمات بتكلفة منخفضة وهو ما يعتبر ميزة تنافسية من منظور اقتصاديات الحجم إذ يمكنها إضعاف منافسيها من حيث السعر وتحقيق أرباح أعلى في الوقت نفسه. إضافة إلى ذلك يتطلب دخول هذه الشركات الجديدة استثمارات مالية ضخمة لمنافسة "تارجت" وغيرها من الشركات المنافسة في هذا القطاع. (looie, 2015, p. 06)

ج. قوة قدرة المشترين:

يقع مشتري شركة تارجت ضمن فئة "التقدير" في هرم ماسلو للحاجات هذا يعني أن عملاء الشركة يبحثون عن التفوق واحترام الذات والمكانة الاجتماعية، تقدم العلامة التجارية منتجات عالية الجودة بأسعار معقولة جدا

وبالتالي إذا فشلت الشركة في التنبؤ بتغيرات تفضيلات المستهلكين أو أنماط الانفاق فسيؤدي ذلك إلى انخفاض المبيعات وتأثير سلبي على سمعة العلامة التجارية. (الرحمنوف، 2019، صفحة 03)

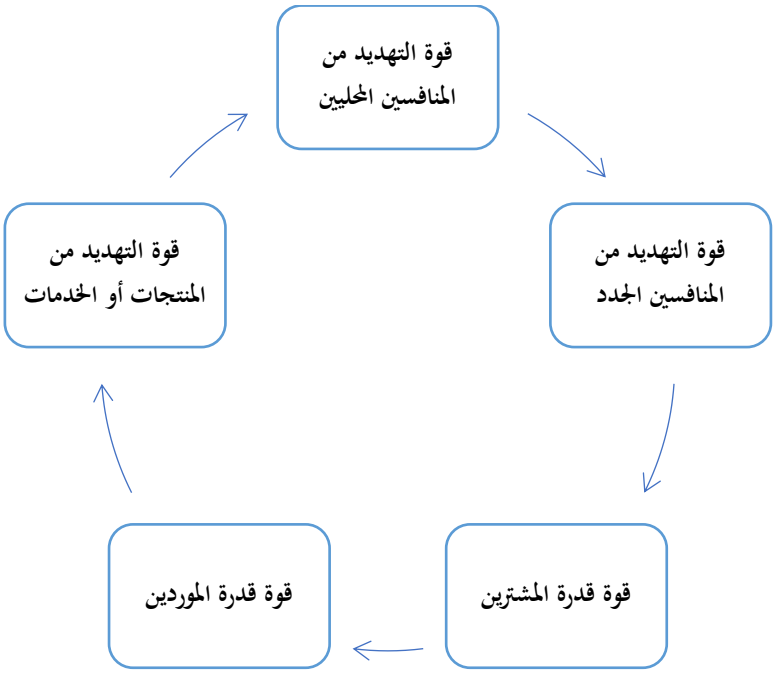
د. قوة قدرة الموردين:

تدرك شركة تارجت أهمية الاستثمار في المجتمعات والموردين الذين تتعامل معهم فهي تتمتع بقدرة عالية في كمشتري وتستطيع تلبية الطلبات بتكلفة أقل بفضل حجم مشترياتها الكبير، كما يمكنها تغيير الموردين متى شاءت عندما لا يلبي الموردون أمرا صعبا في هذا القطاع نظرا لضعف قدرة المنتجات والخدمات التي يقدمها المورد ستجد هذه الامدادات التي استوفت معايير التأهيل المسبق بسهولة فرصة محتملة للتعامل مع رواد هذا القطاع. (looie, 2015, p. 6 7)

هـ.. قوة التهديد من المنتجات او الخدمات البديلة:

تحاول تارجت التخفيف من خطر المنتجات البديلة من خلال تمييز منتجاتها وإنشاء متاجر في مواقع تجارية مركزية، على الرغم من قلة البدائل لتجربة التسوق الفعلية التي تقدمها تارجت إلا أن منتجاتها قابلة للاستبدال لذا فإن خطر المنتجات البديلة كبير بما يكفي للتأثير على ربحية الشركة. (الرحمنوف، 2019، صفحة 03)

الشكل رقم (13): تحليل بورتر لشركة تارجت للتجزئة.



المصدر: من اعداد الطالبتين اعتمادا على ما سبق.

المطلب الثاني: تعزيز الأمن السيبراني بعد الهجمات

بعد الهجوم السيبراني الواسع الذي استهدف الشركة، تبين أن الإجراءات الأمنية التقليدية لم تعد كافية للتصدي للتهديدات المعقدة والمتطورة. وقد مثلت هذه الحادثة نقطة تحول دفعت الشركة إلى مراجعة بنيتها الأمنية واعتماد تقنيات حديثة لتعزيز الحماية وتحسين قدرات الكشف المبكر وفيما يلي أبرز التقنيات:

الفرع الأول: الإجراءات الأمنية المعتمدة بعد عملية الاختراق

بعد حادثة الاختراق أدركت الشركة أهمية تعزيز بنيتها الأمنية، مما أدى إلى اعتماد عدد من التقنيات والإجراءات الوقائية لتعزيز الحماية الداخلية وتحسين القدرة على الكشف المبكر عن محاولات الاختراق ومن أبرزها: (munro, 2024)

1. الفصل بين تكنولوجيا المعلومات وتكنولوجيا التشغيل.
2. مراجعة أمن الموردين وخاصة أولئك الذين يتمتعون بإمكانية الوصول الموثوقة.
3. إنشاء القدرة على مراقبة الشبكات الداخلية بحثا عن أي اختراق.

ويمكن أيضا توضيح بعض الإجراءات الأخرى: (brooks, 2024)

4. تستخدم الشركة في الوقت الحالي تقنيات ناشئة مثل الذكاء الاصطناعي وسلسلة الكتل (البلوك تشين) لتتبع عمليات سلسلة التوريد والاخطار بها وتقييمها.
5. الاعتماد على أنظمة منع فقدان البيانات، التشفير وإدارة السجلات، أنظمة التحكم في الهوية والوصول، منصات إدارة معلومات الأمن والأحداث للحد من التهديدات السيبرانية.
6. يمكن لتقنيات الذكاء الاصطناعي والتعلم الالي توفير رؤية وتحليلات تنبؤية.
7. المحافظة على تغطية تأمينية تهدف إلى الحد من التعرض لبعض مسائل أمن الشبكات والخصوصية.
8. إجراء تدريب دوري وأنشطة امتثال لأعضاء فريق الأمن السيبراني لفهم السلوكيات والمتطلبات التقنية اللازمة لحماية معلومات الشركة والضيوف.
9. التعاون مع أبرز مزودي خدمات الأمن والتكنولوجيا لتقييم برنامج أمن المعلومات والأمن السيبراني واختبار قدراتنا التقنية.

وبعد تطبيق هذه الإجراءات والتقنيات وتطوير النظام الأمني للشركة بعد حادثة الاختراق التي بسببها اختل التوازن المالي حققت استقرارا ماليا وزيادة في ايراداتها ومبيعاتها والتعافي من الأزمة، يمكن توضيح أرباحها كما يلي: (Target corporation, 2019, p. 16)

أ. بلغت الأرباح وفقا للمبادئ المحاسبية المقبولة عموما لكل سهم من العمليات المستمرة 6.34 دولارا.

ب. بلغت الأرباح المعدلة للسهم الواحد من المليات المستمرة 9.39 دولارا.

ج. ارتفعت الايرادات الإجمالية بنسبة 3.7 بالمئة، مدفوعة بزيادة مماثلة في المبيعات ومبيعات المتاجر الجديدة.

د. ارتفعت المبيعات المماثلة بنسبة 3.4 بالمئة، مدفوعة بزيادة في حركة المرور بنسبة 2.7 بالمئة.

(ارتفعت مبيعات المتاجر المماثلة بنسبة 1.4 بالمئة وارتفعت مبيعات القنوات الرقمية بنسبة 29 بالمئة في عام 2019 مقارنة بالفترة المقابلة من العام السابق).

هـ. بلغ الدخل التشغيلي 4658 مليون دولار، وهو أعلى بنسبة 13.3 بالمئة في عام 2019 مقارنة بالفترة المقابلة من العام السابق.

الفرع الثاني: توصيات استباقية للحد من المخاطر المستقبلية

بالرغم من تنفيذ عدة إجراءات تقنية لتعزيز الحماية السيبرانية، لا تزال هناك حاجة إلى توصيات استراتيجية تكميلية تضمن الوقاية المستمرة من الهجمات الالكترونية ونذكر منها ما يلي: (Sanchez, 2025)

1. ينبغي على الشركة اجراء تقييمات دورية لمخاطر الموردين وتطبيق تحليل ثغرات الامن السيبراني لضمان التزام شركائها بمعايير أمنية.

2. يجب على الشركة ضمان تشفير المعلومات الحساسة للحد من مخاطر اختراق البيانات.

3. المراقبة الفورية والاستجابة السريعة للتنبيهات الأمنية.

4. تحتاج الشركة الى اعداد خطة شاملة للاستجابة للحوادث، وتشمل فريق تكنولوجيا المعلومات وفرق القيادة التنفيذية والعلاقات العامة لضمان استجابة منسقة للهجمات الالكترونية.

5. يمكن لتطبيق استراتيجيات تجزئة الشبكة منع المهاجمين من التغلغل داخل البنية التحتية والوصول الى الأنظمة الحيوية.

المطلب الثالث: تقييم التعافي المالي خلال الفترة (2015–2019)

يركز هذا المطلب لتقييم مسار التعافي المالي الذي شهدته شركة **Target**، وذلك من خلال تحليل منهجي لمجموعة من المؤشرات المالية الأساسية، بما في ذلك الإيرادات، وصافي الأرباح، ومستوى المبيعات، بهدف الوقوف على مدى فاعلية الأداء المالي خلال فترة ما بعد الأزمة.

الفرع الأول: دراسة تحليلية لمسار تعافي الإيرادات في شركة **Target** خلال الفترة(2015–2019)

تشكل دراسة مسار الإيرادات أداة تحليلية محورية في استجلاء ملامح التعافي المالي للشركة المتأثرة بالأزمات، لا سيما تلك ذات الطابع السيبراني، وفي هذا الإطار يستعرض الجدول الآتي تطور إيرادات شركة **Target** خلال الفترة الممتدة من 2015 -2019، باعتباره مؤشرا كميا يعكس استجابة الشركة للتحديات التي فرضتها الأزمة الرقمية.

جدول رقم (09): تطور حجم الإيرادات لشركة Target (2015–2019)

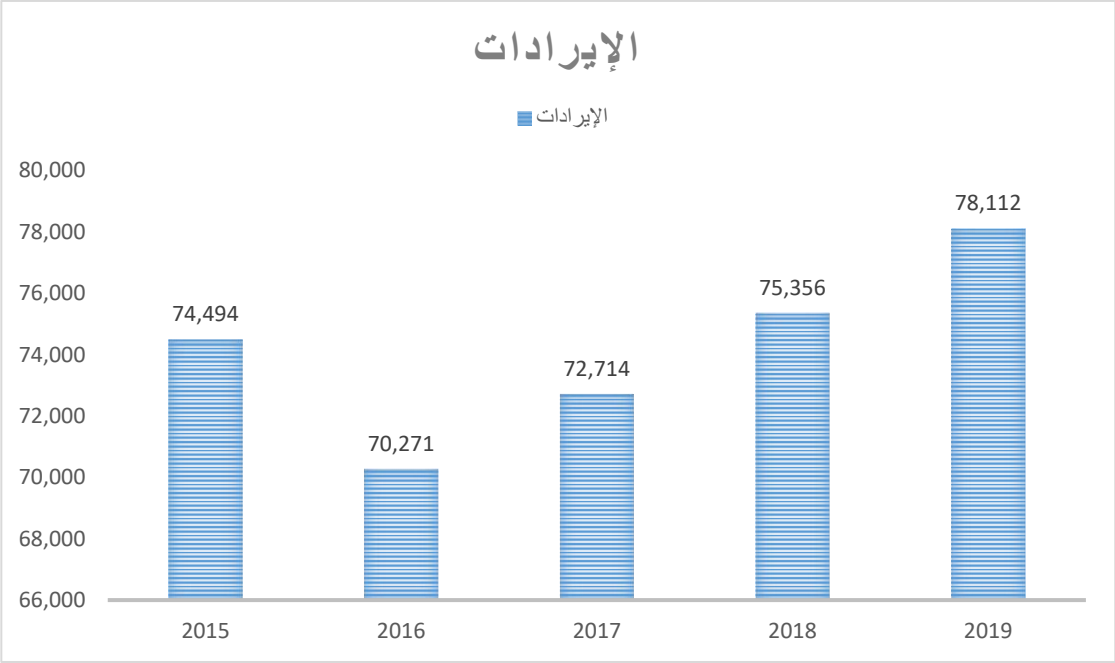
الوحدة: مليون دولار

السنوات	2015	2016	2017	2018	2019
الإيرادات	74,494	70,271	72,714	75,356	78,112

المصدر: من اعداد الطالبتين بالاعتماد على التقرير السنوي (2015-2019).

كما تعرض بيانات الإيرادات في الشكل التالي بناءا على الجدول رقم (09)

الشكل رقم (14): التمثيل البياني لتطور حجم إيرادات شركة Target (2015–2019)



المصدر: من اعداد الطالبتين بالاعتماد على الجدول رقم (09)

بالاعتماد على تحليل الأعمدة البيانية الخاصة بإيرادات شركة **Target** خلال الفترة الممتدة بين عامي 2015 و2019، يتضح أن الشركة قد مرت بثلاث مراحل متمايزة في مسار تطورها المالي، وهو ما يعكس بوضوح أثر التحديات التقنية والأمنية المرتبطة بالهجمات السيبرانية، إلى جانب استجابتها التدريجية لهذه الأزمة من خلال تبنّي إصلاحات هيكلية واستراتيجيات استعادة الثقة.

المرحلة الأولى التأثر السلبي بالهجمات(2016–2015) ، شهدت الشركة خلال هذه المرحلة تراجعا ملموسا في إيراداتها، حيث انخفضت من 74.494 مليار دولار في عام 2015 إلى 70.271 مليار دولار في عام 2016، مسجلة انخفاضا نسبته5.66% نحو ويعزى هذا التراجع بدرجة كبيرة إلى التداعيات الفورية للهجمات السيبرانية التي أثّرت على سلامة البنية التحتية الرقمية للشركة، الأمر الذي انعكس سلبا على مستويات الطلب، نتيجة تزايد مخاوف العملاء حيال خصوصية بياناتهم وأمان معاملاتهم الإلكترونية. وقد ساهم هذا التراجع في تسليط الضوء على الثغرات الأمنية، ما دفع إلى المطالبة بإعادة هيكلة شاملة على مستوى الحوكمة الرقمية.

المرحلة الثانية مرحلة بداية التعافي (2017–2016)، في هذه المرحلة، بدأت المؤشرات الأولية للتعافي المالي بالظهور، حيث ارتفعت الإيرادات إلى 72.714 مليار دولار في عام 2017، بزيادة قدرها حوالي 3.48% مقارنة بالعام السابق. ويشير هذا التحسن إلى استعادة تدريجية لثقة المستهلكين، يحتمل أنها ناتجة عن الإجراءات التصحيحية التي أطلقتها الشركة، لا سيما فيما يتعلق بتعزيز أنظمتها الأمنية، وتطوير قدراتها الرقمية، إلى جانب إطلاق حملات علاقات عامة هدفت إلى تحسين الصورة المؤسسية وطمأنة المتعاملين حيال بيئة التسوق الآمنة.

المرحلة الثالثة مرحلة استعادة النمو والتوسع (2019–2017)، تميزت هذه المرحلة بعودة **Target** إلى مسار النمو المستدام، حيث ارتفعت الإيرادات من 72.714 مليار دولار في عام 2017 إلى 75.356 مليار دولار في عام 2018، ثم إلى 78.112 مليار دولار في عام 2019، محققة نسب نمو سنوي تقدر بـ 3.63و3.66% على التوالي. ويعبر هذا النمو المتواصل عن نجاح الشركة في استعادة قدرتها التنافسية، مدفوعة بتطبيق استراتيجيات فعالة في مجالات التسويق الرقمي، وتوسيع البنية التحتية الرقمية، وتحسين كفاءة سلسلة الإمداد، كما يبرز هذا الأداء الإيجابي فعالية الاستثمارات التي وجهتها الشركة نحو التحول الرقمي وتعزيز مرونة عملياتها التشغيلية في مواجهة التحديات.

الفرع الثاني: دراسة تحليلية لمسار تعافي المبيعات في شركة **Target** خلال الفترة(2015–2019)

يعتبر التقييم تحليلا مسار المبيعات في شركة Target من خلال استعراض المراحل الثلاث التي تلت الأزمة السيبرانية، وذلك بهدف فهم ديناميكيات التكيف المالي التي اعتمدتها الشركة ومدى مساهمتها في استعادة الاستقرار الربحي. ويظهر الجدول الآتي تطور صافي أرباح الشركة خلال الفترة الممتدة من 2015 إلى 2019.

جدول رقم (10): المبيعات السنوية لشركة Target (2015–2019)

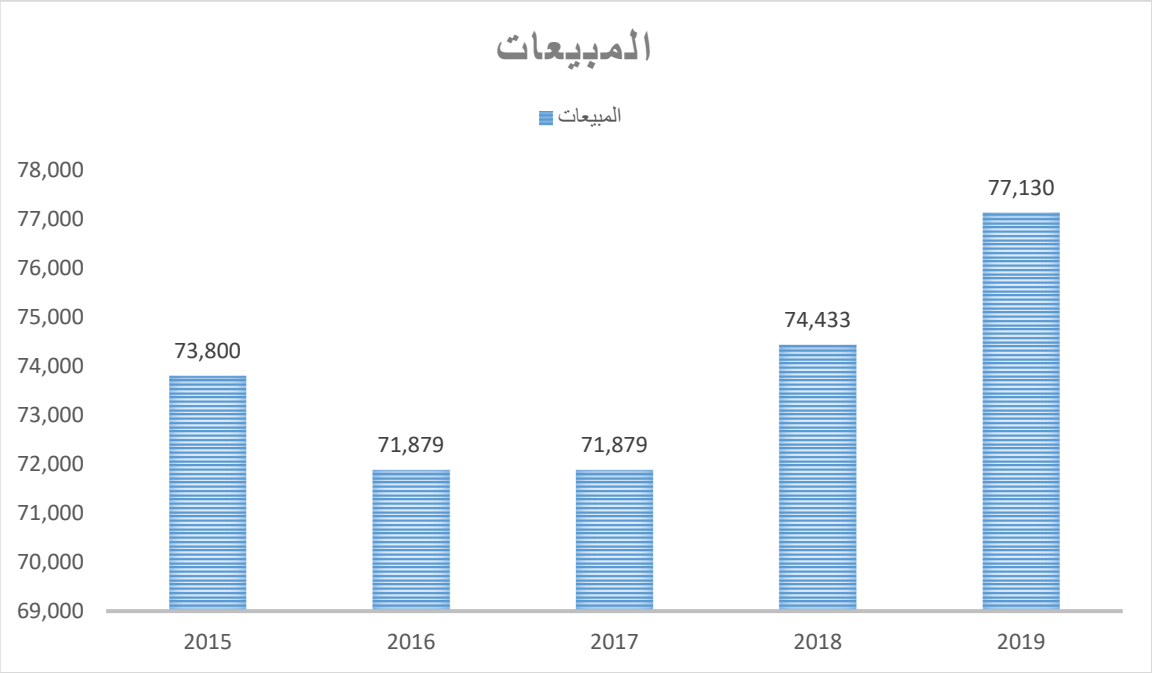
الوحدة: مليار دولار

السنوات	2015	2016	2017	2018	2019
المبيعات	73,8	69,495	71,879	74,433	77,130

المصدر: من اعداد الطالبتين بالاعتماد على التقرير السنوي لشركة Target سنة (2015-2019)

وسيتم ترجمة بيانات الجدول الموالي في تمثيل بياني لتوضيح المبيعات السنوية للشركة:

الشكل رقم (15): التمثيل البياني للمبيعات السنوية للشركة خلال الفترة (2015–2019)



المصدر: من اعداد الطالبتين بالاعتماد على الجدول رقم (10)

بالاعتماد على تحليل الاعمدة البيانية للفترة الممتدة بين عامي 2015 و2019، يتبيّن أن شركة **Target**قد مرت بثلاث مراحل محورية في تطور أدائها المالي، لاسيما على صعيد الإيرادات، وذلك ضمن سياق تفاعلي مع تداعيات الهجمات السيبرانية التي طالت بنيتها الرقمية. وتبرز هذه المراحل بوصفها محطات نوعية عكست قدرة الشركة على التكيّف مع الأزمات، واستعادة ثقة المتعاملين، وتعزيز موقعها التنافسي في سوق التجزئة.

مرحة التأثير السلبي (2016–2015)، تمثل هذه المرحلة نقطة تراجع حادة في الأداء المالي للشركة، حيث تراجعت الإيرادات من 74.494 مليار دولار في عام 2015 إلى 70.271 مليار دولار في عام 2016، بنسبة انخفاض بلغت 5.66% وهو ما يعكس الأثر الفوري للهجمات السيبرانية على ثقة العملاء. ويعزى هذا الانخفاض بصورة أساسية إلى تراجع ثقة المستهلكين في البيئة الرقمية الآمنة التي تقدمها الشركة، الأمر الذي أدى إلى انخفاض في الطلب وتردد في استخدام المنصات الإلكترونية لـ **Target** وقد شكل هذا التراجع إشارة واضحة إلى الحاجة الملحة لتبني إصلاحات هيكلية في مجال أمن المعلومات وتعزيز البنية الرقمية.

مرحلة التعافي التدريجي(2017–2016) ، شهدت هذه المرحلة بداية تحول إيجابي في مسار الأداء المالي، حيث ارتفعت الإيرادات إلى 72.714 مليار دولار في عام 2017، بنسبة نمو قدرها 3.47% ويعد هذا التحسن مؤشرا على استعادة جزئية لثقة العملاء، من المرجّح أنها جاءت نتيجة لحزمة من الإجراءات التصحيحية التي بادرت بها الشركة. تضمنت هذه الإجراءات تحسينات واسعة في أنظمة الحماية الإلكترونية، وزيادة الاستثمارات في أمن البيانات، وتطوير تجربة العملاء الرقمية، فضلا عن إطلاق حملات علاقات عامة هدفت إلى استعادة السمعة المؤسسية وتحسين الصورة الذهنية للشركة في السوق.

مرحلة النمو (2019–2017)، تميزت هذه المرحلة بعودة الشركة إلى مسار النمو المالي المستدام، حيث ارتفعت الإيرادات إلى 75.356 مليار دولار في عام 2018، ثم إلى 78.112 مليار دولار في عام 2019 بنسب نمو سنوي بلغت 3.63% و3.66% على التوالي، ويعد هذا النمو دلالة على نجاح **Target** في احتواء تداعيات الأزمة السيبرانية، وتحقيق تحول استراتيجي في نموذجها التشغيلي. وقد ساهمت مجموعة من السياسات والقرارات في هذا التحول، من أبرزها توسيع البنية التحتية الرقمية، تطوير قنوات التجارة الإلكترونية، تعزيز كفاءة سلسلة الإمداد، وتبني أساليب تسويق رقمي مبتكرة. كما أثبتت الاستثمارات في مجال التحول الرقمي فعاليتها من خلال ترسيخ موقع الشركة كلاعب رئيسي في سوق التجزئة الأمريكية.

الفرع الثالث: دراسة تحليلية لمسار تعافي صافي الارباح في شركة **Target** خلال الفترة(2019–2015)

يهدف التحليل لتقييم مسار تعافي صافي الأرباح الذي شهدته شركة Target، وذلك من خلال استعراض المراحل الثلاث التي مرت بها عقب الأزمة السيبرانية، بهدف فهم ديناميكيات التكيف المالي واستعادة الاستقرار الربحي، يبرز الجدول الموالي تطور صافي أرباح الشركة Target خلال الفترة الممتدة من 2015 -2019.

جدول رقم (11): تطور حجم صافي الارباح لشركة Target (2015–2019)

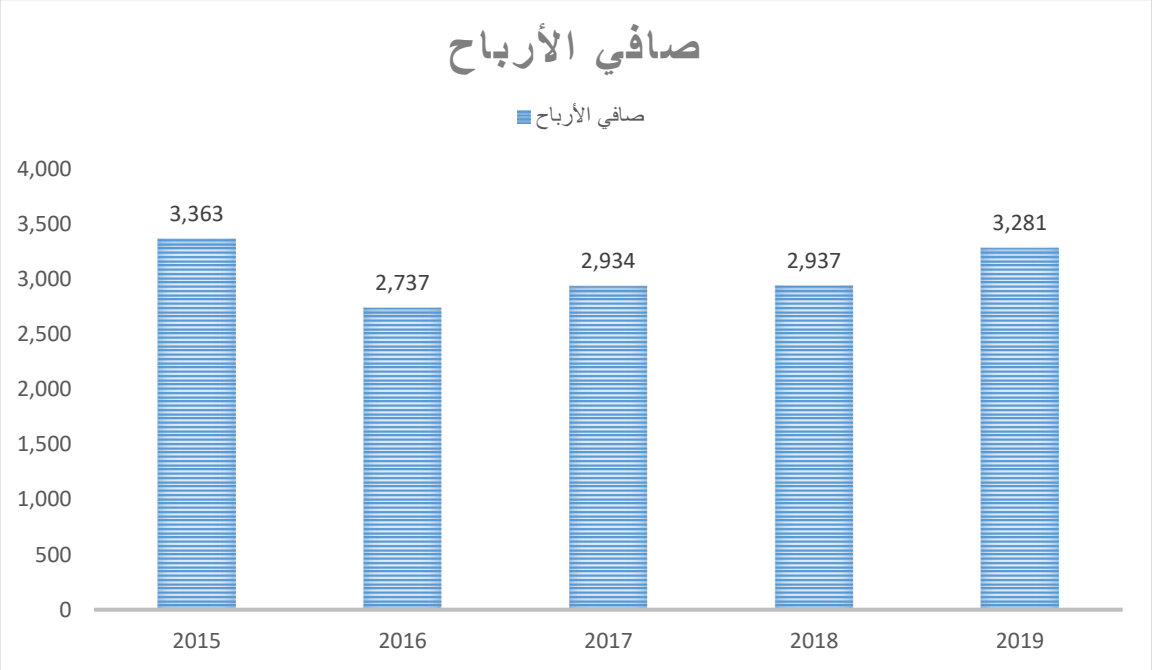
الوحدة: مليون دولار

السنوات	2015	2016	2017	2018	2019
صافي الأرباح	3,363	2,737	2,934	2,937	3,281

المصدر: من اعداد الطالبتين بالاعتماد على التقرير السنوي 2019،2018،2017،2016،2015.

وانطلاقا من هذا الجدول سيتم ابراز حجم أرباح صافي الشركة في التمثيل البياني الموالي:

الشكل رقم (16): التمثيل البياني لحجم صافي الأرباح للشركة خلال الفترة (2015–2019)



المصدر: من اعداد الطالبتين بالاعتماد على الجدول رقم (11)

استنادا إلى تحليل الأعمدة البيانية الخاصة بتطور صافي أرباح شركة **Target** خلال الفترة الممتدة من عام 2015 إلى عام 2019، يمكن تمييز ثلاث مراحل رئيسية تعكس التفاعل المالي للشركة مع تداعيات الهجمات السيبرانية التي تعرضت لها، ومدى قدرتها على التكيف واستعادة الاستقرار المالي. وتبرز هذه المراحل التحول التدريجي في الأداء المالي من التأثر السلبي إلى التعافي، ثم الوصول إلى مرحلة التوازن والنمو المستدام.

المرحلة الأولى مرحلة التراجع الحاد في الربحية (2015–2016)، شهدت الشركة خلال هذه المرحلة انخفاضا كبيرا في صافي أرباحها، حيث تراجع من 3.363 مليار دولار في عام 2015 إلى 2.737 مليار دولار في عام 2016، مسجّلًا انخفاضًا بنسبة تقارب 18.6%. ويعزى هذا التراجع إلى التأثيرات المباشرة للأزمة السيبرانية، التي أفرزت تكاليف مالية مرتفعة نتيجة لتعزيز إجراءات الأمن الإلكتروني، وتراجع المبيعات بسبب اهتزاز ثقة العملاء،

إلى جانب الأعباء القانونية والتعويضات المحتملة. كما يعكس هذا الأداء محدودية مرونة البنية التشغيلية للشركة في التعامل مع الأزمات المفاجئة، في ظل ارتفاع التكاليف التشغيلية وتراجع الكفاءة المؤسسية خلال تلك الفترة.

المرحلة الثانية مرحلة بداية استعادة الربحية(2017–2016) ، في هذه المرحلة، بدأت بوادر التحسن المالي في الظهور، حيث ارتفع صافي الأرباح إلى 2.934 مليار دولار في عام 2017، بزيادة تقدر بنسبة 7.2% مقارنة بعام 2016. ويعتبر هذا الارتفاع مؤشراً إيجابياً على فاعلية الإجراءات التي اتخذتها الشركة للتعامل مع تداعيات الأزمة، لاسيما فيما يتعلق بضبط التكاليف التشغيلية، وتحسين كفاءة الأداء الداخلي، وتعزيز منظومة الأمن السيبراني. كما ساهم تحسن نسبي في ثقة المستهلكين وتعافي السوق في تخفيف الضغط المالي، ما مكن الشركة من استعادة جزء من ربحيتها.

المرحلة الثالثة مرحلة الاستقرار والنمو المالي (2019–2017)، دخلت **Target** خلال هذه المرحلة في فترة من الاستقرار المالي، حيث بلغ صافي الأرباح 2.937 مليار دولار في عام 2018، وهو ما يعكس قدرة الشركة على الحفاظ على مستوى ربحي ثابت رغم استمرار تحديات السوق. وفي عام 2019، تحقق تحسن واضح في صافي الأرباح، لتصل إلى 3.281 مليار دولار، مقتربة من مستويات ما قبل الأزمة. ويمثل هذا النمو التدريجي مؤشرا على نجاح استراتيجيات الشركة في تعزيز قدرتها على توليد الأرباح من أنشطتها التشغيلية. كما يُظهر نتائج ملموسة للاستثمارات التي قامت بها في مجالات التحول الرقمي وتعزيز الأمن السيبراني، بالإضافة إلى كفاءة إدارة التكاليف وتوظيف أدوات التسويق الرقمي بفعالية، وهو ما ساهم في تحسين أدائها المالي وتعزيز موقعها التنافسي في السوق.

خلاصة الفصل:

تحتل شركة **Target** موقعا ريياديا ضمن كبرى شركات البيع بالتجزئة عالميا، حيث تميزت بتبنيها المتسارع للتحول الرقمي واعتمادها الحلول التقنية المتطورة لتعزيز كفاءة سلسلة القيمة التشغيلية وتحسين تجربة المستهلك. إلا أن هذا التحول الرقمي غير المدعوم باستراتيجية أمنية متكاملة وعدم كفاية الاستثمارات في مجال الأمن السيبراني قد عرضها لمخاطر إلكترونية جسيمة، فاعتماد نظام أمني متكامل ومتطور لا يمثل مجرد إجراء وقائي بل يشكل استثمارا استراتيجيا في رأس المال غير المادي للشركة، وضمانة أساسية لتعزيز ثقة العملاء والحفاظ على السمعة المؤسسية في سوق تشهد تنافسية متزايدة.

الخاتمة

في ظل التسارع التكنولوجي المتزايد والتحول الرقمي الشامل، برز الأمن السيبراني كعامل محوري في تعزيز متانة القطاع المالي وضمان استقراره أمام التهديدات الإلكترونية المتنامية. وتكشف هذه الدراسة أن تعزيز آليات التعاون المشترك بين الأطراف المعنية بما في ذلك الحكومات والقطاع الخاص والمؤسسات الدولية يمثل ركيزة أساسية لمواجهة التحديات الأمنية الرقمية.

كما تؤكد النتائج على الأهمية الاستراتيجية لاعتماد الحلول التقنية المتطورة، مثل أنظمة الذكاء الاصطناعي وخوارزميات تعلم الآلة، في تعزيز قدرات الكشف المبكر عن التهديدات السيبرانية ورفع كفاءة آليات الاستجابة، ويسهم ذلك في بناء منظومة مالية أكثر مرونة.

يتضح من التحليل أن ضمان الحماية السيبرانية الفاعلة لم يعد خيارا ثانويا، بل أصبح متطلبا جوهريا لتحقيق الاستدامة المالية. ويتطلب ذلك تعزيز الاستثمار في البنى التحتية الرقمية الآمنة، ورفع مستوى الوعي بالمخاطر السيبرانية عبر برامج التوعية المتخصصة، بالإضافة إلى تعزيز أواصر التعاون الدولي لمواكبة التحديات المستقبلية في هذا المجال الحيوي. وبذلك يمكن التأكيد على أن تعزيز الأمن السيبراني يشكل مدخلا استراتيجيا لضمان استقرار المنظومة المالية، وحماية مصالح جميع الأطراف المعنية في ظل المشهد الرقمي المتغير.

1. اختبار الفرضيات:

أ. الفرضية الأولى:

– (يرتبط تحسين مستوى الأمن السيبراني بارتفاع مؤشرات السلامة المالية، من خلال تقليص مخاطر الاختراقات، وتعزيز ثقة المتعاملين في استقرار النظام المالي)، وما يثبت صحة هذه الفرضية هو أن تعزيز مستوى الأمن السيبراني يسهم بشكل فعال في تحسين مؤشرات السلامة المالية، وذلك من خلال الحد من مخاطر الاختراقات الإلكترونية وتعزيز ثقة المتعاملين في استقرار النظام المالي، كما أن تقوية البنية التحتية السيبرانية للمؤسسات المالية تقلل من احتمالية تعرضها للهجمات الإلكترونية، الأمر الذي ينعكس إيجابا على استقرار النظام المالي ويعزز من ثقة المشاركين فيه.

ب. الفرضية الثانية:

–)يقوم الأمن السيبراني بدور محوري في تعزيز كفاءة نظم الإنذار المبكر داخل النظام المالي، مما يمكن الجهات الرقابية من الكشف الاستباقي والاستجابة الفعالة للتهديدات المالية المحتملة)، وما يثبت صحتها هو أن للأمن السيبراني دورا محوريا في تعزيز كفاءة نظم الإنذار المبكر، حيث أفضى اعتماد آليات متقدمة للرصد والتحليل إلى تحسين قدرة الجهات الرقابية داخل الشركة على الكشف المسبق والاستجابة الفعالة للتهديدات

المالية المحتملة، وقد أسهمت في تحسين قدرة الجهات الرقابية على اكتشاف التهديدات في مراحلها الأولية، وتقليص زمن الاستجابة، مما أتاح اتخاذ قرارات استباقية للتخفيف من الأثر السلبي المحتمل.

ج. الفرضية الثالثة:

– (يساعد الأمن السيبراني في رفع كفاءة تطبيق سياسات الحيطة الكلية، من خلال تقليص المخاطر التكنولوجية التي تواجه المؤسسات المالية)، وما يثبت صحة هذه الفرضية ان الأمن السيبراني يعد عاملا داعما في تطبيق سياسات الحيطة الكلية، حيث يساهم في بناء بيئة مالية آمنة تقل فيها المخاطر التكنولوجية، مما يوفر إطارا أكثر صلابة لاتخاذ قرارات سيادية ومؤسسية مستندة إلى معلومات دقيقة وآمنة.

د. الفرضية الرابعة:

– (يساهم الأمن السيبراني بشكل فعال في تحسين سرعة ودقة اكتشاف التهديدات التي قد تؤثر على سلامة البيانات المالية)، وما يثبت صحة هذه الفرضية أن توافر أنظمة سيبرانية متطورة يسهم في رفع كفاءة اكتشاف التهديدات في مراحلها المبكرة، مع تقليل الوقت اللازم للمعالجة، مما يعزز سلامة البيانات المالية ويقلل من فرص التسرب أو التلاعب بالمعلومات المحاسبية والمالية الحساسة.

2. نتائج الدراسة:

من خلال الأفكار التي استعرضتها الدراسة لموضوع **مساهمة الامن السيبراني في تعزيز الاستقرار المالي**، تم تقسيم نتائج الدراسة إلى نتائج نظرية وأخرى تطبيقية، وذلك على النحو التالي:

أ. النتائج التي تعنى بالناحية النظرية والأكاديمية للدراسة، والمتمثلة فيما يلي:

– يعد تعزيز إجراءات الأمن السيبراني عاملا حاسما في التخفيف من حدة المخاطر والهجمات الإلكترونية التي تهدد أمن البيانات وسلامة العمليات.

– يساهم تطبيق معايير الأمن السيبراني في تأمين المعلومات الحساسة ومنع وصول الجهات غير المصرح بها إليها، مما يحد من مخاطر التعرض للهجمات الإلكترونية.

– لا يمكن ضمان أمن سيبراني شامل دون تعاون وثيق وتكامل جهود جميع الجهات الفاعلة، بما في ذلك الحكومات والقطاعات التجارية والمؤسسات المختلفة.

– يعد الاستقرار المالي عاملا أساسيا في تعزيز القدرة على مواجهة التقلبات المالية، مما يسهم في الحفاظ على استدامة نمو الشركة وتحقيق أهدافه الاستراتيجية.

-لا يمكن تحقيق استقرار مالي مستدام في ظل التهديدات السيبرانية المتزايدة، ما لم يصاحبه تعاون فعال بين الإدارات الداخلية والجهات المعنية لتطوير سياسات وقائية وتعزيز البنية الأمنية.

-يعد الاستقرار المالي من العوامل الأساسية التي تعزز قدرة الشركة على التكيف مع التغيرات، بالإضافة إلى ذلك يكتسب الأمن السيبراني أهمية متزايدة إذ يعتبر عنصراً حيوياً في حماية البيانات والأنظمة المعلوماتية من المخاطر الرقمية.

ب. النتائج التي تعنى بالجانب العملي التطبيقي الخاص بدراسة حالة شركة تارجت الأمريكية، وخلصت الدراسة إلى النتائج التالية:

-أظهرت البيانات المالية لشركة **Target** تقلبا ملحوظا في كل من الإيرادات والمبيعات وصافي الأرباح، وذلك على خلفية الهجمات السيبرانية التي تعرضت لها في عام 2013، وعلى الرغم من أن الشركة نجحت في استعادة نمو الإيرادات والمبيعات خلال عام 2014، إلا أن صافي الأرباح ظل متأثرا بشكل واضح، مما يعكس الأثر المالي الكبير للتكاليف غير المباشرة المرتبطة بانتهاكات الأمن السيبراني، بما في ذلك تراجع ثقة العملاء.

-شرعت الشركة في تنفيذ عملية شاملة لإعادة هيكلة بنيتها التحتية للأمن السيبراني في أعقاب الحادثة، حيث تضمنت هذه العملية تحديث الأنظمة التقنية المعتمدة، إلى جانب إعادة تنظيم الهيكل الإداري المتعلق بإدارة المخاطر والأمن السيبراني.

-تمكنت شركة **Target** من تحقيق الاستقرار المالي وإعادة التوازن، وقد انعكس ذلك إيجابا في استعادة ثقة العملاء تدريجيا، وهو ما أسهم في استقرار الإيرادات والمبيعات، إلى جانب تحسن في صافي الأرباح. وتعد هذه النتائج مؤشرا على فعالية التدابير التصحيحية التي اتبعتها الشركة، وعلى نجاحها في استعادة موقعها التنافسي في السوق بعد الأزمة.

3. التوصيات:

على ضوء النتائج المتوصل لها من خلال هذه الدراسة، يتم التوصية بما يلي:

أ. ينبغي تبني منهجية شاملة لتعزيز الوعي بالأمن السيبراني عبر تصميم برامج تدريبية مكثفة ودورات متخصصة تركز على معايير الأمن الرقمي، وذلك لرفع كفاءة الموظفين في التعامل مع التهديدات السيبرانية المتطورة.

ب. يتطلب ضمان مواكبة التطورات التقنية تحديث البنية التحتية التكنولوجية للشركة وفقا لأحدث المعايير العالمية، مع التركيز على تبني حلول قابلة للتطوير والتكيف مع المتغيرات التقنية المستقبلية.

ج. يجب تعزيز إجراءات حماية البيانات الحساسة من خلال توظيف تقنيات تشفير متقدمة واعتماد آليات أمنية حديثة لضمان سلامة المعلومات وسريتها.

د. لا بد من إقامة شراكات استراتيجية مع جهات وخبراء متخصصين في الأمن السيبراني لتعزيز تبادل المعرفة الموثوقة وتبني أفضل الممارسات الأمنية، بما يسهم في تطوير سياسات الحماية السيبرانية للشركة.

هـ. إدارة أفضل لسلسلة التوريد والموردين وهذا عن طريق فرض سياسات وصول محددة للموردين بحيث لا يمكن للموردين الوصول إلا لما يحتاجونه فقط.

و. إنشاء وتقوية قسم خاص بالأمن السيبراني بقيادة مسؤول أمن معلومات تنفيذي مستقل يرفع تقاريره للإدارة العليا.

4. آفاق الدراسة

إن موضوع "**مساهمة الأمن السيبراني في تعزيز الاستقرار المالي: دراسة حالة شركة تارجت**"، يساهم في تحليل الأثر الاستراتيجي للأمن السيبراني على تعزيز الاستقرار المالي، من خلال استعراض حالة تطبيقية لسياسات الحماية الرقمية في شركة تارجت. حيث تقدم رؤية تحليلية حول الآليات والتقنيات الأمنية الضرورية لضمان المرونة المالية في بيئات الأعمال الرقمية. كما تسلط الضوء على مجموعة من المحاور البحثية التي يمكن أن تشكل إطارا لدراسات مستقبلية في هذا المجال، والمتمثلة فيما يلي:

أ. دور الذكاء الاصطناعي والتعلم الآلي في التنبؤ بالهجمات السيبرانية المالية.

ج. دور الهجمات السيبرانية في زعزعة استقرار النظم المالية.

د. تحليل جهوزية القطاع المالي الجزائري للاعتماد على تقنيات الأمن السيبراني.

قائمة المراجع

أولا. المراجع باللغة العربية

أ. الكتب:

1. أحمد مداني، (2020)، **نظم صناعة الاستقرار المالي في أسواق الأوراق المالية العربية الناشئة**، مؤسسة الوراق للنشر والتوزيع، عمان، الأردن، ص 22.

2. أيمن أحمد الحديدي، (2023)، **كتاب الأمن السيبراني في ظل الانفجار المعرفي**، دار اليازوري العلمية للنشر والتوزيع، الطبعة الأولى، عمان وسط البلد، ص 72.

3. عبد الله اللقاني، (2023)، **دور الأمن السيبراني في تعزيز أمن المعلومات المالية والالكترونية**، دار اليازوري العلمية للنشر والتوزيع، الطبعة الأولى، عمان، الأردن، ص 153.

4. محمد عبد الله شاهين محمد، (2024)، **الأمن السيبراني ونظم حماية المعلومات**، دار يافا العلمية للنشر والتوزيع، الطبعة الأولى، عمان، الأردن، ص88-89-90.

ب. المقالات:

5. إبراهيم السيد أحمد رضوان، 2025، **مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي**، مجلة العلوم القانونية والاقتصادية، المجلد 67، العدد 01، ص 1755.

6. إبراهيم زكرياء الشربيني، (2018)، **محددات الاستقرار المالي وكيفية قياسه**، مجلة التجارة والتمويل، المجلد 38، العدد 3، جامعة دمياط، مصر، ص308-309.

7. أحمد الباسوسي، (2023)، **الجهود الدولية لمكافحة الهجمات السيبرانية على قطاع الطاقة**، مجلة كلية الاقتصاد والعلوم السياسية، المجلد 24، العدد 4، الجامعة المصرية-الروسية، مصر، ص156.

8. إدريس عطية، (2019)، **مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري**، مصداقية، المجلد 01، العدد 01، جامعة العربي تبسي، تبسة، الجزائر، ص 105-106.

9. إسماعيل زروقة، (2019)، **الفضاء السيبراني والتحول في مفهوم القوة والصراع**، مجلة العلوم القانونية والعلوم السياسية، المجلد 10، العدد 01، جامعة الشهيد حمه لخضر، الوادي، الجزائر، ص 10-23.

10. آسيا بن داية وأسماء سفاري، (2020)، **الاستقرار المالي بين وقع الأزمة المالية العالمية وضغط معايير بازل الدولية-أي دور البنوك المركزية كنموجا-**، مجلة العلوم الإنسانية، المجلد 7، العدد 2، ص 581.

11. أشرف محمد إبراهيم أبو صيام، 2024، **الهجمات السيبرانية على الاحتلال الإسرائيلي وأثرها على القضية الفلسطينية من منظور القانون الدولي**، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، المجلد 17، العدد 01، ص 47/46.

12. افتخار محمد مناحي الرفيعي، (2022)، **الاستقرار المالي في القطاع المصرفي العراقي العام للمدة(2009–2019)**، المجلة الجزائرية للمالية العامة، المجلد 12، العدد 01، الجامعة العراقية، العراق، ص105.

13. الجوهرة بنت عبد الرحمان إبراهيم المنيع، 2022، **متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية 2030**، إدارة البحوث والنشر العلمي، المجلد 38، العدد 01، ص 164.

14. أمال بن الدين وعبد القادر مطاي، 2019، **تحليل مؤشرات قياس الاستقرار المالي والمصرفي: دراسة تطبيقية حالة الجزائر**، مجلة العلوم الاقتصادية والتسيير والعلوم التجارية، المجلد 12، العدد 02، الجزائر، ص93.

15. بدر الدين عاشوري وحمزة طيبي، (2023)، **أثر الحوكمة البنكية في تحقيق الاستقرار المالي داخل المنظومة البنكية الجزائرية دراسة تحليلية لبنك الجزائر للفترة(2014–2021)**، مجلة البحوث في العلوم المالية والمحاسبية، المجلد 08، العدد 01، جامعة الأغواط، الجزائر، ص223.

16. بدر عدنان أحمد سعد الخبيزي، (2023)، **تحديات وتهديدات الأمن السيبراني وكيفية التغلب عليها**، حوليات آداب عين شمس، المجلد 51، العدد 07، الكويت، ص 246.

17. بلعيد سمية وبوراس أحمد، (2022)، **أثر مؤشرات الحيطة الكلية على تطور القطاع المصرفي الجزائري دراسة قياسية للفترة (2000–2017)**، مجلة الدراسات المالية والمحاسبية والإدارية، المجلد 09، العدد 01، الجزائر، ص 555.

18. بوطبة عبد الله وبوستي توفيق، 2024، **دور الأمن السيبراني في تعزيز الأمن الصحي الدولي**، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 09، العدد 02، ص 706.

19. بوقرين عبد الحليم، 2022، **الأمن السيبراني والمضامين المفاهيمية المرتبطة به**، مجلة طبنة للدراسات العلمية الأكاديمية، المجلد 05، العدد 02، الجزائر، ص 48.

20. حرز الله محمد لخضر، 2023، **جرائم الانترنت وتحديات الأمن السيبراني: دراسة متغيرات الجريمة ومقارباتها العلاجية**، مجلة المفكر، المجلد 18، العدد 01، الجزائر، ص 515.

21. حكمت رشيد سلطان، (2024)، **دور المرونة المالية في تحقيق الاستقرار المالي دراسة تحليلية لعينة من المصارف الخاصة المدرجة في سوق العراق للأوراق المالية للمدة(2012–2021)**، المجلة الأكاديمية لجامعة نوروز، المجلد 13، العدد 01، اقليم كوردستان، العراق، ص 649.

22. حميدي حياة وطايلب نسيمة، (2022)، **مدخل مفاهيمي حول الأمن السيبراني**، مدار للدراسات الاتصالية الرقمية، المجلد 2، العدد 2، الجزائر، ص 9-10.

23. خالد ظاهر عبد الله جابر السهيل المطيري، (2022-2023)، **دور التشريعات الجزائرية في حماية الأمن السيبراني**، مجلة البحوث الفقهية، المجلد 34، العدد 38، الكويت، ص 994.

24. دراعو عز الدين،2022، **الآثار الاقتصادية والمالية للهجمات السيبرانية في ظل التحول الرقمي: النتائج والتجارب والحلول**، مجلة التكامل الاقتصادي، المجلد، العدد، البلد، ص 115.

25. رحاب يوسف ووليد محمود السيد، (2022)، **الأمن السيبراني والنظافة الرقمية**، المجلة المصرية لعلوم المعلومات، المجلد 09، العدد 02، مصر، ص 394.

26. زواد نجاة، (2023)، **دور التمويل المستدام في تحقيق الاستقرار المالي**، مجلة التنمية والاستشراف للبحوث والدراسات، المجلد 08، العدد 01، الجزائر، ص100.

27. ساعد بوقرص، 2022، **الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة**، مجلة الأبحاث في الحماية الاجتماعية، المجلد 03، العدد 01، ص 65.

28. سامي محمد بونيف، 2019، **دور الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية – الردع السيبراني انموذجا–**، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 04، العدد 07، الجزائر، ص 125.

29. سرين حشمان، (2024)، **المخاطر السيبرانية في الصناعة المالية الإسلامية**، المجلة الجزائرية للعولمة والسياسات الاقتصادية، المجلد 15، العدد 01، تيبازة، الجزائر، ص 62.

30. سنوساوي فاطمة وبوشامة مصطفى، (2022)، **تعزيز الاستقرار المالي في الجزائر على ضوء اتفاقية بازل 03**، مجلة الابداع، المجلد 12، العدد 01، الجزائر، ص 209.

31. شرقي عبد الغاني، (2023)، **التهديدات السيبرانية واشكالية السيادة: إعادة قراءة لسيادة واستفاليا**، مجلة السياسة العالمية، المجلد 7، العدد 2، بومرداس، الجزائر، ص 275.

32. طالة لمياء، 2021، الإرهاب السيبراني والأمن القومي: قراءة في تحولات الاستراتيجية الدفاعية، حوليات جامعة الجزائر 1، المجلد 35، العدد 04، الجزائر، ص 361.

33. فاطمة الزهراء مغدور وعماد معوشي، (2022)، الشمول المالي كاستراتيجية لتعزيز الاستقرار المالي في الدول العربية، مجلة شعاع للدراسات الاقتصادية، المجلد 06، العدد 02، المدية، الجزائر، ص 176.

34. فاطمة علي إبراهيم ورحاب يوسف ووليد محمود السيد، (2022)، **الأمن والنظافة الرقمية**، المجلة المصرية للعلوم والمعلومات، المجلد 9، العدد 2، جامعة بني سويف، مصر، ص 398.

35. فريدة موهوب وصندرة لعور، (2022)، **تحليل دور مؤشرات السلامة المالية في تحقيق الاستقرار المالي في القطاع المصرفي العربي**، مجلة التحليل الاقتصادي ودراسات التنمية، المجلد 01، العدد 02، النعامة، الجزائر، ص 40-41.

36. لمياء زواوي، 2023، **التهديدات السيبرانية وأمن المجتمع الرقمي: دراسة حالة الجزائر**، المجلة الجزائرية للأمن والتنمية، المجلد 12، العدد 02، ص 151.

37. محمد الصغير كاوجة، (2022)، **الهجومات السيبرانية بين الواقع وسبل المواجهة**، مجلة الرسالة للدراسات الإعلامية، المجلد 06، العدد 03، تبسة، الجزائر، ص 88-89-90.

38. محمد العيداني، (2024)، **التهديدات السيبرانية وجرائم المعلومات**، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 13، العدد 1، الجزائر، جامعة بوشوشة آفلو، الأغواط، الجزائر، ص 17.

39. محمد دحماني، (2023)، **التهديدات السيبرانية –الهندسة الاجتماعية كنموذجا–**، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 7، العدد 2، الأغواط، الجزائر، ص686.

40. محمد مجدي عبد السلام وراغب أحمد ومحمد صقر، (2024)، **أثر المخاطر النظامية على الاستقرار المالي للبنوك دراسة تطبيقية على عينة من البنوك المصرية خلال الفترة 2018–2022**، جامعة الإسكندرية للعلوم الإدارية، المجلد 61، العدد 3، مصر، ص 426.

41. مروة فتحي السيد البغدادي، 2021، **اقتصاديات الأمن السيبراني في القطاع المصرفي**، مجلة البحوث القانونية والاقتصادية، المجلد 01، العدد 76، الإسكندرية، ص 146.

42. معن نايل محمود المعايطة، (2024)، **استراتيجيات الأمن السيبراني ودورها في تعزيز حماية الشبكات الالكترونية في البلديات**، مجلة العلوم السياسية والطبيعية، المجلد 4، العدد 5، الأردن، ص 367-368.

43. منى عبد الله السمحان، (2023)، **متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية**، مجلة كلية التربية جامعة المنصورة، المجلد 111، العدد 1، مصر، ص 12.

44. مهند حميد ياسر العطوي وأحمد رزاق كاظم التميمي، (2023)، **تشخيص مستوى الركود المالي واستثماره في تحقيق الاستقرار المالي للشركات الصناعية المساهمة**، مجلة الغري للعلوم الاقتصادية والإدارية، المجلد 19، العدد 4، جامعة الكوفة، العراق، ص 474-475.

45. نظيرة قلادي، (2017)، **مدى فعالية أنظمة الإنذار المبكر في قياس الاستقرار المالي**، مجلة العلوم الإنسانية، المجلد 02، العدد 08، أم البواقي، الجزائر، ص 323.

46. هاني محمد خليل العزازي، (2023)، **النظام القانوني الدولي لمكافحة المخاطر السيبرانية**، مصر المعاصرة، المجلد 114، العدد 549، جامعة الزقازيق، مصر، ص 474.

47. وسام محمود عارفان، (2024)، **سبل مكافحة الهجمات دوليا**، مجلة الدراسات القانونية والاقتصادية، المجلد 10، العدد 3، ص 474.

ج. الأطروحات والرسائل:

48. أمال بن الدين، (2019-2020)، **دور البنوك المركزية في تحقيق الاستقرار المالي في ظل الأزمات المالية**، (أطروحة دكتورا)، قسم الاقتصاد كلية العلوم الاقتصادية والتجارية وعلوم التسيير جامعة حسيبة بن بوعلي، الشلف، الجزائر، ص06.

49. أماني تموز عبد الرحمان الخفاجي، (2024)، **الحماية التأمينية للشركات التجارية من المخاطر السيبرانية**، (أطروحة دكتورا)، قسم القانون الخاص كلية القانون، جامعة ميسان، العراق، ص 39.

50. أميرة بن مخلوف، (2015-2016)، **آليات الحوكمة لإدارة المخاطر المصرفية وتعزيز الاستقرار المالي**، (أطروحة دكتورا)، قسم الاقتصاد كلية العلوم الاقتصادية والتجارية وعلوم التسيير جامعة العربي بن مهيدي، أم البواقي، الجزائر، 172-173.

51. إيمان يحيى حمدان، (2021)، **الهجمات السيبرانية في ضوء القانون الدولي الإنساني**، (أطروحة دكتورا)، قسم القانون الدولي الإنساني، الجامعة الافتراضية السورية، سوريا، ص 26-27.

52. بوجلخة إبراهيم، (2022-2023)، **الاستقرار المالي للبنوك الإسلامية في ظل الأزمات المالية العالمية مقارنتها بالبنوك التقليدية**، (أطروحة دكتورا)، قسم الاقتصاد كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة محمد خيضر، بسكرة، الجزائر، ص13.

53. ذهبي ريمة، (2012-2013)، **الاستقرار المالي النظامي: بناء مؤشر تجميعي للنظام المالي الجزائري للفترة 2003-2011**، (أطروحة دكتورا)، قسم الاقتصاد كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة قسنطينة 2، الجزائر، ص 26-27.

54. سهيلة قطاف، (2019-2020)، **دور أنظمة الإنذار المبكر في التنبؤ بالأزمات المالية حالة أزمة جنوب شرق آسيا 1997 مع اقتراح نظام إنذار مبكر لأزمة محتملة بالجزائر**، قسم الاقتصاد، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة الجزائر 3، ص 52-53.

55. عبد الرحمان بن ساعد، (2013-2014)، **اتجاهات وآليات الاستقرار المالي العالمي في أعقاب الأزمة المالية العالمية**، (اطروحة دكتورا)، قسم التسيير، كلية العلم الاقتصادية والتجارية وعلوم التسيير، جامعة الجزائر 3، ص 91.

56. لعصامي آمنة، (2020-2021)، **تأثير المتغيرات الاقتصادية الكلية على مؤشرات الأسواق المالية العربية دراسة حالة السوق المالية السعودية وبورصة عمان خلال الفترة 2000-2018**، (أطروحة دكتورا)، قسم الاقتصاد، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة فرحات عباس، سطيف 1، الجزائر، ص 49-50-51.

57. لينة خالد فخر الدين وصفا جاسم سعيد، (2022)، **دور الاستقرار المالي في تطور القطاع المصرفي**، (رسالة ماجستير)، قسم العلوم المالية والمصرفية، كلية الإدارة والاقتصاد، جامعة الموصل، العراق، ص 06.

58. محمد رحيم، (2023-2024)، **التحديات الجديدة للأمن الدولي التهديدات السيبرانية**، (أطروحة دكتورا)، قسم العلاقات الدولية، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر3، ص8-9.

59. مصطفى بوبكر، (2014-2015)، **الاستقرار المالي في إطار مقاربة الاحتراز الكلي حالة النظام المصرفي الجزائري**، (أطروحة دكتورا)، قسم الاقتصاد، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة فرحات عباس، سطيف 1، الجزائر، ص 209.

60. نرمين محمد غسان الحموي، (2016)، **نموذج مقترح للتنبؤ المبكر بالفشل المالي في المصارف السورية الخاصة**، (أطروحة دكتورا)، قسم المصارف والتأمين، كلية الاقتصاد، جامعة دمشق، ص42.

61. هاجر بوديار، (2022-2023)، **دور البنوك المركزية في تحقيق الاستقرار المالي دراسة حالة بنك الجزائر 1962-2023**، (أطروحة دكتورا)، قسم الاقتصاد كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة شبوط إبراهيم، الجزائر، ص 52.

د. المحاضرات والمؤتمرات:

62. أحمد شفيق الشاذلي، (2014)، **الإطار العام للاستقرار المالي ودور البنوك المركزية في تحقيقه**، صندوق النقد العربي، ص13.

63. أكبر عبد الرحمانوف، (2019)، **تحليل القوى الخمس لشركة Target corporation**، كلية اللوجستيات، جامعة إينها، أوزباكستان، ص02.

64. البحري عبد الله وصاري علي، (2015)، **أنظمة الإنذار المبكر بالأزمات المالية ومدى سلامة النظام المصرفي الجزائري**، قسم الاقتصاد كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة أحمد دراية، أدرار، الجزائر، ص 03.

65. غاري شيناسي، (2005)، **الحفاظ على الاستقرار المالي**، قضايا اقتصادية، إدارة العلاقات الخارجية بصندوق النقد الدولي، ص 05.

66. حوامد خولة وجغبلو كريمة، (2023)، **أبعاد الأمن السيبراني والتحديات المرتبطة به مقاربة مفاهيمية**، الإطار القانوني الدولي للأمن السيبراني، ص03.

67. سليم دحمان، (2017-2018)، **أثر التهديدات السيبرانية على الأمن القومي الولايات المتحدة الأمريكية(2001-2017)**، ص33.

68. عادل عبد العزيز السن، (2015)، **دور الشمول المالي في تحقيق الاستقرار والنمو الاقتصادي**، جامعة الدول العربية، ص 31.

69. فاطمة بنت محمد بن سابق القحطاني، (2022)، **استراتيجيات الأمن السيبراني وتطبيقها بالتخطيط الاستراتيجي لمواجهة الإرهاب الالكتروني**، المؤتمر الدولي لمكافحة الإرهاب الالكتروني، ص125.

70. محمد يسر برنيه وغسان أبو رميس، (2015)، **العلاقة المتداخلة بين الاستقرار المالي والشمول المالي**، صندوق النقد العربي، ص54.

71. ميلاد سالم المختار مغراف وعبد الله صالح أحمد المطاع، (2025)، **الذكاء الاصطناعي ودوره في الحد من الهجمات السيبرانية**، جامعة بني وليد للعلوم الإنسانية والتطبيقية، طرابلس، ص77.

72. نورس فرحان كاظم، (2025)، **الأمن السيبراني مفهومه وتاريخه**، قسم هندسة الاتصالات والإلكترونيك، جامعة الكوفة، العراق، ص01.

ثانيا. المراجع باللغة الأجنبية:

-Article:

73 . Antoine bouveret، (**2018**)، **cyber risk for the financial sectors a framework for quantitative assessment**، strategy and policy and review departement، IMF working paper، page 9.

74. Alaa alsaeed،(2021) ، The **cyber attack on saudia aramco in 2012**، Asian journal of engineering and applied technology، united state، volume 10، issue 02، p 25-26.

75. Francisco jose herrera luque، (2021)، **cyber risk as a threat to financial stability**، espanya، p 191.

76. Frank adelman and jennifer elliote، (2020) ، IMF **STAFF disussion NOTE**، p 10.

77. Jin lai and philip chin، (2021)، **cyber security strategy for hong kong financial services industry financial services developement council**، p 14-16.

78. Mahich kumar jain، (2023)، **cyber security for a safer financial system central bankers speeches**، p 4.

79. Naser alshakoori and ahmed alkenaizi and ebrahim nadeem، (2016)، **business strategies of discount retailers**: **A comparative study of target corporation and costco wholsale**، international journal of reasearch in management economic and commerce، bahrain، volume 6، issue 6، p 21.

80. Cyat29labs، (2014)، **the untold story targeted attack step by step**، target corporation، new york، p 08.

81. Saba ajmal، (2019)، **reasearch project in finance target corporation lindewood university**، p15.

82. Sean stadtenberg and adam steinan and kyle terry،(2021)، **targeting a cyber attack a columbia university**: **case study**، school of international and public affairs columbia university، p 02.

83. Tara looie، (2015)، **porters five competitive forces analysis of target corporation**، business strategy p 06.

84. Target corporation، (2019)، **annual repport of 2019**، new york، p 16.

85. Xiangyua pan، (2022)، **reasearch on evaluation if target corporate and its stocks**، BCP business and management، california، volume 28 p 167.

86. without writer، (2014)، **kill chain analysis of the 2013 target data breach**،commerce and science and transportaion،p 13

87. Xian sun، (2025)، **target breach**: **case study assistant professor in finance cary business**، school johns hopkins university، p 4-5.

88. Xia and kui xe and ke tian، (2023)، **target hack**: **An analysis of the** target data breach and lessons learned، p 04.

ثالثا: المواقع الالكترونية

89. https://corporate.target.com

90. https://corporate.target.com/products-services

91. /https://www.organimi.com

92. /https://www.questionpro.com

93. https://bakkah.com/ar

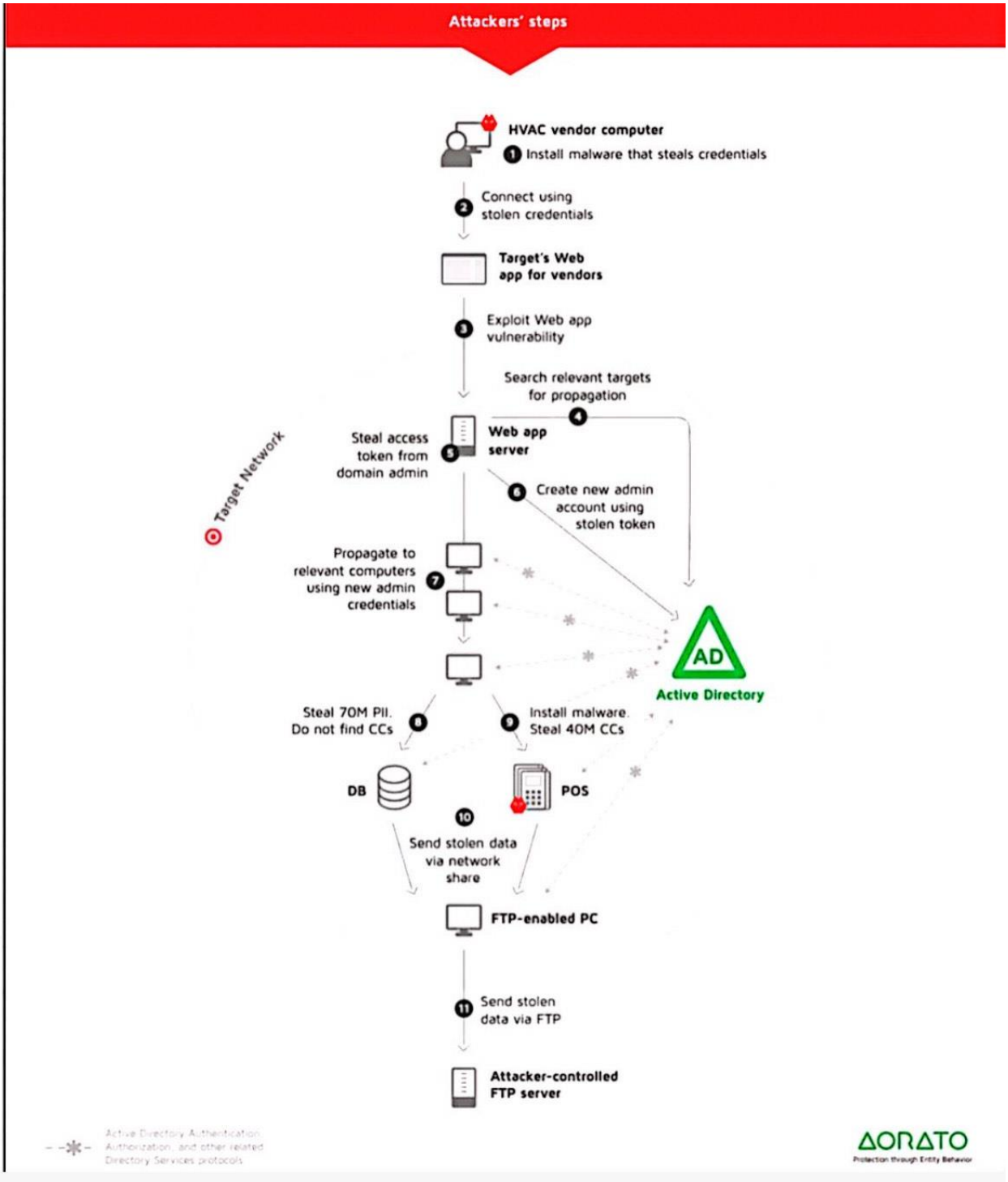
94. /https://smtcenter.net

95. /https://almsaey.akhbarelyom.com

96. /https://www.frameworksec.com

قائمة الملاحق

الملحق رقم (01): كيفية تنفيذ الهجوم السيبراني على شركة Target



الملحق رقم (02): التصريح الشرفي للطالبة هناء بوزيان

ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ماي 2020 .....
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،
السيد(ة): بوزيان هناء ..... الصفة: طالب، أستاذ، باحث ..... طالبة .....
الحامل(ة) لبطاقة التعريف الوطنية رقم 205885545 ..... والصادرة بتاريخ 2020/06/10 .....
المسجل(ة) بكلية / معهد العلوم الاقتصادية ..... قسم مالية وتجارة دولية .....
والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،
عنوانها: دور الأمن السيبراني في تعزيز الاستقرار المالي دراسة حالة لسنة 2023 تغطي الفترة 2012 - 2022 .....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 2025/05/25 .....

توقيع المعني (ة)
Bouziane

الملحق رقم (03): التصريح الشرفي للطالبة منال بوزرقون

ملحق بالقرار رقم ....1082.... المؤرخ في 27 2020

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): منال بوزرقون الصفة: طالب، أستاذ، باحث ... طالب .....

الحامل(ة) لبطاقة التعريف الوطنية رقم 209808776 والصادرة بتاريخ 2023-11-20

المسجل(ة) بكلية / معهد العلوم الاقتصادية قسم التجارية

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: مساهمة الإدخار السيراني في تعزيز الاستثمار المالي دراسة حالة سوق الجزائر

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 2025.12.06

توقيع المعني (ة)

منال بوزرقون

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد خيضر–بسكرة بسكرة في: 2025/05/27

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

قسم العلوم التجارية

إذن بالإيداع

أنا الممضي أسفله الأستاذ: بن ابراهيم الغالي.

الرتبـــة: أستاذ التعليم العالي.

قسم الارتباط: قسم العلوم التجارية.

أستاذ مشرف على مذكرة ماستر الطلبة (ة):

1. بوزيان هناء؛
2. بوزرقون منال.

الشعبة: العلوم التجارية

التخصـــص: مالية وتجارة دولية.

بعنـــوان: مساهمة الأمن السيبراني في تعزيز الاستقرار المالي

دراسة حالة شركة تارقات TARGET

ارخص بإيداع المذكرة المذكورة.

إمضاء الاستاذ المشرف

.

الأستاذ الدكتور/ بن ابراهيم الغالي

Prof.Dr/ BENBRAHIM ELGHALI