STARDOM UNIVERSITY

جامعة ستاردوم

المجلة العلمية للدراسات الانسانية و الاجتماعية

مجلة ستاردوم العلمية للدراسات الإنسانية و الاجتماعية

تصدر يشكل ربع سنوي من جامعة ستاردوم

المجلد الثاني-العدد الثاني- لعام 2024م

رقم الإيداع الدولي : ISSN 2980-3772

الأمن السيبراني والتحديات المُستقبلية

الباحث: أيمن علي أوغلو

ملخص

هدفت الدراسة لبيان التحديات التي قد تُحدق بالأمن السيبراني في المُستقبل، حيث استخدم الباحث المنهج الوصفي والتحليلي، ويشمل الأمن السيبراني مجموعة من السياسات والتقنيات التي تهدف إلى الوقاية من الهجمات والحفاظ على سلامة الأنظمة الرقمية، بالإضافة إلى بناء حاجز ضد التهديدات السيبرانية المتزايدة. ويتم ذلك من خلال استخدام برامج مكافحة الفيروسات، وجدران الحماية، وتحديثات البرمجيات. وقد توصلت الدراسة إلى ان في جميع جوانب الحياة اليومية يتطلب الأمان السيبراني تكاملًا شاملًا لتقديم حماية فعّالة، حيث يعتبر تحقيق توازن بين هذه الأنواع العديدة أمرًا حاسمًا لضمان سلامة البيئة الرقمية. وستستمر التهديدات السيبرانية في التطور والتقدم في السنوات القادمة مع تقدم التكنولوجيا. ويشير خبراء الأمن إلى إمكانية ظهور تحديات وتهديدات جديدة في المستقبل. وأوصى الباحث بالتأكيد على المراقبة المستمرة وفي الوقت الفعلي لجميع الموارد الإلكترونية، التي قد يمكن التعامل معها في أي وقت. ووضع استراتيجيات لاستعادة البيانات واستئناف العمليات بشكل سريع بعد وقوع حوادث الأمان السيبراني.

الكلمات المفتاحية: الأمن، السيبرانية، الأمن السيبراني، التحديات، التحديات المستقبلية.

Abstract

The study aimed to show the challenges that may beset cybersecurity in the future, where the researcher used the descriptive and analytical approach, and cybersecurity includes a set of policies and technologies aimed at preventing attacks and maintaining the integrity of digital systems, in addition to building a barrier against increasing cyber threats This is done through the use of antivirus programs, firewalls, and software updates The study found that In all aspects of daily life, cybersecurity requires comprehensive integration to provide effective protection, as balancing these many types is crucial to ensuring the safety of the digital environment and cyber threats will continue to evolve and advance in the coming years as technology advances and security experts point to the possibility of new challenges and threats emerging in the future. The researcher recommended emphasizing the monitoring Continuous and real-time for all electronic resources, which may be handled at any time. Develop strategies for data recovery and rapid resumption of operations after cybersecurity incidents.

Keywords: Security, Cyber, Cybersecurity, Challenges, Future Challenges.

المقدمة:

لا شك أن الأمن السيبراني يعد الدرع الرقمي الذي يحمي العالم المتصل بالإنترنت. وفي عصر تكنولوجيا المعلومات، حيث تتداخل حياتنا مع الشبكة العنكبوتية، يصبح الأمن السيبراني أمرًا حيويًا للحفاظ على الخصوصية وأمن البيانات والمعلومات.

ويشمل الأمن السيبراني مجموعة من السياسات والتقنيات التي تهدف إلى الوقاية من الهجمات والحفاظ على سلامة الأنظمة الرقمية، بالإضافة إلى بناء حاجز ضد التهديدات السيبرانية المتزايدة. يتم ذلك من خلال استخدام برامج مكافحة الفيروسات، وجدران الحماية، وتحديثات البرمجيات.

ويمثل تحقيق التوازن بين التقدم التكنولوجي والحفاظ على الأمن تحديًا مستمرًا، يتطلب تطوير وتبني استراتيجيات فعّالة للدفاع عن عالمنا الرقمي. في هذا السياق، يلعب الأمن السيبراني دورًا حيويًا في حماية معلوماتنا الشخصية وضمان استمرارية العمليات الأساسية للشركات والحكومات.

ويُعتبر الأمن السيبراني عملية تهدف إلى حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية، التي تسعى عادةً إلى الوصول إلى المعلومات الحساسة أو تعديلها أو تدميرها، بغرض الاستيلاء على الأموال من المستخدمين أو تعطيل العمليات.

ويشمل الأمن السيبراني مجموعة متنوعة من الإجراءات والتقنيات التي تهدف إلى حماية الأنظمة الإلكترونية والبيانات من التهديدات السيبرانية، بما في ذلك حماية البيانات الشخصية والمعلومات السرية الأخرى من السرقة أو التخريب بواسطة الفيروسات وبرامج الفدية.

كما يتضمن الأمن السيبراني حماية الشبكات والأنظمة ومنع المهاجمين من الوصول إليها، بالإضافة إلى اكتشاف الهجمات السيبرانية والتعامل معها بسرعة. ويتطلب الاستعداد لمواجهة هذه الهجمات تنفيذ تدابير وقائية، مثل: تحديث البرمجيات بانتظام، وفحص نقاط الضعف الأمنية، وتطبيق سياسات وصول صارمة.

إشكالية الدراسة:

يعد مفهوم الأمن السيبراني من المفاهيم الحديثة التي أصبح تشكل منعطفا كبيراً في شكل التكنولوجيا التي تلعب دورا مهما في البيانات وحمايتها، حيث أصبح بعض من المفكرين في عالم التكنولوجيا ينظ إلى السيبرانية على إنها عامل إيجابي في حياة البشر، يمكنهم من جعله حماية لبياناتهم ومعلوماتهم، ويقيهم من الأخطار التي قد تحدق بهم جراء هجمات يقوم بها بعض القراصنة أو بعض الهكرز، فيما ترى بعض الدول فيه منفعة كبيرة لكثير من الجوانب التي تهم حياة الدولة، فيما ينظر جانب آخر معارض لكل ما ينظر إليه

هؤلاء من باب أن الأمن السيبراني يشكل هاجسا وتحديا كبيرا لهم ولدولهم، فضلا عن أن مستقبل الأمن السيبراني قد يتعرض للخطر جراء ما يجري على كثير من الساحات والميادين والمجالات. لذا فإن الدراسة تسعى للإجابة على التساؤل التالي: ما هو مستقبل الأمن السيبراني وما التحديات التي تواجها؟

أهمية البحث:

تبرز أهمية هذه الدراسة من خلال تسليطها الضوء على الأمن السيبراني ومستقبله ،والتحديات التي تواجه مع التطورات السريعة في تكنولوجيا المعلومات والاتصالات، وأصبح الفضاء السيبراني ساحة نشطة للصراعات، مما يهدد استقرار الأنظمة السياسية والاقتصادية على مستوى العالم. وتزداد أهمية دراسة هذه الظاهرة في ظل تزايد الهجمات السيبرانية التي تستهدف البنية التحتية الحيوية، وارتفاع قدرة الدول على استخدام الفضاء السيبراني كأداة لفرض القوة أو ردع الخصوم.

أهداف البحث:

يهدف البحث لبيان مايلي:

1. ماهية الأمن السيبراني.
2. مستقبل الأمن السيبراني
3. التحديات التي قد تحدق بالأمن السيبراني في المستقبل.

منهج البحث:

استخدام الباحث المنهج الوصفي والتحليلي، الذي يتناول الظاهرة ويصفها ويسعى لتحليلها بشكل يمكنه من الوصول إلى نتائج، وتوصيات قد تمكن صانع القرار من الاستفادة منها، وذلك من خلال الرجوع لبعض المصادر والمراجع والبحوث والدراسات التي لها علاقة بموضوع البحث.

الدراسات السابقة:

هدفت دراسة (براده ، والقصير،2024) إلى التطرق إلى مجال الأمن السيبراني باعتباره مجموعة من السياسات والتقنيات التي تهدف إلى حماية أنظمة المعلومات خاصة بالمؤسسات والبيانات الرقمية من التهديدات والهجمات الإلكترونية التي يمارسها المخترقون الإلكترونيون، ومن خلال ورقتنا البحثية نسعي إلى تقديم مفهوم شامل للأمن السيبراني وتحديد الأهداف الأساسية للأمن السيبراني اضافة إلى ذلك أبراز أهميته وشروط تطبيقه، وعلاوة على ذلك تم التركيز على إبراز دوره في الحد من الهجمات الألكترونية التي

يمارسها المجرمون المتطفلون على النظام المعلوماتي على الضحية المستهدف، من خلال تحديد مفهوم الهجمات الألكترونية وأنواعها من الهجمات الألكترونية ومخاطرها وتبرز دور تقيم الأمن السيبراني في حد من الهجمات الألكترونية.

وناقش(محمد ،2022) في دراسة الأمن السيبراني والمصطلحات المستخدمة فيه، وكذلك الركائز الأساسية من خلال محورين: ما هو الأمن السيبراني، وأسس الأمن السيبراني والمصطلحات المستخدمة فيه، حيث أنه بعد جديد في أجندة مجال الدراسات الأمنية، فقد جذبت اهتمام العديد من الباحثين في هذا المجال، لذلك كان من الضروري فهم ما هو الأمن السيبراني كمتغير جديد في العلاقات الدولية، وحاول إلقاء الضوء على الأمن السيبراني ومصطلحاته من خلال استخدام المنهج الوصفي والتحليلي، وتوصلت الدراسة إلى تأصيل علمي لماهية الأمن السيبراني والتحكم في المصطلحات المستخدمة فيه، وكذلك الركائز الأساسية للأمن السيبراني.

وتناولت دراسة (أحمد واخرين،2022) موضوع الأمن السيبراني والنظافة الرقمية نظرًا لأهميته الكبير في ظل التحديات الراهنة التي تواجه المستخدمين نتيجة تعاملاتهم مع شبكات الأنترنت والأجهزة، حيث تزداد علميات الاختراق والانتهاكات يومًا بعد يوم ومن ثم كان لازاماً أن يكون هناك ردعًا لها وهنا يأتي دور الأمن السيبراني والنظافة الرقمية. ومن ثم هدفت هذه الدراسة إلى التعرف على مفهوم كل من الأمن السيبراني والنظافة الرقمية، ومعرفة الفرق بينهما، الوقوف على أهم الهجمات التي تعترض عملية الأمن السيبراني وكذا المشكلات التي تواجه النظافة الرقمية. وقد اعتمدت الدراسة على المنهج الوصفي التحليلي، وأظهرت بأن النظافة الرقمية جزء من الأمن السيبراني، وأنه يوجد علاقة فيما بين النظافة الرقمية والأمن السيبراني والذكاء الاصطناعي. وأوصت الدراسة بضرورة تكثيف دورات التوعية بموضوع الأمن السيبراني والنظافة الرقمية للحد من الانتهاكات.

المطلب الأول: التعريف بالأمن السيبراني

الفرع الأول: مفهوم الأمن السيبراني وأهميته

يتكون الأمن السيبراني من لفظتين" :الأمن"، و"السيبراني". (الأشقر ،2016).

الأمن: هو نقيض الخوف، أي بمعنى السلامة. والأمن مصدر الفعل أَمِنَ أَمْناً وأَمَاناً وأَمَنَةً :أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أَمِنَ من الشر، أي سَلِمَ منه .وقد عرّفه قاموس بنغوين للعلاقات الدولية بأنه مصطلح يشير إلى غياب ما يُهدد القيم النادرة.

أما السيبراني، فهو مصطلح السيبرانية الآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وتشير المقاربة الإيتيمولوجية لكلمة "cyber"إلى أنها لفظة يونانية الأصل مشتقة من كلمة «kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم « ."governor وتجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي norbert wieners 1894- 1964وذلك للتعبير عن التحكم الآلي.

ويُعد الأمن السيبراني أحد فروع الأمن الإنساني الذي نشأ نتيجة الثورة المعلوماتية والإلكترونية التي شهدها العالم. يُعتبر هذا المفهوم حديثًا، حيث تزامن مع عملية الرقمنة التي اجتاحت المؤسسات. وعلاوة على ذلك أصبح الأفراد المشاركون في هذه المؤسسات، مثل: الطلبة والأساتذة وموظفي الإدارة، يعتمدون بشكل أساسي على الإنترنت للتواصل والتفاعل الافتراضي في المجال الرقمي، بالإضافة إلى تقديم الخدمات الرقمية من قبل الإدارة أو عبر البوابات والمنصات الإلكترونية. (الحبيب،2021).

ويُعرَّف الأمن السيبراني بأنه مجموعة التدابير التي تركز على حماية الشبكات والأنظمة المعلوماتية في المؤسسات الجامعية. وتعتمد هذه المؤسسات على رقمنة هياكلها لتسهيل التفاعل بين الجامعة ومواردها البشرية، وذلك من خلال استخدام الأجهزة الحاسوبية المتصلة بالإنترنت. تتم عملية الاتصال من خلال تبادل البيانات الرقمية، التي تشمل مستندات وصور وفيديوهات، وتكون خاصة بالمؤسسة. (عوفي،2022).

والأمن السيبراني هو تنظيم وجمع الموارد والعمليات والهياكل المستخدمة لحماية الفضاء السايبري والأنظمة التي تدعم الفضاء السيبراني من الحدوث الذي يتعارض بحكم القانون عن حقوق الملكية الفعلية. وهو تنظيم وجمع الموارد والإجراءات والهياكل، ويلتقط هذا الجانب الأبعاد المتشابكة والتعقيد المتأصل في الأمن السيبراني، والتي تنطوي ظاهريا على تفاعلات بين البشر وبين الأنظمة وبين الإنسان والأنظمة. .(Thibault,2014)

ويرى الباحث أن الأمن السيبراني هو ممارسة حماية الأنظمة المتصلة بالإنترنت مثل الأجهزة والبرامج والبيانات من التهديدات الإلكترونية. يتم استخدامه من قبل الأفراد والمؤسسات للحماية من الوصول غير المصرح به إلى مراكز البيانات والأنظمة المحوسبة الأخرى، ويمكن أن توفر استراتيجية الأمن السيبراني الفعالة وضعا أمنيا قويا ضد الهجمات الخبيثة المصممة للوصول إلى أنظمة المؤسسة أو المستخدم وبياناتها الحساسة أو تغييرها أو حذفها أو تدميرها أو ابتزازها. ويعد الأمن السيبراني أيضا مُفيدا في منع الهجمات المصممة لتعطيل أو تعطيل عمليات النظام أو الجهاز.

ويجب أن يحتوي نهج الأمن السيبراني المثالي على طبقات متعددة من الحماية عبر أي نقطة وصول محتملة أو سطح هجوم. يتضمن ذلك طبقة واقية للبيانات والبرامج والأجهزة والشبكات المتصلة. بالإضافة إلى ذلك، يجب تدريب جميع الموظفين داخل المؤسسة الذين لديهم حق الوصول إلى أي من نقاط النهاية هذه على عمليات الامتثال والأمان المناسبة. تستخدم المؤسسات أيضا أدوات مثل أنظمة إدارة التهديدات الموحدة كطبقة أخرى من الحماية ضد التهديدات. يمكن لهذه الأدوات اكتشاف التهديدات المحتملة وعزلها ومعالجتها وإخطار المستخدمين إذا كانت هناك حاجة إلى إجراء إضافي. ويمكن للهجمات الإلكترونية أن تعطل ضحاياها أو تشل حركتها من خلال وسائل مختلفة، لذا فإن إنشاء استراتيجية قوية للأمن السيبراني هو جزء لا يتجزأ من أي منظمة. يجب أن يكون لدى المؤسسات أيضا خطة للتعافي من الكوارث حتى تتمكن من التعافي بسرعة في حالة حدوث هجوم إلكتروني ناجح. (Shea, Gillis,2024).

وتزايدت أهمية الأمن السيبراني في السنوات الأخيرة، وذلك بسبب تزايد الاعتماد على الأنظمة الرقمية والحوسبة في جميع جوانب الحياة اليومية. فمع تزايد استخدامات الإنترنت وأجهزة الكمبيوتر والأجهزة المحمولة، أصبحت هذه الأنظمة عرضة لهجمات إلكترونية من قبل قراصنة وهجمات سيبرانية يهدفون إلى سرقة البيانات أو تعطيل الخدمات أو إلحاق الضرر بالبنية التحتية، حيث يوجد أكثر من 21.1 مليار جهاز مرتبط بالإنترنت حول العالم.

ويمكن أن يكون لهجمات الأمن السيبراني عواقب وخيمة، ويمكن أن تؤدي إلى خسائر مالية كبيرة وانتهاك الخصوصية وإلحاق الضرر بالبنية التحتية. ويمكن أن تؤثر هذه الهجمات أيضًا على سمعة المؤسسات والمؤسسات المالية والبنوك مما يلحق الضرر بالمجتمع ككل.

فمع تزايد عدد المستخدمين والأجهزة والبرامج في المؤسسات الحديثة، بالإضافة إلى الطوفان المتزايد من البيانات التي يعتبر الكثير منها حساسًا أو سريًا تستمر أهمية الأمن السيبراني في النمو، وإن تزايد حجم وتطور المهاجمين السيبرانيين وتقنيات الهجوم يؤدي إلى تفاقم المشكلة بشكل أكبر من أي وقت مضى، لذا يلعب الأمن السيبراني وبرامج الدفاع الإلكتروني دورا لا غنى عنه في حماية الأشخاص والمؤسسات واقتصاديات الدول. (زيان ،2023).

ويكتسب الأمن السيبراني أهمية كبيرة تتجلى في النقاط التالية: (عبد الرزاق وفتحي، 2024):

1 .يُعتبر تأمين المعلومات الإلكترونية جزءًا أساسيًا من رفاهية الأفراد والعائلات والمؤسسات والحكومات والهيئات الأكاديمية. يجب على الآباء والأسر أن يضعوا حماية أطفالهم من الاحتيال عبر الإنترنت في مقدمة أولوياتهم.

2 .يساهم ضمان حماية البيانات المالية في الحفاظ على الاستقرار المالي للأفراد. بالنسبة للمعلمين والطلاب والموظفين، ويُعد الإنترنت مصدرًا قيمًا يوفر العديد من فرص التعلم، لكنه يحمل أيضًا تهديدات محتملة يجب التعامل معها لضمان سلامة جميع الأطراف المعنية.

3 .يُعتبر الأمن السيبراني من أبرز الأساليب الوقائية لمواجهة الجريمة، وقد اعتمدته العديد من الدول مثل هولندا وكندا للحفاظ على أمنها وتقليل معدلات الجريمة.

4 .تُعد تنمية الوعي الأمني وسيلة وقائية تساهم في تجنيب المجتمع التبعات الاجتماعية والاقتصادية والمعنوية للجريمة. ينبغي على الدولة العمل على تعزيز هذا الوعي وتطويره بما يخدم مصلحة الأمن والاستقرار.

5. يؤدي غياب الوعي الأمني بشكل عام إلى سلوكيات أو أنشطة قد تهدد أمن الفرد وأمن المجتمع بشكل عام.

الفرع الثاني: أنواع الأمن السيبراني

يمكن تقسيم مجال الأمن السيبراني إلى عدة أقسام مختلفة، ويعد التنسيق داخل المنظمة أمرًا بالغ الأهمية لنجاح برنامج الأمن السيبراني. وتشمل هذه الأقسام ما يلي: (زيان،2023):

أمن الشبكة :Network security

يركز هذه المجال على تأمين شبكات الكمبيوتر من المتسللين، سواء كانوا مهاجمين مستهدفين أو برامج ضارة انتهازية. يهدف إلى منع واكتشاف التهديدات والهجمات على الشبكات وتشفير الاتصالات لمنع الوصول غير المصرح به.

أمن التطبيقات:Application security

يركز أمان التطبيقات على إبقاء البرامج والأجهزة خالية من التهديدات والثغرات التي من الممكن أن تصل إلى البيانات المصممة لحماية الشبكة. ويبدأ الأمان في مرحلة التصميم التطبيقي، حيث يهتم بضمان خلو البرامج من الثغرات الأمنية قبل نشرها على الأجهزة.

الأمن السحابي:Cloud security

التأمين السحابي هو شئ ضروري أصبح من اللازم تأمين السحابة الرقمية بسبب احتوائها على كمية بيانات هائلة لهذه المؤسسات يتناول حماية البيانات والتطبيقات المستضافة في بيئات الحوسبة السحابية، مع التركيز على إدارة الهوية والوصول الآمن.

أمن المعلومات :Information security

يحمي سلامة وخصوصية البيانات، سواء أثناء تخزينها أو نقلها، مما يقوم بضمان استخدام أمن للمعلومات يركز على حماية البيانات والمعلومات من التسريب والاستخدام غير المصرح به. يتضمن ذلك استخدام تقنيات التشفير، وتنفيذ سياسات إدارة الوصول، وضمان الامتثال لقوانين حماية البيانات.

الأمن التشغيلي :Operational security

يتضمن العمليات والقرارات الخاصة بحماية أصول البيانات وضمان سلامتها، بما في ذلك إدارة الوصول وتحديد مواقع تخزين البيانات وأيضا يتعلق بتأمين العمليات اليومية للمؤسسة، بما في ذلك إدارة الحسابات والصلاحيات، وتحديد مراقبة الحدود، والتدابير التنظيمية للحد من المخاطر.

التعافي من الكارثة واستمرارية الأعمال :Disaster recovery and business continuity

يحدد كيفية استجابة المؤسسة لحوادث الأمان السيبراني وكيفية استعادة الأعمال والبيانات بشكل سريع وفعال من خلال وضع استراتيجيات لاستعادة البيانات واستئناف العمليات بشكل سريع بعد وقوع حادث أمان سيبراني. ويتطلب الأمان السيبراني تكاملًا شاملًا لتقديم حماية فعّالة، حيث يعتبر تحقيق توازن بين هذه الأنواع العديدة أمرًا حاسمًا لضمان سلامة البيئة الرقمية.

تثقيف المستخدم النهائي :End-user education

يعالج عوامل الأمان المتعلقة بالأفراد، حيث يهدف إلى تثقيف المستخدمين حول ممارسات الأمان الجيدة، مثل التعامل مع المرفقات البريدية بحذر وتجنب توصيل أجهزة USB غير المعروفة والتي من الممكن ان تحمل فيروسات ضارة.

أمان إنترنت الأشياء (IoT)

هو مجموعة من الممارسات والتقنيات التي تحمي الأجهزة المتصلة بالإنترنت من الهجمات الإلكترونية. تواجه أجهزة IoT مجموعة متنوعة من التهديدات.

المطلب الثاني: التهديدات السيبرانية

الفرع الأول: حجم التهديدات السيبرانية

نتيجة لارتفاع حجم التهديد السيبراني، فإن الإنفاق العالمي على حلول الأمن السيبراني يتزايد بشكل طبيعي وتتوقع مؤسسة جارتنر أن يصل الإنفاق على الأمن السيبراني إلى 188.3 مليار دولار أمريكي في عام 2023، ويتجاوز 260 مليار دولار أمريكي عالميًا بحلول عام 2026.

ويمثل التهديد السيبراني العالمي تحديًا متزايدًا، حيث ترتفع وتيرة اختراقات البيانات كل عام. في عام 2019، تم الكشف عن 7.9 مليار سجل صادم من خلال خروقات البيانات. وهذا الرقم يزيد عن ضعف عدد السجلات التي تم الكشف عنها في عام 2018.

وكانت الخدمات الطبية وتجار التجزئة والهيئات العامة أكثر القطاعات تضررًا من الانتهاكات والاختراقات، حيث كان القراصنة مسؤولين عن معظم الحوادث. تجذب بعض هذه القطاعات، مثل الخدمات الطبية، المتسللين لأنها تحتوي على بيانات حساسة، مثل البيانات المالية أو الطبية. ومع ذلك، يمكن استهداف أي شركة تستخدم الشبكات لجمع البيانات أو إرسالها.

وقد استجابت الحكومات في جميع أنحاء العالم للتهديد السيبراني المتزايد بتوجيهات لمساعدة المؤسسات على تنفيذ ممارسات فعالة للأمن السيبراني. في الولايات المتحدة، أنشأ المعهد الوطني للمعايير والتكنولوجيا (NIST)إطار عمل للأمن السيبراني والذي يؤكد على مراقبة مستمرة وفي الوقت الفعلي لجميع الموارد الإلكترونية. (زيان،2023).

الفرع الثاني: أنواع التهديات السيبرانية

من المتوقع أن تستمر التهديدات السيبرانية في التطور والتقدم في السنوات القادمة مع تقدم التكنولوجيا. ويشير خبراء الأمن إلى إمكانية ظهور تحديات وتهديدات جديدة في المستقبل، ومن هذه التهديدات المحتملة:

الذكاء الاصطناعي:

يعد الذكاء الاصطناعي تقنية سريعة التطور ويمكن استخدامها لإنشاء هجمات سيبرانية أكثر تعقيدا وقوة، مما يجعل من الصعب اكتشافها والتصدي لها، حيث يمكن استخدام الذكاء الاصطناعي لإنشاء برامج ضارة أكثر

ذكاء يمكنها التهرب من تقنيات الأمان التقليدية، كما يمكن أيضا استخدام الذكاء الاصطناعي لإنشاء هجمات تستهدف البنية التحتية الحيوية، مثل شبكات الطاقة أو نظم النقل. (عنتر ،2023).

إنترنت الأشياء :(IoT)

وتُستخدم أجهزة إنترنت الأشياء من أجل إنشاء هجمات حجب الخدمة الموزعة (DDoS) أو سرقة البيانات أو حتى السيطرة على الأجهزة، وقد يزداد التركيز على استهدافها للوصول إلى بيانات المستخدمين أو التحكم في الأنظمة المتصلة.

الهجمات الهجينة:

وتَستخدم الهجمات الهجينة مزيجا من الأساليب التقليدية وغير التقليدية، وتتميز بأنها أكثر تعقيدا وصعوبة في الاكتشاف والحماية منها مقارنة بالهجمات التقليدية.

هجمات الحواسيب الكمومية:

قد تظهر هجمات تعتمد على الحوسبة الكمومية من أجل كسر أنظمة التشفير الحالية، حيث تتميز الحواسيب الكمومية بقدرتها على إجراء العمليات الحسابية بشكل أسرع بكثير من الحواسيب التقليدية، وهذا يجعلها قادرة على كسر أنظمة التشفير الحالية. (عنتر،2023).

الهجمات على الذكاء الاصطناعي:

قد تُستهدف نظم الذكاء الاصطناعي بشكل مباشر لتشويه البيانات أو النتائج، وقد تتسبب هذه الهجمات بتعطيل الأنظمة أو سرقة البيانات أو حتى تعديل البيانات أو إتلافها.

التهديدات السيبرانية للصحة الرقمية:

قد تستهدف أجهزة الرعاية الصحية أو نظم السجلات الطبية، وذلك لأنها حساسة للغاية ويمكن استخدامها لأغراض ضارة، مثل الابتزاز أو التجسس أو حتى إلحاق الضرر الجسدي.

هجمات التحكم في الطائرات المسيرة:

أصبح استهداف الطائرات المسيرة أو أنظمة التحكم فيها محط اهتمام متزايد، وقد تتسبب هذه الهجمات بأضرار جسيمة، بما في ذلك تعطيل الطائرات أو سرقة البيانات أو حتى إسقاطها.

ويرى الباحث أن التهديدات السيبرانية أصبحت تُشكل خطراً على الدول والمؤسسات وبشكل يجعل الحياة أكثر تعقيدا جراء الهجمات السيبرانية التي قد يتم شنها من قبل دول أو جماعات أو أفراد، وقد يكون ذلك من قبل جماعات إرهابية تشكل تهديدا للدولة والمجتمع، وتجعل الحياة أكثر صعوبة جراء ما يتم من نتائج كارثية معقدة.

المطلب الثالث: التحديات المُستقبلية التي تواجه الأمن السيبراني

الفرع الأول: تحديات ومخاطر الأمن السيبراني

أولا: تحديات الأمن السيبراني

في الوقت الذي ارتفعت فيه معدلات الاعتماد على التكنولوجيا الرقمية ، أصبحت التهديدات الرقمية تتطور بصورة سريعة مما يجعل تحديات الأمن السيبراني مستقبلا معقدة أكثر وتحتاج إلى حلول متقدمة من أجل التصدي لها وفيما يلي أبرز تحديات الأمن السيبراني: (الكوتي،2023).

تزايد التهديدات السيبرانية

في ظل الانتشار والتوسع المستمر في استخدام التقنيات الذكية والأنظمة الرقمية قد تزيد التهديدات السيبرانية بصورة كبيرة ولا تقتصر التهديدات على البرمجيات الخبيثة أو الفيروسات بل تزيد لتضم هجمات هندسة اجتماعية وهجمات مستهدفة مثل هجمات الفدية التي ارتفعت كثيرا في السنوات الأخيرة.

نقص الكفاءات المتخصصة

قطاع الأمن السيبراني يشهد نقص كبير في المهارات المتخصصة من أجل التصدي لتلك التهديدات مما يرفع من احتياج المؤسسات إلى الخبرة والكفاءة المتخصصة، وذلك النقص يدل على وجود العديد من الفرص الكبيرة للعمل في المجال إلا أنه يمثل في الوقت نفسه تحدي كبير للتكيف بصورة سريعة مع التهديدات المستمرة.

التطور السريع في التكنولوجيا

يعتبر التطور السريع في الذكاء الاصطناعي والمعلومات الضخمة وإنترنت الأشياء من أهم العوامل التي تساعد في توسيع قاعدة الهجمات السيبرانية، وتلك التقنيات نفسها من الممكن أن تكون من الأدوات الفعالة لحماية المعلومات إلا أنها تفتح آفاق جديدة للمهاجمين لاستغلال الثغرات.

التشريعات والقوانين

مع ارتفاع الهجمات السيبرانية أصبح من الواجب القيام بتطوير التشريعات والقوانين لتتماشى مع التطورات في هذا المجال، حيث أن هناك تحديات لها علاقة بتحسين القوانين الدولية وتنظيمها لتكون فعالة أكثر لمواجهة التهديدات الخاصة بالحدود، وهي مسألة من الممكن أن تؤثر على آليات الحماية التي في المستقبل.

ثانيا: مخاطر الأمن السيبراني

تعتبر المخاطر الإلكترونية شكلا من أشكال المخاطر التشغيلية وتعرّف على أنها مخاطر الخسارة الناتجة عن الحوادث الرقمية الناجمة عن الحوادث الداخلية والخارجية. أو أطراف ثالثة، بما في ذلك السرقة أو النزاهة المعرضة للخطر أو تلف المعلومات أو أصول التكنولوجيا، والاحتيال الداخلي والخارجي وتعطيل الأعمال. وهذا التعريف يتوافق إلى حد كبير مع جهود القطاع الخاص المتزامنة المعروفة لتحديد المخاطر السيبرانية، على سبيل المثال: مبادرة مخاطر الأمن السيبراني والمعلوماتية الخاصة بشركة ORX. وقد تؤدي حوادث المخاطر السيبرانية إلى إضعاف سرية وسلامة وتوافر البيانات والمعلومات والتشغيل السليم للبنية التحتية لتكنولوجيا المعلومات. ((Curti, Gerlach, et al.,2019 ،حيث أن أنظمة الأمن السيبراني هي أنظمة مدعومة بالذكاء الاصطناعي للحماية من الانتهاكات الأمنية المحتملة ومنعها، ويستخدم الذكاء الاصطناعي لتطبيق الخدمات المصرفية عبر الهاتف المحمول وتطوير حلول الذكاء الاصطناعي لدعم العملاء وأتمتة العمليات والموارد البشرية والأمن واكتشاف الاحتيال. (Saon, Miglanic, 2019).

وقد عرفت مخاطر الأمن السيبراني على أنه المخاطر التشغيلية لأصول المعلومات والتقنية التي تؤثر على سرية أو توافر أو سلامة المعلومات أو أنظمة المعلومات. (Kumar, Thomas, 2022) وأن سرقة بيانات وهوية المستهلك، وكذلك التلاعب بها، باعتبارها تهديدات إلكترونية رئيسية تؤثر على أعمال البنوك. والتهديدات التي تتعرض لها البنية التحتية المالية، والمخاطر التي تشكلها البرامج الضارة المدمرة (Piotrowski, 2022) وإن تصنيف المخاطر السيبرانية والمحفازت الكامنة وارءها يمكن أن يؤدي إلى وجود تعريف وفهم مشترك عبر البنوك، بما في ذلك بين السلطات والمشاركين من القطاع الخاص. وإلى زيادة تسهيل تبادل المعلومات والتعاون المناسب في إدارة المخاطر الإلكترونية. حيث يتم تنظيم تصنيف المخاطر الإلكترونية للأمن السيبراني إلى: (Curti, Gerlach, et al., 2019)

مسببات المخاطر السيبرانية: الطريقة التي يتم من خلالها تنفيذ هجوم إلكتروني ضار من خلال:

أ– رفض الخدمة: هو هجوم يغمر الأنظمة أو الخوادم أو الشبكات بحركة مرور لاستنفاد الموارد وعرض النطاق الترددي. نتيجة لذلك، النظام غير قادر على تلبية الطلبات المشروعة.

ب– هجوم التنصـــت: يدخل المهاجمون أنفســـهم في معاملة ثنائية الأطراف وذلك بمجرد مقاطعة المهاجمين لحركة المرور، يمكنهم تصفية البيانات وسرقتها.

ت– التصـيد الاحتيالي: هو ممارسـة إرسـال اتصـالات احتيالية التي تبدو أنها واردة من مصـدر حسـن السـمعة، عادة عبر البريد الإلكتروني. والهدف منه سـرقة البيانات الحسـاسـة مثل بطاقة الائتمان ومعلومات تسجيل الدخول أو تثبيت برامج ضارة على جهاز الضحية.

ث– هجوم كلمة المرور: يحدث عندما تحصـل أطراف غير مصـرح لها على حق الوصـول إلى كلمة مرور الشـخص من خلال النظر حول مكتب الشـخص، واسـتنشـاق الاتصـال بالشـبكة للحصـول على كلمات مرور غير مشـفرة، واسـتخدام الهندسـة الاجتماعية، والحصـول على إمكانية الوصـول إلى قاعدة بيانات كلمة المرور أو التخمين المباشر.

ج– حقن SQL: يحدث حقن لغة الاســتعلام الهيكلية (SQL) عندما يقوم المهاجم بإدراج تعليمات برمجية ضارة في خادم يستخدم SQL ويجبر الخادم على الكشف عن المعلومات الخاصة به عادة.

ح– البرمجة النصـــية عبر المواقع: تســتخدم هجمات البرمجة النصـــية عبر المواقع موارد ويب تابعة لجهات خارجية لتشغيل البرامج النصية في متصفح الويب الخاص بالضحية أو التطبيق القابل للبرمجة.

خ– البرامج الضـارة: برنامج مصـمم بقصـد ضـار يحتوي على ميزات أو قدرات يمكن أن تسـبب ضـرر مباشر أو غير مباشر للكيانات أو أنظمة المعلومات الخاصة بها.

د–استغلال Zero–day: ثغرة أمنية في الأجهزة أو البرامج الثابتة أو البرامج غير المعروفة سابقا.

ذ–أخرى: أي نوع آخر من الهجمات الإلكترونية التي لم يتم تعريفها. سـتعمل هذه الفئة كفئة التقاط الكل للهجمات الإلكترونية ذات النوع المعروف ولكن لم يتم التقاطها بواسطة فئة أخرى موجودة.

ر– غير معروف: عندما يكون نوع الهجوم الإلكتروني غير معروف للمؤسسة.

2. نتيجة الحادث السيبراني: نتيجة حادث إلكتروني يؤدي إلى:

أ– اضـطراب الأعمال وفشـل النظام والتنفيذ: هي الحوادث الداخلية أو الخارجية التي تعطل العمل أو تتسبب في فشل البرامج، الأجهزة، تكنولوجيا المعلومات.

ب– خرق البيانات: تعني فقدان البيانات أو التعرض الذي يتضمن معلومات التعريف الشخصية.

ت– سـرقة أو فقدان معلومات غير معلومات: تعني سـرقة أو فقدان التكنولوجيا أو الملكية الفكرية أو المعلومات التجارية أو أي معلومات أخرى ليست معلومات تحديد الهوية الشخصية.

ث– سـرقة الأموال: هي الحوادث التي أدت إلى خسـارة فورية ومباشـرة للأموال وتم تنفيذها عبر قناة رقمية.

3. النية: مؤشر لمعرفة ما إذا كان الحادث الإلكتروني متعمدًا أم عرضيًا:

أ. متعمد: عندما يكون الحادث الإلكتروني متعمدا.

ب. غير مقصود: عندما يكون الحادث السيبراني غير مقصود.

4. المنشأ: مؤشر لمعرفة ما إذا كانت الحادثة الإلكترونية قد نشأت في المؤسسة أو في جهة خارجية:

أ. طرف خارجي: عند وقوع الحادث السيبراني لدى طرف ثالث، بائع أو أي كيان خارجي آخر.

ب. طرف غير خارجي: عندما بدأ الحادث الإلكتروني في المؤسسة أو الشركة التابعة لها.

الفرع الثاني: التطورات المستقبلية المتوقعة في الأمن السيبراني

في ظل التقدم التكنولوجي وازدياد التهديدات الإلكترونية، يشـهد مجال الأمن السـيبراني تطورات سـريعة تهدف إلى تعزيز الحماية الرقمية ومواجهة الهجمات المتطورة وهذا يجعل التوجهات المســـتقبلية المتوقعة في الأمن الســـيبراني محور اهتمام المؤســـســـات والحكومات على مســـتوى العالم، وتتمثل هذه التطورات فيما يلي: (السعيد،2025).

الاستخدام المتزايد للذكاء الاصطناعي

مجال الأمن السيبراني يشـهد تطور كبير في الذكاء الاصـطناعي واسـتخدامه من أجل تعزيز الطرق الخاصـة بالكشف عن التهديد السيبراني حيث يمكن للذكاء الاصطناعي أن يحلل العديد من البيانات الضخمة بسرعة، مما يسـاهم في الكشـف عن كافة الأنماط الغير تقليدية وتحديد التهديد المحتمل قبل أن يقع. ومن المتوقع أن تعتمد المؤسسات بصورة كبيرة على الذكاء الاصطناعي والتعليم الآلي في عمليات الحماية السيبرانية.

تحسين تقنيات التشفير

مع تزايد تعقيد الهجمات السيبرانية، تسعى المؤسسات إلى تعزيز أساليب التشفير لديها لحماية بياناتها بشكل أكثر فعالية. ومن المتوقع أن تشـهد السنوات المقبلة اهتمامًا متزايدًا في تطوير خوارزميات تشفير جديدة، مثل التشفير الكمي، الذي يعتبر حلاً واعدًا لتأمين البيانات الحساسة بشكل أفضل.

زيادة الاهتمام بخصوصية البيانات

الحفاظ على خصوصية المعلومات ستصبح هي المحور الأساسي للحكومات والمؤسسات ويتوقع أن تظهر بعض التقنيات الجديدة التي ترتكز على حماية المستخدمين وخصوصيتهم مثل التقنيات التي تعتمد على الكتل والتي يمكن من خلالها تأمين المعلومات بصورة مبتكرة ومميزة وأكثر شفافية.

نظم الحماية الذاتية والتكيف الذاتي

يتوقع أن يوفر مستقبل الأمن السيبراني بعض الأنظمة التي تشمل قدرات التكيف الذاتية، حيث أن تلك الأنظمة تتعلم محاولات الهجوم السابقة وتقوم بتطوير خطط جديدة لحماية نفسها، وتلك الأنظمة ستكون بمثابة ثورة جديدة في مجال الأمن السيبراني، حيث يمكن أن تتكيف بصفة مستمرة مع التهديدات الجديدة.

دعم التحول إلى تقنيات السحابة الآمنة

وستصبح التهديدات السيبرانية العصرية تمثل تحديات خطيرة للمؤسسات والحكومات على حد سواء. وتتطور هذه التهديدات بشكل سريع، مما يستدعي تطوير آليات دفاعية أكثر فعالية. من بين تلك التهديدات، تبرز البرمجيات الخبيثة وهجمات الفدية كأبرز المخاطر. وتتضمن البرمجيات الخبيثة مجموعة واسعة من البرامج التي تهدف إلى إلحاق الضرر بالنظم أو سرقة المعلومات، ويمكن أن تأتي في شكل فيروس، دودة، أو حصان طروادة. على سبيل المثال، تم اكتشاف برمجية "بدجيت" التي أصابت مئات الآلاف من الأجهزة حول العالم، مما أدى إلى تسرب بيانات حساسة وتكاليف باهظة لإعادتها إلى وضعها الطبيعي.

أما هجمات الفدية، فقد زادت بشكل ملحوظ وتستهدف المؤسسات الكبيرة، حيث يقوم المهاجمون بتشفير بيانات الضحية ويطلبون فدية لإعادتها. واحدة من أشهر هذه الهجمات كانت هجمات"WannaCry" ، التي أثرت على الكثير من المنظمات بما في ذلك المستشفيات، وتسببت في تعطيل خدماتها الطبية. هذه الهجمات لا تؤثر فقط على البيانات، بل تؤدي أيضًا إلى فقدان الثقة من قبل العملاء والشركاء التجاريين.

وسيلعب الذكاء الاصطناعي دوراً متزايد الأهمية في عالم الجرائم الإلكترونية. ويمكن استخدام تقنيات التعلم الآلي في تصميم هجمات أكثر تعقيدًا، مما يزيد من صعوبة اكتشافها. وعلى سبيل المثال: استخدم المهاجمون خوارزميات الذكاء الاصطناعي لإنشاء رسائل بريد إلكتروني أكثر واقعية، مما يجعل الضحية أكثر عرضة للوقوع في الفخ. وتبرز هذه الأمثلة أهمية تعزيز قدرات الأمن السيبراني لمواجهة التهديدات العصرية وضمان سلامة البيانات والبنية التحتية المؤسسية.

ومع تسارع التطورات التكنولوجية، يظهر الأمن السيبراني كأحد أبرز المجالات التي تحتاج إلى ابتكارات دائمة لمواجهة التهديدات المتزايدة. وتتزايد الاعتمادية على تقنيات الذكاء الاصطناعي والتعلم الآلي، حيث

يمكن استخدام هذه التقنيات لمراقبة وتحليل الأنماط السلوكية لضمان كشف التهديدات قبل أن تتسبب في أضرار. ومن المتوقع أن يصبح الذكاء الاصطناعي من الأدوات الرئيسية التي يعتمد عليها المتخصصون في الأمن السيبراني لتسريع استجابة الأنظمة وتحسين دقتها.

ويرى الباحث أن الأخطار الناشئة مستقبلا عن السيبرانية وما فيها من مخاطر وتهديدات تحتاج إلى اهتمام خاص، حيث يمكن أن تتضمن التهديدات الهجومية الجديدة تقنيات متطورة مثل هجمات الفدية التي تستهدف قطاعات حيوية مثل الرعاية الصحية والنقل. وبما أن هذه الهجمات أصبحت أكثر تعقيدًا واحترافية، فإن الأمر يتطلب من المؤسسات الانتباه لكل ما يجري حولها من مخاطر، بحيث تكون جاهزة لصد وردع أي محاولات سيبرانية قد تنال منها ومن أفرادها.

النتائج والتوصيات

النتائج:

بعد أن استعرض الباحث موضوع الدراسة تبين ما يلي:

1. الأمن السيبراني هو مجموعة التدابير التي تركز على حماية الشبكات والأنظمة المعلوماتية في المؤسسات الجامعية.
2. تزايدت أهمية الأمن السيبراني في السنوات الأخيرة، وذلك بسبب تزايد الاعتماد على الأنظمة الرقمية والحوسبة في جميع جوانب الحياة اليومية.
3. يشهد قطاع الأمن السيبراني نقص كبير في المهارات المتخصصة من أجل التصدي لتلك التهديدات مما يرفع من احتياج المؤسسات.
4. إلى الخبرة والكفاءة المتخصصة.
5. يتطلب الأمان السيبراني تكاملًا شاملًا لتقديم حماية فعّالة، حيث يعتبر تحقيق توازن بين هذه الأنواع العديدة أمرًا حاسمًا لضمان سلامة البيئة الرقمية.
6. ستستمر التهديدات السيبرانية في التطور والتقدم في السنوات القادمة مع تقدم التكنولوجيا، ويشير خبراء الأمن إلى إمكانية ظهور تحديات وتهديدات جديدة في المستقبل.
7. هناك مجالات عدة لتعزيز قدرات الدول والمؤسسات الدفاعية من خلال الاستثمار في البنى التحتية المتطورة وتقديم تدريبات متخصصة للعاملين فيها.

التوصيات:

استنادا لما توصلت إليه الدراسة من نتائج فإن الباحث يوصي بما يلي:

1. من الضـــروري القيام بتأمين تلك البيئة الجديدة حيث يتوقع أن تظهر بعض التقنيات الجديدة التي ترتكز على حماية السحابة والعمل على تطوير البروتوكولات الخاصة بالأمان.
2. العمل على إيجاد حلول للتهديدات السيبرانية من خلال التطور والتقدم مع تقدم التكنولوجيا.
3. العمل على تعزيز أساليب التشفير لحماية البيانات بشكل فعل خاصة في ظل تطوير خوارزميات تشفير جديدة.
4. التأكيد على المراقبة المســـتمرة وفي الوقت الفعلي لجميع الموارد الإلكترونية، التي قد يمكن التعامل معها في أي وقت.
5. التركيز على حماية البيانات والمعلومات من التسريب والاستخدام غير المصرح به.
6. وضع استراتيجيات لاستعادة البيانات واستئناف العمليات بشكل سريع بعد وقوع حوادث الأمان السيبراني.
7. تعزيز قدرات الدول والمؤســـســـات الدفاعية من خلال الاســـتثمار في بنى تحتية متطورة وتقديم تدريبات متخصصة للعاملين.
8. الفهم العميق لمجموعات التهديدات الذي يمكن أن يساعد في تحسين الفعالية الدفاعية ويساهم في تقليل الأمور غير المتوقعة.

المراجع

المراجع العربية

الأشـــقر، جبور منى (2016) الســـيبرانية هاجس العصـــر، بيروت: جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية.

الحبيب، ماجد بن عبد الله (2021) "مستوى الوعي بالأمن السيبراني لدى طلاب وطالبات الدراسات العليا في كلية التربية بجامعة الإمام محمد بن سعود الإسلامية." مجلة العلوم التربوية، العدد (31).

زيان، احمد، ما هو الأمن الســـيبراني وما هي أهميته وكيف تحمي نفســـك من الهجمات الإلكترونية، بحث منشور بتاريخ :2023/11/20، على الرابط: https://arabwar.net-cyber-security.

السعيد، رانيه، مستقبل الأمن السيبراني.. التطورات والتحديات والتوجهات المستقبلية، بحث منشور على مجلة الاهرام الاقتصادي، بتاريخ :2025/2/2.

عبد الرزاق، براده، وفتحي، القصـــير (2024) الأمن الســـيبراني ودوره في الحد من الهجمات الإلكترونية، https://www.researchgate.net/publication

عنتر، احمد، تقنيات الأمن الســـيبراني والتحديات المســـتقبلية، بحث منشـــور بتاريخ: 4/12/2023، على الرابط: https://www.aljazeera.net/tech .

عوفي، حبيب (2022) "الفضـــاء الرقمي: تحدٍ أمني جديد واســـتراتيجيات الدول لتحقيق الأمن الســـيبراني العالمي «، المجلة الجزائرية للعلوم الإنسانية والاجتماعية، العدد (6).

الكوتي، محمد، الأمن السيبراني في 2023: تحولات وتحديات عصـر الذكاء الاصـطناعي، بحث منشـور على موقع تريندر للبحوث والدراسات، بتاريخ 2023/1/26.

المراجع الأجنبية

Curti, F., Gerlach, J., Kazinnik, S., Lee, M. J., & Mihov, A. (2019). Cyber risk definition and classification for financial risk management. Federal Reserve Bank of St Louis, August, mimeo.

Kumar, R., & Thomas, B. (2022). BRICS in Global Governance: A Gradual but Steady Expansion. Governance and Politics, 1(1), 100-113

Piotrowski, D. (2022). Consumer perceived ethicality of banks in the era of digitalisation: The case of Poland. Economics and Business Review, 8(1), 90-114.

Saon Raya, S. P., & Miglanic, S., (2019), Use of Blockchain and Aritificial Intelligence to promote financial inclusion in India. TECH MONITOR • Jan-Mar 2019.

Thibault, Nadia Diakun (2014) Defining Cybersecurity, https://www.researchgate.net.

What is cybersecurity, https://www.techtarget.com .

Shea, Sharon& Gillis (2024)

STARDOM UNIVERSITY

Stardom Scientific Journal for Humanitirian and Social Studies

Peer Reviewed Journal of Humanities and Social Studies
Published Quarterly by Stardom University
Volume 2 - 2nd issue 2024
International deposit number : ISSN 2980-3772