جامعة غرداية

كلية العلوم الاقتصادية و التجارية وعلوم التسيير

قسم علوم التسيير

بالتعاون مع مخبر الدراسات التطبيقية في العلوم المالية والمحاسبة

ينظمون ملتقى وطني (حضوري/ عن بعد) بعنوان:

" مخاطر الهندسة الاجتماعية ومتطلبات تحقيق الأمن المجتمعي

للمؤسسات الاقتصادية"، يوم 04 ماي 2025.

مداخلة بعنوان:

التحول الرقمي ومتطلبات الامن السيبراني ـ مراجعة أدبية ـ

من إعداد الباحثين :

- د. مصباح اسماعيل، جامعة غرداية.، mosbah.smail@univ-ghardaia.edu.dz
- د. بن قطاية الحسين، جامعة غرداية، hocineb88@gmail.com .

من خلال المحور رقم: 3

الملخص:

تهدف الدراسة الى ابراز دو التحول الرقمي في تحقيق الامن السبراني حيت تم الاعتماد على المنهج الوصفي من خلال تقديم عرض لمراجعة الدراسة السابقة والوقوف على المناهج المتبعة واهم النتائج المستخلصة منها وتم تقديم مفاهيم حول متغيرات الدراسة وتم عرض للعلاقة بين التحول الرقمي والامن السيبراني كما تم الإشارة الى اهم متطلبات التحول الرقمي لتحقيق الامن السيبراني

الكلمات المفتاحية: الرقمنة، التحول الرقمي ، الامن السيبراني.

Abstract:

The study aims to highlight the role of digital transformation in achieving cybersecurity. The descriptive method was adopted by presenting a review of previous studies and examining the methodologies used and the main findings derived from them. Key concepts related to the study variables were also introduced, along with an overview of the relationship between digital transformation and cybersecurity. Additionally, the study pointed out the main requirements of digital transformation necessary to ensure effective cybersecurity.

Keywords: Digitization, Digital Transformation, Cybersecurity

1. مقدمة:

يشهد التعليم العالي في السنوات الأخيرة تطورًا كبيرًا بفعل اعتماد تقنيات التحول الرقمي، وهو ما غيّر من طريقة تسيير الجامعات وأسلوب تقديم المعرفة. فقد أصبحت الأنظمة الرقمية تحتل مكانة محورية في مختلف الوظائف الجامعية مثل التدريس، البحث العلمي، التقييم، وأرشفة البيانات. إلا أن هذا التحول فرض تحديات جديدة، أبرزها تلك المتعلقة بالأمن السيبراني، نتيجة لزيادة تعرض المؤسسات لهجمات إلكترونية تهدد سرية البيانات وسلامة الخدمات.

وبناء على ما سبق نطرح الإشكالية التالية:

ما دور التحول الرقمي في تحقيق الامن السيبراني؟

وبناء على الإشكالية السابقة نطرح الفرضية التالية:

يلعب التحول الرقمي دوا هاما في تحقيق الامن السيبراني.

اهمية الموضوع

تبرز أهمية هذا الموضوع في كونه يتناول أحد أبرز التحديات التي تواجه المؤسسات في العصر الرقمي. فالتحول الرقمي لم يعد خيارًا بل واقعًا يفرض نفسه، ومعه تتزايد التهديدات السيبرانية. من هنا، تصبح دراسة متطلبات الأمن السيبراني ضرورة لضمان استمرارية المؤسسات، وحماية بياناتها، والحفاظ على سمعتها وثقة عملائها.

كذلك، فإن هذا الموضوع يجمع بين بعدين متكاملين: التطور التكنولوجي، والحماية الأمنية. وهذا ما يجعله موضوعًا حيويًا للباحثين وصناع القرار على حد سواء.

أهداف الدراسة

- توضيح مفهوم التحول الرقمي ومجالات تطبيقه داخل المؤسسات.
- إبراز تطور مفهوم الأمن السيبراني وتوسع نطاقه.
- تحليل العلاقة بين الرقمنة وظهور متطلبات أمنية جديدة.
- استعراض أبرز ما ورد في الأدبيات حول سبل التكيف مع التهديدات السيبرانية.
- تقديم توصيات مبدئية حول سبل بناء أنظمة أمنية فعالة في ظل التحول الرقمي.**الم**

مراجعة ادبية:

تُعد مراجعة الأدبيات من المكونات الأساسية في أي عمل بحثي أكاديمي، إذ تسهم في بناء الإطار النظري للبحث، وتساعد في تحديد موقع الدراسة الحالية ضمن الحقل المعرفي، فضلًا عن إبراز أوجه القصور التي لم تتناولها الدراسات السابقة. وفي سياق البحث حول "تأثير التحول الرقمي على متطلبات الأمن السيبراني" ضمن مجال تسيير المسار المهني للعاملين، فقد تم الاطلاع على مجموعة من الدراسات التي تُظهر بشكل مباشر أو غير مباشر العلاقة المتشابكة بين التحول الرقمي وتطور مفاهيم الأمن السيبراني داخل المؤسسات، لا سيما في البيئات الجامعية أو المؤسسات المالية ذات الطابع المعرفي.

تشير الدراسة الإقليمية حول واقع التحول الرقمي في مؤسسات التعليم العالي العربية إلى أن الرقمنة لم تكن رد فعل لجائحة كورونا فحسب، بل هي امتداد لسياسات تطوير بدأت قبلها بسنوات، حيث تم اعتماد أنظمة إدارية وأكاديمية قائمة على تكنولوجيا المعلومات لتحسين الجودة وضمان الاعتماد المؤسسي. وقد أوضحت الدراسة أن المؤسسات التي تبنّت خططًا استراتيجية وتنظيمية واضحة للتحول الرقمي، كانت الأقدر على التكيّف مع التحديات الأمنية السيبرانية. ومن هذا المنطلق،

يتضح أن التحول الرقمي لا يرتبط فقط بتطوير البنية التقنية، بل يتطلب أيضًا تكاملًا مع منظومات الحوكمة الأمنية، ما يؤسس لفهم أعمق حول كيفية تأثير التحول الرقمي على مكونات البيئة المهنية للعاملين في هذه المؤسسات، خاصة من حيث المهارات الأمنية المطلوبة.

أما دراسة تجربة الإمارات العربية المتحدة في مجال الأمن السيبراني كدعامة أساسية للتحول الرقمي في المنظمات الحكومية، فقد سلطت الضوء على نجاح الدولة في بناء بيئة سيبرانية قوية مدعومة بتشريعات مرنة واستراتيجيات استباقية، ما ساعد على تحقيق تحول رقمي سلس. وتُبرز هذه الدراسة الدور الحيوي الذي تلعبه القيادة المؤسسية والرؤية الحكومية الواضحة في إدماج الأمن السيبراني ضمن استراتيجيات التسيير الشامل، وهو ما ينعكس بالضرورة على ممارسات الموارد البشرية من حيث استقطاب وتكوين الكفاءات المؤهلة للتعامل مع بيئة رقمية عالية المخاطر.

وفي السياق المالي، توضح دراسة العلاقة بين الأمن السيبراني والشمول المالي في ظل التحول الرقمي، أن الاعتماد المتزايد على الخدمات الرقمية عزز من فرص الوصول المالي، ولكنه في الوقت ذاته فتح المجال أمام تهديدات سيبرانية معقدة، تهدد استقرار النظام المالي. هذا التوتر بين الابتكار الرقمي والتهديدات السيبرانية يكشف عن فجوة مؤسساتية تتعلق بغياب توازن بين التوسع الرقمي ومواكبة الإجراءات الأمنية، وهو ما يتطلب تطوير المهارات المهنية للعاملين في هذه القطاعات بما يتلاءم مع مستجدات الأمن السيبراني.

ومن جهة أخرى، تركز دراسة الأمن السيبراني في المؤسسات المالية الإسلامية بفلسطين على العلاقة بين درجة نضج التحول الرقمي ومدى الجاهزية السيبرانية للعاملين، مشيرة إلى وجود علاقة طردية بين مستوى التهديدات السيبرانية وتطور البنية الرقمية للمؤسسة. كما بينت أن تدريب العاملين على المهارات السيبرانية يمثل عاملاً حاسمًا في حماية المكاسب الرقمية. هذا البعد الوظيفي يعزز من أهمية دمج الأمن السيبراني ضمن مسارات تطوير الكفاءات المهنية، ويدعم الطرح الذي يرى في التحول الرقمي محفزًا لإعادة هيكلة ممارسات تسيير المسار المهني.

أما في السياق الجزائري، فقد تناولت إحدى الدراسات أهمية حوكمة الأمن السيبراني كشرط لضمان التحول الرقمي الآمن للخدمة العمومية، موضحة أن غياب استراتيجيات فعالة يعوق تطوير القدرات السيبرانية. وقد دعت الدراسة إلى الاستفادة من التجارب الدولية وتطوير كفاءات بشرية ذات مهارات عالية في مجال الأمن السيبراني، ما يعكس بوضوح أن الأمن السيبراني لم يعد مجرد تقنية بل أصبح مكونًا جوهريًا في تخطيط وإدارة الموارد البشرية. كذلك، أظهرت دراسة حول جامعة بني سويف أن أعضاء هيئة التدريس يتفقون على مجموعة من المتطلبات التقنية والبشرية لتحقيق الأمن السيبراني، مما يعكس وعيًا متزايدًا بأهمية تضمين هذه الأبعاد في إدارة الموارد داخل المؤسسات التعليمية.

ورغم تنوع السياقات والمؤسسات التي تناولتها هذه الدراسات، فإنها تشترك في التأكيد على أهمية ملاءمة البنية البشرية مع التحولات الرقمية، وضرورة رفع كفاءات العاملين لمواكبة التطورات في مجال الأمن السيبراني. غير أن معظم الدراسات ركزت على الجوانب التقنية والتنظيمية، دون الغوص العميق في كيفية تأثير هذه التحولات على تسيير المسار المهني للعاملين بشكل مباشر، مثل استراتيجيات التكوين، الترقية، أو إعادة التأهيل الوظيفي في ضوء التحديات السيبرانية. كما أن بعض الدراسات اكتفت بتوصيف الواقع دون تقديم أطر تحليلية تمكن من بناء نماذج متكاملة للمواءمة بين التحول الرقمي والأمن السيبراني وتسيير المسارات المهنية.

بناء على ما سبق، تسعى الدراسة الحالية إلى سد هذه الفجوة المعرفية من خلال تحليل متكامل للعلاقة بين التحول الرقمي ومتطلبات الأمن السيبراني، وانعكاساتها على تسيير المسار المهني للعاملين، وذلك عبر الربط بين التحول في البيئة التقنية وتغير متطلبات الكفاءة والتأهيل المهني داخل المؤسسات. وتسعى الدراسة إلى تقديم نموذج نظري تطبيقي يساعد على فهم ديناميات التفاعل بين هذه المتغيرات، مما يسهم في تطوير سياسات فعالة لإدارة المسارات المهنية في عصر الرقمنة.

1.2 ماهية الرقمنة:

يعد تبني الرقمنة حتمية ينبغي على كافة المؤسسات اعتمادها في مختلف المهام والأعمال، باعتبارها "العملية التي يتم عن طريقها تحويل المعلومات من الشكل التقليدي الحالي إلى الشكل الرقمي سواء كانت صور أو بيانات نصية أو أي شكل آخر (حفطاري و حمزاوي، 2016، صفحة 255) ، و تعد عملية لتحويل البيانات إلى الشكل الرقمي من خلال معالجتها بواسطة الحاسب الإلكتروني في سياق نظم المعلومات عادة ما تشير الرقمنة الى تحويل (النصوص، المطبوعات الو الصور....) الى إشارات ثنائية (ساسي و هاني، 2021، صفحة 26).

وعرفت الرقمنة على أنها "استخدام التكنولوجيا من أجل تحسين الجدري للأداء والوصول إلى أهداف المؤسسة (نعموني، 2020، صفحة 562).

بناء على ما سبق يمكن تعريف الرقمنة على أنها أسلوب لتحسين أداء المؤسسة، من خلال إدراج التكنولوجيا الحديثة في تحويل الأعمال الادارية من الشكل التقليدي الى الشكل الرقمي أي عرض انشطة وخدمات المؤسسات السياحية في شكل رقمي بواسطة استخدام التكنولوجيا الحديثة وتطبيقاتها.

2.2 أبعاد تكنولوجيا الرقمية:

يعتمد أغلب الباحثين في دراسة البنية التحتية التكنولوجية على الأبعاد التالية:

الأجهزة والمعدات: تعد الوسيلة الأساسية لتكنولوجيا المعلومات والاتصال، يتم من خلالها إدخال البيانات ومعالجتها وتخزينها في قواعد البيانات واسترجاعها عند الحاجة إليها.

البرمجيات: هي مجموعة من التعليمات والأوامر المعقد التي توجه المكونات المادية للحاسوب للعمل بطريقة معينة بغرض الحصول على النتائج المطلوبة.

قواعد البيانات: وهي أماكن محددة يتم على مستواها حفظ المعلومات.

الاتصال والشبكات: إن الشبكات والاتصالات عنصران ضروريان مرتبطان مع بعضهما البعض ويكمل أحدهما الأخر، فلا يمكن بناء شبكات دون توفير بيئة جيدة للاتصالات لخدمة هذه الشبكات. الاتصال هو عملية تفاعل مشترك بين طرفين لتبادل فكرة أو خبرة معينة عن طريق وسيلة ما، أما الشبكات فهي مجموعة من الحواسيب مرتبطة مع بعضها البعض بخطوط اتصال بحيث يمكن لمستخدميها المشاركة في الموارد المتاحة ونقل المعلومات فيما بينهم (لالوش، 2010، صفحة 54).

المورد البشري: يعتبر الأفراد أهم العناصر المكونة لنظام المعلومات القائم على الحاسوب ويتكون أفراد نظم المعلومات من الذين يقومون بإدارة، تشغيل البرمجة وصيانة نظام المعلومات (يعد كل مستخدم للحاسوب من أفراد نظام المعلومات) (بن زيادي، 2016، صفحة 143).

أنواع التحول الرقمي : (قرايري ، 2023)

2. التحول الرقمي للحكومة ركز هذا النوع على تحسين التقديم الخدمات الحكومية المواطنين وتبسيط الإجراءات الإدارية يتم ذلك من خلال تطبيقات الهاتف المحمول والمواقع الالكترونية التي تهدف إلى تعزيز سهولة الوصول والحسين البحرية المستخدم.

2 التحول الرقمي للعمليات يستهدف النوع تحسين كفاءة العمليات الداخلية للمؤسسات غير اعتماد التكنولوجيا الرقمية يتضمن ذلك ألسنة العمليات وتحليل البيانات للتحقيق الكفاءة التشغيلية وتعزيز التحسين المستمر.

3. التحول الرقمي للإنتاج والتصنيع يتمثل في استخدام التكنولوجيا الرقمية لتحسين العمليات الإنتاجية والعزيز الابتكار في الصناعات التقليدية تشمل هذه الجهود استخدام الروبوتات الذكاء الاصطناعي، وتحليل البيانات بهدف التحقيق كفاءا أعلى وجود محشية
4. التحول الرقمي لسلسلة التوريد يهدف إلى تحسين إدارة سلسلة التورية من خلال تعزيز عمليات الشحن والتوزيع يشمل ذلك استخدام تقنيات الطب التحليل، والتواصل الرقمي للتعزيز الكفاءة والتعاون مع الموردين.
5. التحول الرقمي للقطاع المالي يسعى هذا النوع إلى تحسين الخدمات المالية وتسهيل العمليات المصرفية. يشمل ذلك التطبيقات المصرفية المحافظ الرقمية، وتكنولوجيا الدفع الإلكتروني بهدف توفير الحرية مالية مبتكرة وسلسة
6. التحول الرقمي للتعليم يهدف إلى تطوير الحرية التعلم من خلال دمج التكنولوجيا الرقمية في وسائل التعليم من ذلك منصات التعلم عن بعد الطبقات التعليم الإلكتروني، وتوفير محتوى تعليمى رقمي حديث التحول الرقمي للسياحة والضيافة يركز على تحسين الحرية السياح والمسافرين من خلال تسهيل عمليات الحجز والإقامة يشمل ذلك استخدام تقنيات الواقع المعزز والتطبيقات السياحية الرقمية التعزيز الراحة والتفاعل مع الزوار.
7. التحول الرقمي للتسويق والمبيعات يعلمه على استخدام الوسائل الرقمية للتعزيز استراتيجيات التسويق والمبيعات يشمل ذلك التسويق عبر البريد الإلكتروني، وسائل التواصل الاجتماعي، والحرية التسوق الإلكتروني التقلبية احتياجات العملاء بشكل أفضل
8. التحول الرقمي لتجربة العملاء يهدف هذا النوع إلى تحسين الفاعل العملاء مع المنتجات والخدمات من خلال توفير تجربة شخصية ومنيرة، يتم التحقيق ذلك باستخدام تحليلات البيانات وتقنيات الذكاء الاصطناعي لتلبية. توقعات العملاء بشكل أكثر دقة وفعالية .

خصائص التحول الرقمي: (عفيف، 2022)

- خصائص التحول الرقمي: تتمثل خصائص التحول الرقمي في الاعتماد بشكل كبير على الأصول غير الملموسة التي تشتمل على الملكية الفكرية وتطوير واستخدام البرمجيات والخوارزميات التي تحلل كمية كبيرة من البيانات الناتجة عن الأعمال التجارية على منصات الأنترنت، وكذلك المحتوى الإبداعي الذي يلعب دورا رئيسيا في الإنتاج أو تقديم الخدمات عبر الأنترنت؛
- إنشاء علاقات عبر الحدود للمسافات البعيدة مع العملاء دون الحاجة إلى تواجد مؤسسة دائمة في غيرها من الدول؛ مشاركة العملاء والمستخدمين في خلق القيمة حيث تستخدم المؤسسات المنصات الرقمية للتفاعل مع عملائها، من خلال تحليل سلوك العملاء وزيادة عائداتها مثل إعادة بيع البيانات؛
- إن المؤسسات التي تهيمن على الأعمال الرقمية غالبا ما تكون منصات تمكن الجانبين من التفاعل، ويمكن أن يكون الجانبان بالعين ومشترين للسلع أو الخدمات التقليدية، وفي هذه الحالة تكون هذه المؤسسات نشطاء يستفيدون من الانترنت لتقليل تكاليف المعاملات والبحث، ويمكنهم أيضا الربط بين المنتجين والمستهلكين وتزويد المستهلكين بخدمات مجانية؛

- التحول من الإدارة الورقية إلى الإدارة الرقمية أو الإلكترونية أو إدارة بدون أوراق، كالية جديدة للتسجيل أو للتخزين والاسترجاع ونقل المعلومات، مما يسهل من عملية اتحاد القرار ويزيد من سرعتها؛
- تميل المؤسسات الرقمية مثل مؤسسات التجارة الالكترونية والإعلانات عبر الأنترنيت والحوسبة السحابية إلى الاحتكار، وذلك بسبب تأثير الشبكة والحجم الكبير وقيود الاستخدام والأنظمة المتعددة الجوانب. يتميز التحول الرقمي بخصائص منفردة حيث أتاح للعالم سهولة الاتصال والتواصل وكسر الحدود الجغرافية حيث تستخدم.
- اهداف التحول الرقمي:
- هناك العديد من الأهداف العامة تتلخص بما يأتي
- عملية التحول الرقمي تهدف إلى دفع المؤسسات الى تبني نهج يتم عن طريقه وضع استراتيجية تحول واضحة واعطاء تطلع واضح عن التزام جميع اصحاب المصلحة
- التطور الشامل وسرعة وكفاءة العمليات والخدمات المالية وبأسعار معقولة للعملاء وبكل سهولة
- ممارسة الأعمال بشكل أكثر شفافية وبساطة في المعلومات وإظهارها إلى العملاء، المواطنين والموردين
- الحد من التكاليف العالية في التحويلات بين الدول
- تعظيم الكفاءة والشفافية في العمليات الحكومية التي تحد من الفساد
- تسريع التحويلات الاجتماعية والإنسانية التطور المتواصل وبناء المعرفة والخبرات
- التكنولوجيا الرقمية هدفها توضيح طريقة أداء العمليات التنظيمية والتوصل إلى مستويات مبتكرة والعمل على تطوير نماذج الأعمال وخدمات الإنتاج.

أهمية التحول الرقمي: (مختار، 2022)

- تحسين الكفاءة: يسهم التحول الرقمي في تسريع العمليات الإدارية والتشغيلية، وتقليل الأخطاء، وتحسين جودة الخدمات المقدمة. كما يساهم في تبسيط الإجراءات، مما يسهل على الجمهور الحصول على الخدمات بشكل أسرع وأكثر فعالية .
- تعزيز التنافسية تمكن المؤسسات التي تتبنى التحول الرقمي من تقديم خدمات مبتكرة وإبداعية تتجاوز الأساليب التقليدية، مما يمنحها ميزة تنافسية في الأسواق ويعزز قدرتها على خلق فرص جديدة ...
- تحسين تجربة العملاء: يتيح التحول الرقمي للمؤسسات جمع وتحليل البيانات بشكل دقيق، مما يساعدها على فهم احتياجات العملاء بشكل أفضل. ينعكس ذلك في تقديم خدمات محسنة وتجربة متكاملة تلبي توقعات العملاء بفعالية.
- تحقيق الشفافية يوفر التحول الرقمي أدوات تمكن المؤسسات من مراقبة الأداء في الوقت الفعلي، مما يعزز الشفافية ويزيد من وضوح العمليات. كما يسهل الوصول إلى المعلومات ويضمن وضوح الإجراءات لجميع الأطراف المعنية. خفض التكاليف: يساعد التحول الرقمي في تقليل التكاليف التشغيلية والجهد المبذول من خلال تحسين الكفاءة وتنظيم العمليات، مما يتيح للمؤسسات توفير الموارد واستثمارها في مجالات أخرى.

- تحقيق التنمية المستدامة بدعم التحول الرقمي تحسين قطاعات حيوية مثل التعليم، الصحة، والطاقة من خلال تقنيات مبتكرة تقلل من التأثير البيئي السلبي. كما يسهم في بناء.

مفهوم الامن السيبراني: (طواهير، 2023)

الأمن السيبراني مصطلح جاء من الكلمة اللاتينية (سايبر Cyber) ومعناها تخيلي أو افتراضي، ودرج استخدامها لوصف الفضاء الذي يضم الشبكات المحوسبة التي تعني فضاء المعلومات)، البعليكي، ٢٠٠٤، ٢٤٣)، ومنها اشتقت صفة السيبراني والسيبرانية Cybernetic وتعني علم التحكم الأوتوماتيكي، أو علم الضبط. وبهذا فإن الأمن السيبراني يعني أمن الفضاء المعلوماتي)، وبهذا فهو معني بالأمن المرتبط بشبكات الإنترنت، وكذلك شبكات الاتصالات وتختلف تعاريف الفضاء السيبراني حسب طبيعة كل دولة أو مؤسسة

4- تحديات الأمن السيبراني: (جغفل ، 2023)

يعتبر الأمن السيبراني تحديا خطيرا بالنسبة للقطاع المالي بسبب التوجه السريع نحو التحول الرقمي بهدف تحسين جودة الخدمات المالية وزيادة فرص الوصول المالي ضمن إستراتيجية تعزيز الشمول المالي وتتمثل هذه التحديات في العوامل التالية

نقص الوعي: إن الوعي لأهمية الأمن السيبراني بين الناس منخفضاً للغاية، ولا تستثمر العديد من الشركات في التدريب وتحسين الوعى العام بالأمن السيبراني.

الميزانيات غير الكافية والافتقار إلى الإدارة: يمنح الأمن السيبراني أولوية وميزانية منخفضة غالباً، ولا يزال تركيز الإدارة العليا على الأمن السيبراني منخفضاً في معظم البنوك، وتعطى مشاريع الأمن السيبراني أولوية منخفضة. قد يكون هذا لأن الإدارة العليا لا تكترث لتأثير تهديدات الأمن السيبراني.

ضعف أمن هوية الدخول والوصول الى الشبكات: إن إدارة هوية الدخول والوصول إلى الشبكات الإلكترونية هي العنصر الأساسي في الأمن السيبراني إذ أن اختراق واحد لهوية الدخول والوصول إلى الشبكة كاف لاختراق كل شبكة البنك وإلحاق الضرر بها.

زيادة برامج الفدية Ransomware: يتزايد خطر برامج الفدية حيث بدأ مجرمو الإنترنت في استخدام الأساليب التي تتجنب اكتشافهم بالتركيز على الملفات القابلة للتنفيذ ووضع الضرر فيها. الأجهزة المحمولة والتطبيقات اعتمدت معظم المؤسسات المصرفية الهواتف المحمولة كوسيلة لإجراء الأعمال، ومع زيادة قاعدة استخدام الأجهزة المحمولة وارتفاع حجم المعاملات عبرها، تصبح هذه الأجهزة هدفاً للمتسللين.

أنواع الامن السيبراني: (بن برغوثي ليلة، 2023)

في ضوء التعريفات المتنوعة للأمن السيبراني، يمكن تحديد أنواع مختلفة له، تتمثل في مايلي:

أمن الشبكات (Network Security) وفيه تتم حماية أجهزة الحاسوب من الهجمات التي قد يتعرض لها داخل الشبكة وخارجها، ومن أبرز التقنيات المستخدمة لتطبيق أمن الشبكات جدار الحماية الذي يعمل واقيا بين الجهاز الشخصي والأجهزة الأخرى في الشبكة، بالإضافة إلى أمن البريد الإلكتروني.

أمن التطبيقات (Application Securin) وفيه تتم حماية المعلومات المتعلقة بتطبيق على جهاز الحاسوب، كإجراءات وضع كلمات المرور، وعمليات المصادقة، وأسئلة الأمان التي تضمن هوية مستخدم التطبيق.

لأمن السحابي (Cloud Security) تعرف البرامج السحابية بأنها برامج تخزين البيانات وحفظها عبر الإنترنت، ويلجأ الكثير إلى حفظ بياناتهم عبر البرامج الإلكترونية عوضا عن برامج التخزين

المحلية، مما أدى إلى ظهور الحاجة إلى حماية تلك البيانات، فتعنى البرامج السحابية بتوفير الحماية اللازمة لمستخدميها.

الأمن التشغيلي (Operational Security) وهو إدارة مخاطر عمليات الأمن السيبراني الداخلي، وفيه يوظف خبراء إدارة المخاطر لإيجاد خطة بديلة في حال تعرض بيانات المستخدمين لهجوم إلكتروني، ويشمل كذلك توعية الموظفين وتدريبهم على أفضل الممارسات لتجنب المخاطر بالخطأ إلى نظام أمن إذا لم يتبع ممارسات أمان جيدة.

دواعي الاهتمام بالأمن السيبراني: (محمد توفيق، 2023)

ورغم أن الأمن السيبراني موجود منذ وجود الحاسوب نفسه، فقد بدأ هذا الموضوع يحظى باهتمام متزايدة وغير مسبوق على المستوى العالمي، وذلك بالنظر إلى:

أولاً. المخاطر التي تنطوي على التهديد الإلكتروني على مختلف نواحي الحياة (انواع الأمن السيبراني. بلا تاريخ حيث يمكن أن يتسبب في وقف قطاعات حيوية أو حتى تدميرها. ثانياً، تنوع هذه التهديدات المتعلقة بالأمن السيبراني: حيث تشمل:

- الجرائم الإلكترونية التي تشمل قيام أفراد أو مجموعات باستهداف النظم الإلكترونية من أجل مكاسب مادية أو الحصول على فدية مالية أو لخلق اضطراب وخلل فيها. ووفقاً لتقرير صادر عن موقع متخصص في هذا المجال، فإن معدل تكلفة الجرائم الإلكترونية لأي منظمة زادت بنسبة 23% عن العام الماضي وقد تكلف العالم 10 تريليونات دولار سنوياً بحلول 2025 وفقاً لتقرير آخر
- الهجمات السيبرانية التي تهدف عادة إلى جمع معلومات الدوافع سياسية أو لاستغلالها في تضليل الناخبين مثلاً، كما حصل في الانتخابات الرئاسية في الولايات المتحدة عام 2016، حيث خلصت التحقيقات إلى أن دولاً تدخلت إلكترونياً للتأثير في توجهات الناخبين ما ساهم بشكل أو بآخر في فوز أحد المرشحين وخسارة الآخر
- الإرهاب الإلكتروني، الذي يهدف إلى تقويض النظم الإلكترونية بهدف إحداث الرعب أو الخوف. والذي قد يستخدمه أفراد أو جماعات إرهابية أيضاً. باختصار، إن الأمن السيبراني مهم جداً، بل هو حيوي لأنه يحمي الأفراد والشركات والمؤسسات من أي تهديد إلكتروني محتمل فالتطور التكنولوجي الهائل ترك كثيراً من الناس والدول عرضة لهجمات إجرامية

اشكال تهديدات الامن

- البيانات غير المشفرة أحد التهديدات الشائعة التي تواجهها البنوك هو عندما تترك البيانات غير مشفرة، ويستخدم المتسللون أو مجرمو الإنترنت البيانات على الفور، مما يتسبب في مشكلات خطيرة يجب أن تكون جميع البيانات المخزنة على أجهزة الكمبيوتر في البنوك والمؤسسات أو عبر الإنترنت مشفرة بالكامل، مما يضمن أنه حتى في حالة سرقة البيانات، فقد لا يتمكن مجرمو الإنترنت من استخدام هذه البيانات.
- البرامج الضارة تستخدم أجهزة الكومبيوتر والأجهزة المحمولة في الغالب لإجراء المعاملات الرقمية مما يستوجب تزويدها بالحماية. وتشكل البرامج الضارة خطراً كبيراً على البنوك عندما تتم المعاملات عبر الشبكات الالكترونية والانترنت، تمر البيانات الحساسة عبر

الشبكات الالكترونية والانترنت، وإذا كان جهاز المستخدم يحتوي على برامج ضارة مثبتة فيه دون أي حماية يمكن أن تشكل البرامج الضارة تحديداً خطيراً لشبكة البنك.

- خدمات الطرف الثالث: تلجأ العديد من البنوك والمؤسسات إلى الجهات الخارجية من البائعين وغيرهم (خدمات الطرف الثالث بهدف خدمة عملائهم بشكل أفضل، وإذا لم يكن لدى هؤلاء الجهات الخارجية إجراءات صارمة للأمن السيبراني، فقد يواجه البنك مشاكل أمنية من خدمات الطرف الثالث.
- الانتحال : إنه أحد أحدث أشكال التهديدات الإلكترونية التي تواجهها البنوك، حيث ينتحل مجرمو الإنترنت عنوان موقع المصرف على الويب URL بموقع ويب مشابه للموقع الأصلي ويعمل بالطريقة عينها، وعندما يقوم المستخدم بإدخال بيانات تسجيل الدخول الخاصة به على الموقع المزيف، يتم سرقة بيانات تسجيل الدخول من قبل هؤلاء المجرمين واستخدامها لاحقاً. وتتزايد حدة هذا التهديد مع استخدام تقنيات انتحال جديدة من قبل مجرمي الإنترنت.

العلاقة بين التحول الرقمي ومتطلبات الأمن السيبراني

تشير الأدبيات إلى أن هناك علاقة طردية بين مستوى التحول الرقمي وحجم متطلبات الأمن السيبراني. فكلما تبنت المؤسسات أدوات رقمية أكثر تعقيدًا، ظهرت ثغرات جديدة وازدادت الحاجة لتأمينها. على سبيل المثال، اعتماد المؤسسات على تقنيات مثل إنترنت الأشياء (IoT) يجعلها عرضة لهجمات تستهدف أجهزة غير محمية بالشكل الكافي.

من جهة أخرى، تؤدي سرعة التحول الرقمي إلى صعوبة مواكبة التغيرات الأمنية، ما يتطلب من المؤسسات وضع استراتيجيات أمنية مرنة وقابلة للتكيف. وقد بينت دراسات حديثة مثل تلك التي قام بها Bada & Sasse (2019) أن المؤسسات التي لم تدمج الأمن السيبراني منذ المراحل الأولى للتحول الرقمي تعاني من فجوات كبيرة في أنظمتها.

علاوة على ذلك، تشير البحوث إلى أن التحول الرقمي لا يغيّر فقط طبيعة المخاطر، بل يوسع نطاقها ليشمل شركاء خارجيين، ومزودي خدمات، وسلاسل التوريد الرقمية، ما يجعل من التنسيق الأمني عبر الشبكات عاملاً أساسيًا.

.4المتطلبات الجديدة للأمن السيبراني في ظل التحول الرقمي

تشير الأدبيات إلى ظهور عدة متطلبات جديدة، من أبرزها:

- **المرونة السيبرانية :**وتعني قدرة المؤسسة على الصمود أمام الهجمات والتعافي بسرعة. لم يعد يكفي منع الهجوم، بل يجب أيضًا الاستعداد لما بعده، من خلال خطط استجابة مدروسة وتمارين محاكاة.
- **إدارة الهوية والصلاحيات :(IAM)** من المهم تحديد من يستطيع الوصول إلى ماذا، مع مراقبة دقيقة لكل الأنشطة، باستخدام أساليب تحقق متعددة العوامل (MFA) لضمان سلامة الوصول.
- **التحليل السيبراني والتنبؤ :**لا يقتصر الأمر على مراقبة الحوادث، بل يتطلب توظيف تقنيات التحليل التنبئي التي تعتمد على الذكاء الاصطناعي والتعلم الآلي لاكتشاف التهديدات قبل وقوعها.
- **حماية البيانات الضخمة :**أصبحت المؤسسات تخزن كميات هائلة من البيانات، ما يتطلب بنية حماية متقدمة تشمل التشفير، وسياسات التحكم في الوصول، وتدقيق الاستخدام.

- **التدريب والتوعية :**العنصر البشري يظل نقطة ضعف رئيسية. لذلك، لا بد من نشر ثقافة الأمن الرقمي بين العاملين، وتقديم برامج تدريبية دورية تحاكي سيناريوهات الهجمات.
- **التكامل الأمني مع نظم التحول الرقمي :**يجب دمج اعتبارات الأمن ضمن البنية الأساسية الرقمية من البداية، وعدم النظر إليها كإضافة لاحقة.

قائمة المراجع:

- أسماء بن زيادي. (01 12, 2016). دور عناصر نظام المعلومات في تفعيل إدارة المعرفة واقع المؤسسة الاقتصادية الجزائرية. مجلة الأقتصاد و المناجمنت، 15(02)، الصفحات 140-163.
- بن برغوثي ليلة. (2023). الامن السيبراني و حماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي و الذكاء الاصطناعي.
- جغفل , ج .(2023) .الأمن السيبراني والشمول المالي في ظل التجول الرقمي للقطاع المالي.
- خديجة مختار. (2022). التحول الرقمي في الجزائر في ظل جائحة كوفيد19.
- سفيان ساسي، و أمينة هاني. (30 11, 2021). تجربة الجزائر في رقمنة قطاع التعليم العالي في ظل جائحة كورونا (العراقيل والتحديات). *مجلة التميز الفكري للعلوم الاجتماعية و الانسانية، 03*(03)، الصفحات 194-202.
- سمير حفطاري، و سهى حمزاوي. (01 04, 2016). الرقمنة ومدى تأثيرها على الفعالية التنظيمية تثمين رأس المال البشري في المؤسسة بين الإدارة الكلاسيكية والالكترونية. *مجلة الباحث الاجتماعي، 12*(01)، الصفحات 253-270.
- صلاح الدين محمد توفيق. (2023). متطلبات تحقيق الأمن السيبراني بالجامعات المصرية فى ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس (جامعة بنها أنموذجاً).
- طواهير, ع .(2023) .استراتيجيات الأمن السيبراني كتحدي للتحول الرقمي بالمنظمات الحكومية مع الإشارة لتجربة دولة الإمارات العربية المتحدة.
- عفيف, ه .(2022) .الاتجاه نحو التحول الرقمي: حتمية أو خيار؟.
- غنية لالوش. (01 08, 2010). البنية التحتية لتكنولوجيا المعلومات في ظل الاقتصاد الرقمي. *مجلة دراسات اقتصادية، 04*(02)، الصفحات 46-59.
- قرايري , ن .(2023) .التحول الرقمي في قطاع الأعمال: مفاهيم أساسية.
- مريم نعموني. (31 12, 2020). تأثير الثقافة التنظيمية على نجاح التحول الرقمي في المؤسسة. *مجلة معهد العلوم الإقتصادية، 23*(02)، الصفحات 561-575.