الأمن السيبراني والنظافة الرقمية

فاطمة علي إبراهيم

مدرس مساعد بقسم علوم المعلومات- كلية الآداب- جامعة بني سويف

أ.د/ رحاب يوسف

قسم علوم المعلومات كلية الآداب جامعة بني سويف

د/ وليد محمود السيد

قسم نظم المعلومات كلية الحاسبات والذكاء الاصطناعي جامعة بني سويف

مستخلص:

تتناول الدراسة موضوع الأمن السيبر اني 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 لازامًا أن يكون هناك ردعًا لها وهنا يأتي دور الأمن السيبر اني والنظافة الرقمية. ومن ثم هدفت هذه الدراسة إلى التعرف على مفهوم كلًا من الأمن السيبر اني والنظافة الرقمية، ومعرفة الفرق بينهما، الوقوف على أهم الهجمات التي تعترض عملية الأمن السيبر اني وكذا المشكلات التي تواجه النظافة الرقمية. وقد اعتمدت الدراسة على المنهج الوصفي التحليلي، وخرجت بعدة نتائج أهمها أن النظافة الرقمية جزء من الأمن السيبر اني، أنه يوجد علاقة فيما بين النظافة الرقمية والأمن السيبر اني والذكاء الاصطناعي. وقد أوصت الدراسة بضرورة تكثيف دورات التوعية بموضوع الأمن السيبر اني والنظافة الرقمية للحد من الانتهاكات.

Abstract

The study deals with the issue of cybersecurity and digital hygiene due to its great importance in light of the current challenges facing users as a result of their interactions with internet networks and devices, as penetration and violations are increasing day by day, and then there was a need to deter them, and here comes the role of cybersecurity and digital hygiene. Hence, this study aimed to identify the concept of both cybersecurity and digital hygiene, find out the difference between them, and identify the most important attacks that obstruct the cybersecurity process, as well as the problems facing digital hygiene. The study relied on the descriptive analytical approach, and came out with several results, the most important of which is that digital hygiene is part of cyber security, that there is a relationship between digital hygiene, cyber security and artificial intelligence. The study recommended the need to intensify awareness sessions on the issue of cyber security and digital hygiene to reduce violations.

أولًا الإطار المنهجي للدراسة:

تمهيد:

لقد انتشرت مؤخَّرًا نوعية خطيرة من الهجمات والجرائم السيبرانية تعتمد على تقنيات متقدمة (كالحوسبة السحابية والذكاء الاصطناعي و إنترنت الأشياء)، وأجهزة تصنت على شبكات الاتصال، وبرمجيات لتشفير العمليات المشبوهة، وبرمجيات خبيثة لاختراق أنظمة أمن الشبكات والحاسبات لتسخيرها في القيام بعمليات إجرامية وتعاملات مشبوهة دون علم أصحابها فيما يُسمَّى بالشبكات الآلية، حيث يمكن أن تضم شبكة آلية واحدة عشرات أو مئات الآلاف أو ملايين الحواسب أو الأجهزة المتصلة بالإنترنت التي يمكن استخدامها لشن هجمات متنوعة، مثل الهجمات الموزَّعة لإعاقة الخدمات على شبكات ومواقع مستهدفة لأغراض إجرامية كالتخريب والإرهاب والتهديد والابتزاز.

كما أن الأمور لم تتوقف عند هذا الحد بل تطرقت إلى المؤسسات الأكاديمية كالجامعات والمعاهد البحثية حيث لا يخفى على أحد أن هناك الكثير من الجرائم المعلوماتية التي تتم داخل الجامعات كالسرقات العلمية و القرصنة الإلكترونية التي تتم على مواقع الجامعات ذاتها والاختراقات وما إلى ذلك فكم سمعنا عن أساتذة قاموا بانتحال بحوث وكتابات علمية لآخرين، وكم سمعنا عن مواقع لجامعات تم اختراقها، ومن ثم تظهر أهمية النظافة الرقمية" الممارسات والاحتياطات التي يتخذها المستخدمون بهدف الحفاظ على البيانات الحساسة منظمة ومنظمة وآمنة من السرقة والهجمات الخارجية" (Tandon, Gaurav H,2019). وأهمية تطبيق الممارسات الخاصة بها للحد من مثل هذه الجرائم ومجابهة مثل هذه الظواهر، ومن ثم تناولت هذه الدراسة موضوع ممارسات النظافة الرقمية ومعرفة السبل والكيفية التي يمكن من خلالها حماية الأشخاص أثناء تعاملاتهم مع الأجهزة والشبكات.

مشكلة الدراسة:

أعلنت شركة rend Micro المتخصصة في أمن المعلومات، في تقرير نصف سنوي صدر مؤخرًا أنها عالجت ١٢,٤ مليون تهديد إلكتروني عبر البريد الإلكتروني في مصر في النصف الأول (النصف الأول) من عام ٢٠٢٠. كشف التقرير أيضًا أن حلول Trend Micro حظرت ما يقرب من مليون رابط URL، مما منع المستخدمين من الوصول إليها وأشارت إلى أنه تم اكتشاف أكثر من ٢٣٥ ألف هجوم برمجيات خبيثة في مصر، وتم العثور على أكثر من ٦,٨ مليون تطبيق خبيث للهواتف المحمولة. على المستوى العالمي، تم حظر ٢٧,٨ مليار تهديد إلكتروني في النصف الأول

من عام ٢٠٢٠، مع حدوث ما يقرب من ٩٣٪ من هذه التهديدات عبر البريد الإلكتروني أظهر التقرير تحولًا في الاستراتيجيات التي يستخدمها مجرمو الإنترنت، الذين حولوا تركيزهم خلال النصف الأول من عام ٢٠٢٠ نحو استغلال آثار فيروس كورونا الجديد (COVID-19). تفاقمت المخاطر التي تتعرض لها الشركات بسبب الثغرات الأمنية الناتجة عن العمل عن بعد.. (Alaa El-Din ، ٢٠٢٠)

وبالنظر إلى قطاع التعليم من ضمن القطاعات السابقة سنجد أن العديد من الجامعات قد تعرضت لهجوم وحوادث اختراق فعلى سبيل المثال: ما حدث في عام ٢٠١٥ من تعرض جامعة ميتشجان، جامعة كامبريدج وجامعة أكسفورد للهجوم من قبل مجموعة من الهاكرز المحترفين على شبكة الحاسوب الأكاديمية الممولة من القطاع العام. (حسني،إسراء، ٢٠١٥). كذلك ما تعرضت له جامعة" كشمير" في أغسطس ٢٠٢٢ من تسلل كشف عن المعلومات الشخصية لأكثر من مليون طالب وموظف حالي وسابق. كما أعلن مجلس مدرسة Waterloo Public School أن المتسللين وصلوا إلى قاعدة بيانات الطلاب أثناء هجوم إلكتروني وقع في يوليو ٢٠٢٢ (ALLIANCE، ٢٠٢٢). ومن ثم تطرح الدراسة التساؤل التالي: كيف يمكن مجابهة هذه الظاهرة من خلال الأمن السيبراني والنظافة الرقمية؟

أهداف الدراسة:

هدفت هذه الدراسة إلى تحقيق الأهداف التالية:

١- التعرف على مفهوم كلًا من الأمن السيبراني والنظافة الرقمية.

٢- معرفة خصائص وأهداف كلًا من الأمن السيبراني والنظافة الرقمية.

٣- التعرف على الهجمات التي تعترض عملية الأمن السيبراني وكذلك المشكلات التي تواجه النظافة الرقمية وكيفية التغلب عليهما.

٤- معرفة الدور الذي يؤديه الأمن السيبراني وكذلك النظافة الرقمية في المؤسسات من حيث النهوض بالمؤسسات والتغلب على المشكلات الأمنية وهذا من خلال رصد مزايا وفوائد كلًا منهما

منهج الدراسة وأدواتها:

اعتمدت الدراسة على المنهج الوصفي التحليلي وذلك من خلال الاستعانة بالإنتاج الفكري ذات الصلة بموضوع الأمن السيبراني والنظافة الرقمية.

مصطلحات الدراسة:

الأمن السيبراني: مجموعة التدابير المتخذة للحفاظ على خصوصية المعلومات الإلكترونية وأمانها من التلف أو السرقة. يتم استخدامه أيضًا للتأكد من عدم إساءة استخدام الأجهزة والبيانات. ينطبق الأمن السيبراني على كل من البرامج والأجهزة، وكذلك المعلومات على الإنترنت، ويمكن استخدامه لحماية كل شيء من المعلومات الشخصية إلى الأنظمة الحكومية المعقدة .*Invalid source specified.*

النظافة الرقمية: مصطلح يستخدم لوصف نظافة أو عدم نظافة الوسيط الرقمي أو البنية الرقمية. ويمكن استخدامه لوصف رموز سطح المكتب، أو بنية الملف أو عمليات المجلدات أو ملفات "الفوتوشوب" أو محرك الأقراص الثابتة أو صفحة شخصية على الـ" فيس بوك" (cyborganthropology.2012).

الذكاء الاصطناعي: يشير مصطلح الذكاء الاصطناعي (AI) إلى الأنظمة أو الأجهزة التي تحاكي الذكاء البشري لأداء المهام والتي يمكنها أن تحسن من نفسها استنادًا إلى المعلومات التي تجمعها.

الدراسات السابقة:

هناك عدد من الدراسات التي تناولت موضوع الدراسة سواء باللغة العربية أو باللغة الأجنبية ومن ضمن هذه الدراسات ما يلي:

أولًا الدراسات باللغة العربية:

من بين الدراسات العربية التي تناولت موضوع الدراسة:

☒ دراسة بشائر حامد عبد القادر.(٢٠٢٠).بعنوان " دور الصحف السعودية في تنمية الوعي بالأمن السيبراني : دراسة على القائم بالاتصال "

هدفت هذه الدراسة إلى قياس وعي الصحفيين بموضوع الأمن السيبراني، من خلال التعرف على مدى إلمامهم بمصطلح الأمن السيبراني والمصطلحات المرادفة له، وما مدى معرفتهم بالأنظمة والتشريعات التي تتعلق بالفضاء السيبراني، وماهي الإجراءات والآليات التي تم إتباعها لتوعية أفراد المجتمع بأهمية هذا الموضوع، واعتمدت الدراسة على المنهج المسحي ومن أهم النتائج التي توصلت إليها الدراسة: أن نسبة (٨٤,٣٪) على دراية بمصطلح الأمن السيبراني، في مقابل نسبة من المبحوثين تبلغ (١٥,٧٪) ليسوا على دراية به. كما أوضحت النتائج أسباب اهتمام مبحوثي الدراسة بالأمن السيبراني؛ جاء في مقدمة هذه الأسباب "تعزيز

حماية وسرية وخصوصية البيانات الشخصية" بنسبة (٧٧,١٪). كما حرص مبحوثي الدراسة على إيصال هذه الأنظمة والتشريعات إلى الجمهور من خلال الفنون الصحفية المختلفة؛ "بدرجة كبيرة" بنسبة (٣٨,٦ %)

☒ دراسة أوغلو، أرسين جاهموت. (٢٠١٩). بعنوان" سياسات الإستخبارات والأمن السيبراني في تركيا".

تناولت هذه الدراسة الأمن السيبراني التركي والتهديدات التي تعرضت لها تركيا في ظل الفضاء السيبراني، كما أن هذه الدراسة قد ذكرت أحد عوامل الوقوع في الخطر حيث أن ضعف وعي الأفراد والمجتمعات بالأمن السيبراني وأمن البيانات الحساسة تشكل نقاط ضعف أمنية، وقد تم الاستشهاد بهجوم ستوكسن(Stuxnet) ، الذي حدث في إيران نتيجة ضعف الموظف. كما تناولت بعض من التهديدات التي تهدد الأمن السيبراني. وقد أثمرت الدراسة بأن الحصول على البيانات الحساسة للمؤسسات تتم بطريقة هجمات سيبرانية مختلفة، وهي ما تعرف بالهندسة الاجتماعية، وأن الاهتمام بهذا النوع من التهديدات يتطلب الاهتمام الجاد بالبنية التحتية للنت، واخذ الاحتياطات الضرورية لتحقيق أمن إنترنت الأشياء وكذلك أمن الأنظمة الذكية. ومن ثم ينبغي رفع الوعي بهذه المجالات.

ثانيًا الدراسات باللغة الأجنبية:

من بين الدراسات الأجنبية التي تناولت موضوع الدراسة:

☒ Solms, Rossouwvon & Niekerk, Johanvan .(2013) From information security to cyber security.

تدورهذه الدراسة حول مصطلحي أمن المعلومات والأمن السيبراني حيث كثيرا ما يستخدم مصطلح الأمن السيبراني بالتبادل مع مصطلح أمن المعلومات. ولكن هذه بالرغم من وجود تداخل كبيربين الأمن السيبراني وأمن المعلومات، فإن هذين المفهومين ليسا متشابهين تماماً. وعلاوة على ذلك، تفترض الدراسة أن الأمن السيبراني يتجاوزحدود أمن المعلومات التقليدية ليشمل حماية موارد المعلومات ليس فقط، ولكن أيضا حماية الأصول الأخرى، بما في ذلك الشخص نفسه. في أمن المعلومات، الإشارة إلى العامل البشري عادة ما تتعلق بدور(أدوار) البشر في عملية الأمن. ففي الأمن السيبراني هذا العامل له بعد إضافي، وهو البشر كأهداف محتملة للهجمات السيبرانية أو حتى المشاركة دون علم في هجوم إلكتروني. ولهذا البعد

الإضافي آثار أخلاقية على المجتمع ككل، حيث يمكن النظر إلى حماية بعض الفئات الضعيفة، مثل الأطفال، على أنها مسؤولية مجتمعية.

☒ Wenye, Wang & ZhuoLu(2013). Cyber security in the Smart Grid: Survey and challenges

قامت هذه الدراسة بعمل استبيان شامل لقضايا الأمن السيبراني للشبكة الذكية وعلى وجه التحديد ركزت على مراجعة ومناقشة متطلبات الأمان ونقاط الضعف في الشبكة والتدابير المضادة للهجوم وبروتوكولات الاتصال الآمنة والمعماريات في الشبكة الذكية. كما هدفت الدراسة إلى توفير فهم عميق لنقاط الضعف الأمنية والحلول في الشبكة الذكية وإلقاء الضوء على اتجاهات البحث المستقبلية للشبكة الذكية.

ومن خلال الدراسات السابقة يتضح أنها إما دراسات استطلاعية قد جاءت مبنية على أراء معينة، أو أنها قد جاءت منصبة على منطقة معينة لدراسة التهديدات التي تعترضها في حين ان الدراسة الحالية دراسة نظرية فهي تركز فقط على الجانب النظري من حيث مفهوم وأهداف وأهمية وخصائص كلًا من الأمن السيبراني والنظافة الرقمية وذلك بشكل عام دون ربط الموضوع بحدود مكانية معينة.

ثانيًا الإطار النظري للدراسة

١/ الأمن السيبراني:

يشكل الأمن السيبراني جزءًا أساسياً من أي سياسة أمنية وطنية، حيث بات معلوماً أن صناع القرار في العديد من الدول، أصبحوا يصنفون مسائل الدفاع السيبراني/الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية. بالإضافة إلى ما تقدم، فقد أعلنت أكثر من ١٣٠ دولة حول العالم عن تخصيص أقساماً وسيناريوهات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني. تضاف جميع هذه الجهود إلى الجهود الأمنية التقليدية لمحاربة الجرائم الالكترونية، الاحتيال الالكتروني والأوجه الأخرى للمخاطر السيبرانية (الهيئة المنظمة للإتصالات، ٢٠٠٨). وسوف نستعرض فيما يلي مفهوم وأهمية وخصائص وأهداف الأمن السيبراني.

١/١ تعريف الأمن السيبراني:

فبالنظر إلى التعريفات اللغوية الواردة عن الأمن السيبراني سنجد ما جاء في:

موسوعة " إنفستوبيديا " حيث عرفته على أنه: التدابير المتخذة للحفاظ على خصوصية المعلومات الإلكترونية وأمانها من التلف أو السرقة. يتم استخدامه أيضًا للتأكد من عدم

إساءة استخدام الأجهزة والبيانات. ينطبق الأمن السيبراني على كل من البرامج والأجهزة، وكذلك المعلومات على الإنترنت، ويمكن استخدامه لحماية كل شيء من المعلومات الشخصية إلى الأنظمة الحكومية المعقدة .*Invalid source specified.*

كما عرفه قاموس oxford (cybersecurity, 2020)، وقاموس word-reference على أنه: حالة الأمان من الجريمة الإلكترونية والإجراءات المتخذة لتنفيذ ذلك (cybersecurity، ٢٠٢٠).

قاموس مريام وبستر Merriam-webster حيث عرف مصطلح الأمن السيبراني cybersecurity على أنه:" التدابير المتخذة لحماية الكمبيوتر أو نظام الكمبيوتر (كما هو الحال على الإنترنت) من الوصول أو الهجوم غير المصرح به" (cybersecurity noun، ٢٠٢٠).

وقد وردت كلمة سايبر"Syper" في معجم المعاني؛ بمعنى تخيلي أو تقني (ترجمة و معنى cyber في قاموس المعاني، ٢٠٢٠).

وهناك الكثير من التعريفات والتي ذكرها المؤلفين عن الأمن السيبراني ومن بين هذه التعريفات ما يلي:

وذكره غسان على أنه " عبارة عن مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الوصول غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان تو افرواستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين، والمستهلكين في الفضاء السيبراني (غسان، ٢٠١٩).

وبعدما تم عرضه من تعريفات سابقة للأمن السيبراني، تقوم الدراسة بوضع التعريف الإجرائي التالي وفقًا لمقتضياتها:

الأمن السيبراني هو: مجموعة من الوسائل والتدابير التكنولوجية التي يتم استخدامها سواء من قبل أشخاص، أو هيئات، أو منظمات، أو أي كيانات أخرى، هدفها حماية كل ما يتعلق بها من بيانات، أو أدوات، أو أنظمة وبرامج، أو معدات، أو أجهزة سواء أكانت أجهزة حاسب آلي أو الحاسوب الشخصي أو هواتف ذكية ... غيرها من الدخول غير المصرح به أو المساس بها.

٢/١ أهمية الأمن السيبراني وخصائصه:

تتجلى أهمية الأمن السيبراني في قدرته على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، وبالتالي التخلص من الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا

المعلومات والاتصالات أو بسبب إساءة استخدامها، وكنتيجة حتمية لهذه الأهمية جعلته العديد من الدول على قمة أولوياتها وخصيصًا بعد الحروب الإلكترونية التي بدأت تظهر تجلياتها بين بعض الدول الكبرى، في إشارة صريحة إلى نهاية الحروب التقليدية التي كانت تستخدم فيها الأسلحة الثقيلة، والإعلان عن بداية حروب جديدة هي الحروب الإلكترونية. (الموسوعة السياسية، ٢٠٢٠).

يتميز الأمن السيبراني بمجموعة من الخصائص وهي (الهيئة الوطنية للأمن السيبراني، ٢٠١٨):

١- ضمان الوصول المنطقي إلى الأصول المعلوماتية والتقنية للمؤسسة، وذلك لمنع الوصول غير المصرح به وتقييد الوصول لما هو مطلوب لإنجاز الأعمال المتعلقة بالجهة.

٢- قدرته على حماية أنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية للمؤسسة، وكذلك القدرة على حماية البريد الإلكتروني من المخاطر السيبرانية.

٣- لديه قدرة على حماية وإدارة أمن الشبكات.

٤- ضمان حماية أجهزة المؤسسة المحمولة بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية من المخاطر السيبرانية. وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في المؤسسة.

٥- السرية وسلامة البيانات والمعلومات ودقتها وتوافرها وفق السياسات والإجراءات التنظيمية للمؤسسة.

ترى الباحثة أنه بعدما تم تناول خصائص وأهمية الأمن السيبراني أصبح إلزامًا على كل جهة أو مؤسسة أن تعمل على توفيره (الأمن السيبراني) لحمايتها من أي وصول غير مصرح به فهو يعمل على الوصول المنطقي والمحدود إلى الأصول المعلوماتية الخاصة بالمؤسسات كذلك يمنحها قدرة فائقة في حماية أنظمتها وأجهزتها من المساس الضار بها، والتعامل بشكل آمن مع المعلومات الحساسة الخاصة بالمؤسسة والعاملين بها بما يكفل ضمان سرية وسلامة وتحقيق الأمان للبيانات واستخدامها على النحو الصحيح. يعمل على تقليل احتمالية حدوث الاختراق حيث إن لديه قدرة عالية على التعامل مع الثغرات الأمنية واكتشافها ومعالجتها، وبالتالي

تقليل الآثار المترتبة على حدوث تضارب في الخدمات الإلكترونية التي تقوم المؤسسة بتقديمها وذلك إثر حدوث مخاطر سيبرانية.

٣/١ أهداف الأمن السيبراني:

تتعدد أهداف الأمن السيبراني، ومن بينها ما يلي:

١- تأمين البنى التحتية لأمن المعلومات والبيانات الخاصة بالمواطنين (البكر، ٢٠١٨).

٢- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حدٍ سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة (الرابغي، ٢٠٢٠).

٣- " حماية شبكة المعلومات من أي هجوم وذلك بمعرفة آخر التقنيات والتكنيكيات الموجود في هذا المجال ومن أهمها كشف أهداف رسائل هذا العدو والتعرّف على طبيعة هذا المهاجم وذلك وماذا يريد من خلال معرفة تكنيكاته المستخدمة والأساليب المختلفة لكي يتم العمل على إيقاف هذا الهجوم بأسلوب علمي وتقني مُحكم يمنع هذا الهجوم". (البكر، ٢٠١٨)

٤- حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة، وضمان توافر استمرارية عمل نظم المعلومات (الرابغي، ٢٠٢٠)

ترى الدراسة انه لنجاح أي مؤسسة ينبغي عليها تحقيق الغرض الذي أُقيمت من أجله وهذا الغرض يتحقق من خلاله استقرار المؤسسات وأمانها وأمان عملياتها الأمر الذي يمكن تحقيق من خلال أن تحظى تلك المؤسسات بالأمن السيبراني حيث تأمين بنيتها التحتية فهو أولى الأهداف التي يسعى إليها الأمن السيبراني وبالتالي هذا الأمر يسهم في استقرار المنظمات وحماية معلوماتها ومعلومات العاملين بها وبالتالي تحقيق الأمان النفسي للعاملين يجعلهم يبدعون أكثر في أداء مهامهم الوظيفية كذلك أن الأمن السيبراني في حد ذاته يسعى إلى تحقيق الكثير من الأهداف والتي بدورها تؤدي إلى رفعة المؤسسات سواء أكانت تعليمية أو بحثية أو حكومية وما إلى ذلك الأمر الذي يجعل أي مؤسسة ترغب في الارتقاء من تبني عملية الأمن السيبراني لتحقيق الجانب الأكبر من أهدافها.

شكل (١) أنواع الهجمات التي تعترض الأمن السيبراني

٢/ أنواع الهجمات التي تعترض الأمن السيبراني:

لقد تم تقسيم الهجمات التي تعترض الأمن السيبراني إلى ثلاثة أنواع كما هو موضح بالشكل التالي:

١/٢ الهجمات السيبرانية:

١/١/٢ تعريف الهجمات السيبرانية:

لقد تعددت التعريفات الدائرة حول الهجمات السيبرانية وسنتناول فيما يلي المقصود بها من الناحيتين اللغوية والاصطلاحية.

من خلال البحث في المعاجم اللغوية وجد الآتي أن كلمة هجمات في المعجم الوسيط قد جاءت بالصورة التالية: هَجَمَ عليه هَجَمَ هُجُومًا: دخَلَ عليه بَغتةً (المعجم الوسيط، ٢٠٢٠) .

وعرف قاموس مريام وبستر Merriam-webster الهجوم السيبراني على أنه: محاولة للوصول غير القانوني إلى جهاز كمبيوتر أو نظام كمبيوتر بغرض إحداث ضرر، واستغلال هذا الوصول الخفي لجمع المعلومات الاستخبارية، وفي بعض الأحيان لتقديم هجوم إلكتروني مدمر.

يتضح من خلال هذا التعريف أنه قد جاء من منظور عسكري أو سياسي حيث أن الهدف من الهجوم فيه قد جاء منصبًا على جمع المعلومات الاستخبارية.

وقد جاء معنى السيبرانية في قاموس المورد بأنها: "هي علم الضبط، ومصدرها Cybernetics (البعلبكي، ٢٠٠٤).

وجاءت كلمة Cyber في قاموس word reference بمعنى إلكتروني، سيبراني، على الإنترنت، عبر الإنترنت.

هذا وقد ذكر أحمد عبيس، ونعمة الفتلاوي أن كلمة سايبر (Cyber) كلمة يونانية الأصل ومصدرها (cybernetes) والذي كان بداية استخدامه في مؤلفات الخيال العلمي ويعني القيادة

أو التحكم عن بعد (أحمد و الفتلاوي، ع٤، ٢٠١٦). وكلمة Cyber في قاموس المعاني تعني " تخيلي".

ومن خلال التعريفات اللغوية لـــ لفظ السيبرانية، أو كلمة Cyber يمكن القول بأن الهجمات السيبرانية Cyber Attack، يقصد بها من الناحية اللغوية الهجوم الي يتم عبر الإنترنت، حيث أن كلمة هجوم واضحة المعنى من مسماها وأن كلمة السيبرانية كلمة تقنية تعني إلكتروني أو تقني أو عبر الإنترنت.

وبالنظر إلى الهجمات السيبرانية من الناحية الاصطلاحية سنجد أن لها الكثير من التعريفات ومن بينها:

تعريف Michael N. Schmitt حيث عرفها على أنها:" تلك الإجراءات التي تتخذها الدول من أجل الهجوم على نظم المعلومات للعدو وبهدف التأثير والإضرار فيها، والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة" (Schmitt, 1998– 1999, Vol. 37,).

كما عرفها "Fuertes " بأنها هجوم عبر الإنترنت يقوم على التسلل إلى مواقع إلكترونية غير مرخص بالدخول إليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها، وهى عبارة عن سلسلة هجمات إلكترونية تقوم بها دولة ضد أخرى" (أحمد و الفتلاوي، ع٤، ٢٠١٦).

وترى الدراسة أن هناك تو افق في وجهات النظر بين تعريف Michael (1999) وتعريف Fuertes (2016) حيث إن كلاهما قد جاء وفقًا لرؤية سياسية واضحة فالأول هدفه الهجوم على أنظمة المعلومات المتعلقة بالعدو أو الخصم، وفي المقابل حماية نظم المعلومات الخاصة بالدولة التي تقوم بشن الهجوم. والثاني: قد ذكر ان هذه الهجمات تقوم من قبل دول وضد أخرى أي أن مخزاه حرب سيبرانية، الأمر الذي يجعلنا نقول إن هدفهما سياسي.

وهي أيضًا: " أي هجوم يحدث بشكل أساسي عبر شبكة كمبيوتر، حيث يكون الكيان الذي يتم مهاجمته عبارة عن شبكة أو نظام كمبيوتر (أو كليهما)" (Layton، ٢٠١٦).

عرفها موقع phoenixnap على أنها: استغلال متعمد لأنظمة الحاسوب والشبكات والمؤسسات المعتمدة على التكنولوجيا. باستخدام تعليمات برمجية ضارة لتعديل كود الحاسوب أو البيانات أو المنطق. تؤدي إلى عواقب مدمرة يمكن أن تعرض بياناتك للخطر وسرقة الهوية، يطلق على الهجمات السيبراني أيضًا هجوم شبكة الحاسوب (CNA) (phoenixnap، ٢٠١٩).

ويتضح من خلال التعريفات السابقة أن جميعها قد إشترك في كون أن هذه الهجمات تتم بصورة إلكترونية.

نظرًا لما قد جاء في التعريفات السابقة واختلاف رؤيتها عن الدراسة الحالية التي تجريها الباحثة، قامت الباحثة بصياغة التعريف الإجرائي التالي وفقًا لما يتماشى مع مفهوم دراستها: - الهجمات السيبرانية: هي عبارة عن هجمات محددة في أهدافها وتتم بصورة مقننه محددة في ذهن المهاجم لأهداف عدة قد تكون سياسية، أو قومية، أو غيرها، ولكنها بالطبع أهداف تدميريه يترأسها الوصول خلسة إلى نظام معلوماتي قد يكون مؤمن أو لا بهدف الاستيلاء على ما به من معلومات لأهداف أخرى قد تكون مادية أو بغرض تشويه السمعة أو بغرض إتلاف البيانات والتلاعب بالأشخاص والكيانات التي تحتوي هذه المعلومات ضمن أنظمتها وأجهزتها أو لأية أهداف أخرى في ذهن المهاجم. مستخدمًا بعض السبل المتعارف عليها لتحقيق هدفه كالبرامج الضارة...

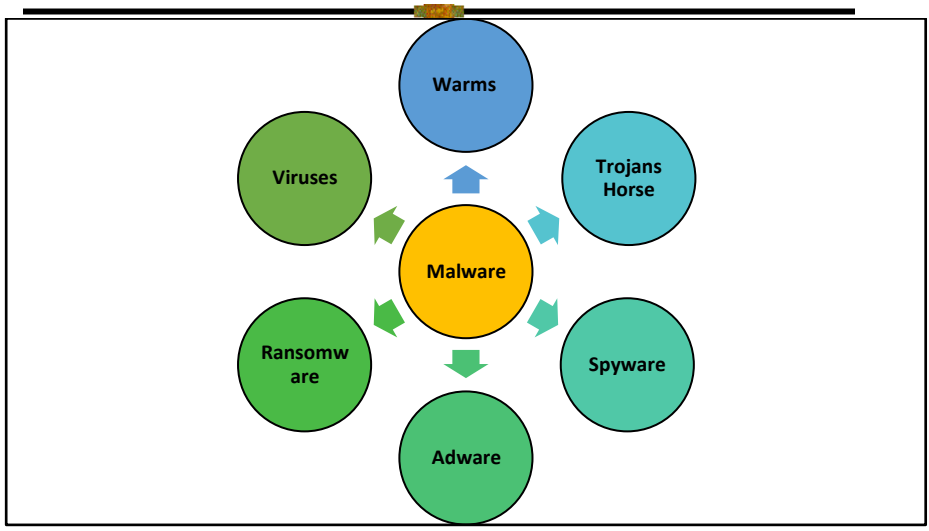
٢/١/٢ أنواع الهجمات السيبرانية:

تتعدد أنواع الهجمات السيبرانية التي يقوم بها المهاجمين، وسوف نتناول فيما يلي أشهر الأنواع التي من شأنها إلحاق الضرر بالأجهزة أو الأنظمة أو الشبكات بهدف الإضرار بالمعلومات وتهديد البيانات:

أ- البرامج الضارة Malware:البرامج الضارة (بهاء،قيصر، بلا تاريخ): مصطلح شامل لمجموعة متنوعة من التهديدات السيبرانية، وهي عبارة عن برمجيات يتم برمجتها لاستهداف وظائف الحاسوب وتدميرها وربما سرقة البيانات أو استهداف نظم الحماية للحاسوب وتخطيها للتحكم في عمل الحاسوب.

ويشتمل هذا النوع من الهجمات السيبرانية على عدة أنواع بداخلها ويمكن توضيحها من خلال الشكل التالي:

شكل (٢) أشهر أنواع البرامج الضارة.



وسوف نتناول بعض من المعلومات عن كل نوع من الأنواع السابقة فيما يلي:

١/أ الفيروسات Viruses:

برامج لها القدرة على نَسْخ نفسها أكثر من مرَّة، ويَمتاز بقدرته على التخفِّي، وله آثار تدميريَّة على أنظمة تشغيل الحاسوب؛ لأنَّ عملية النَّسْخ والتَّكرار الدائم لِملفَّاته تَجْعل هذه الملفات تحلُّ مَحلَّ الملفات الأصلية الموجودة على القرص الصلب Hard Disk للحاسوب (المجدوب، أحمد المهدي، ٢٠١٧). وتمر دورة حياة الفيروس بعدة مراحل للإضرار بجهاز الكمبيوتر، وهذه المراحل هي (Birleanu, Anghelescu, & Bizon, 2018) :

- مرحلة الخمول: عندما يكون الفيروس خاملاً في انتظار تنشيطه من قبل المستخدم.
- مرحلة الانتشار: وفيها يقوم الفيروس باستنساخ نفسه في برنامج معين من البرامج المحفوظة على جهاز الحاسب الآلي.
- مرحلة التفجير والتنفيذ: يقوم فيها الفيروس بالتحرك في تنفيذ الوظائف المطلوبة منه، والتي قد تكون تدمير البرامج أو تسريب المعلومات أو إتلافها.

٢/أ الديدان Warms:

عبارة عن برامج تنتقل غالبًا عبْر البريد الإلكتروني، وتَمتاز بقدرتها على التنقُّل عبْر شبكات الإنترنت؛ لغرَضِ تعطيلها أو التشويش عليها عن طريق شلِّ قدرتها على تبادل المعلومات (خميس، ٢٠١٨). فعادةً ما يكون الهدف منها نفس الأهداف الخاصة بالفئتين السابقتين وهو

إحداث الضرر بأنظمة الكمبيوتر لتدمير المعلومات التي يحتويها، أو لجمع المعلومات الشخصية بدون علم صاحب جهاز الكمبيوتر (جوهري و طه، ٢٠٢٠).

وفي الغالب تنتشر هذه الديدان ذاتياً عبر شبكة الإنترنت من خلال وجود الثغرات الأمنية الموجودة في نظام أمن المعلومات حي أنها تشكل نقاط ضعف تستغلها هذه البرامج للتسلل إلى الجهاز (Benarous, Leila, & Nouridane, 2017).

٣/أ أحصنة طروادة: Trojans Horse

وهى برامج تجسسيه، تقوم بعمل معيَّن يحدِّده الشَّخصُ الذي صمَّمَه أو زرَعَه في جهاز الضحية، يُمكِّنه من الحصول على مبتغاه (المجدوب، ٢٠١٧) ، وهى من البرمجيات الضارة التي تظهر في شكل برامج مشروعة ولكنها تخفي في داخلها برامج ضارة حتى يقوم الضحية بتثبيتها على جهازه أو تشغيلها لكي يتمكن المخترق من الوصول عن طريقها إلى جهاز الضحية ويتم تصميمها بحيث يمكن تحميلها عن طريق الإنترنت وبمجرد تحميلها تقوم هذه البرمجيات على إعادة تسمية البرامج المثبتة على جهاز الضحية أو حذفها بالكامل، بالإضافة إلى سرقة كلمات السر وتعطيل الجهاز عن العمل أو ضرب برامج الحماية من الفيروسات (Chiew, Yong , & Chek, 2018).

٤/ أ برامج التجسس: Spyware

تقوم هذه البرامج على رصد ومر اقبة كل ما يقوم به الضحية فهي تسجل كل نقرة على لوحة المفاتيح (Hassan & Hijazi, 2018).

كما تقوم بجمع معلومات حول ما يقوم به المستخدم من أنشطة سواء في حالة الاتصال بالإنترنت أو عدمه، ثم يتم ارسال هذه المعلومات إلى المخترق فور الاتصال بالإنترنت (A. & M., 2017).

٥/أ برامج الفدية Ransomware:

وهذه البرامج مهمتها منع تمنع الضحايا من الوصول إلى بياناتهم، وعادة ما تهدد بحذفها في حالة عدم دفع الفدية. كما أن ليس هناك ما يضمن أن دفع الفدية سيعيد الوصول إلى البيانات، غالبًا ما يتم تنفيذ برامج الفدية عبر حصان طروادة لتقديم حمولة متخفية كملف شرعي.

٦/أ برامج الإعلانات المتسللة Adware:

برامج إعلانية يمكن استخدامها لنشر البرامج الضارة (kaspersky، ٢٠٢٠). كذلك من ضمن الهجمات السيبرانية:

ب- هجوم man-in-the-middle:

هو نوع من الهجمات السيبرانية يعترض فيه المهاجم الإنترنت الاتصال بين شخصين لسرقة البيانات. مثلًا: في شبكة WiFi غير آمنة، يمكن للمهاجم اعتراض البيانات التي يتم تمريرها من جهاز الضحية والشبكة (kaspersky، ٢٠٢٠).

٢/٢ هجمات الهندسة الاجتماعية

لإيضاح مفهوم هجمات الهندسة الاجتماعية ينبغي عرض بعضًا من مفاهيم الهندسة الاجتماعية حيث أن مفاهيم الأخيرة قد تعددت ومن بينها ما يلي:

عرفها معجم المعاني بأنها: " مجموعة من التقنيات المستخدمة لتضليل المستخدمين الداخليين للقيام بإجراءات معينة أو كشف معلومات سرية". (almaany، ٢٠٢٢)

بينما عرفها (conteh & Schmick, 2016) بأنها: " إحدى أبسط الطرق لجمع المعلومات حول الهدف من خلال عملية استغلال الضعف البشري الموروث لكل مؤسسة"..

وقد عرفتها مها أحمد (إبراهيم، ٢٠١٩).على أنها: استخدام المخترق لمجموعة من الحيل النفسية من شأنها خداع مستخدمي الكمبيوتر تمكنه من الوصول إلى أجهزة الكمبيوتر أو المعلومات المخزنة فيها كنتيجة لما قد يتوهم به بعض الناس، ومن هنا يجب أن تكون الهندسة الاجتماعية على قمة قائمة وسائل الاختراق والهجمات الإلكترونية التي ينبغي حماية المعلومات منها

أو أنها: قدرة المخترق على الحصول على معلومات هامة وسرية باستخدام أسلوب من أساليب الاحتيال العقلي والتلاعب، حيث يتم من خلاله اقتحام شبكةٍ ما أو نظام تشغيلي ما نتيجة الخطأ البشري فالهندسة الاجتماعية تكمن في البحث عن أي أخطاء بشرية من أجل أن يتمكن المخترق من الحصول على غايته كالثقة الزائدة أو الفضول، أو عدم التركيز فيبدأ الاختراق باكتشاف نقاط الضعف التي يمكن استغلالها (إبراهيم، ٢٠١٩).

وعرفها كلًا من Kunwar,Bansla&Gupt على أنها: أسلوب قائم على السلوك البشري لاختراق عقول الأشخاص واستدراجهم للتسلل إلى الأنظمة الخاصة بهم (Bansla, Kunwar, & Gupta, 2019).

كما تعرف على أنها:" أي فعل يؤثر على شخصٍ ما في اتخاذ إجراء قد يكون أو لا يكون في مصلحته"(Social Engineerin,iNC. , 2020) .

١/٢/٢ المقصود بهجمات الهندسة الاجتماعية: -

ومن خلال ما سبق عرضه من تعريفات لمصطلح الهندسة الاجتماعية يمكن تعريف هجمات الهندسة الاجتماعية على أنها: تلك الهجمات التي يقوم بها المخترقين مستخدمين فيها مجموعة من الأساليب التي تمكنهم من الحصول على المعلومات التي يريدونها من الضحايا وهذه الأساليب هي التي تعرف بأساليب الهندسة الاجتماعية، والتي تعتمد في تطبيقها على الخداع والتلاعب بالعقول وهو الأمر الذي يعكس في طياته مفهوم الهندسة الاجتماعية.

٢/٢/٢ أنواع هجمات الهندسة الاجتماعية:

تُعد هجمات الهندسة الاجتماعية النمط الثاني من أنماط الهجمات التي تعترض عملية الأمن السيبراني ويشتمل على الأنواع التالية:

أولًا هجمات معتمدة على العامل التقني:

أ/ التصيد: الذي يُعد الشكل الأكثر شيوعًا من بين هجمات الهندسة الاجتماعية ويعتمد على استغلال الخطأ البشري؛ للحصول على البيانات أو نشر البرامج الضارة، أو إرسال مواقع عبر البريد الإلكتروني تحيل إلى روابط ويب ضارة (IT Governance Ltd، ٢٠٠٣-٢٠٢٠).

ويشتمل هذا النمط على أنماط أخرى كالتصيد الإحتيالي Phishing: ويقصد به هجمات التصيد التي تتم عبر حسابات خدمة العملاء المزيفة على وسائل التواصل الاجتماعي، اختراق البريد الإلكتروني: وفي هذا النوع يتم إرسال رسائل نصية عبر البريد الإلكتروني يُزعم أنها من كبار الموظفين للتسلل إلى الأعمال (IT Governance Ltd، ٢٠٠٣-٢٠٢٠).

ووفقًا لما أصدرته "Kaspersky Lab" فقد زادت محاولات التصيد الاحتيالي بمقدار ٣٠ مليونًا من عام ٢٠١٧ إلى عام ٢٠١٨. (phoenixnap، ٢٠٢٠)

ب/ التصيد الاحتيالي عبر الرسائل القصيرة Phishing SMSهنا تُستخدم الرسائل النصية على أنها من كيانات شرعية موثوقة بالإضافة إلى بعض التقنيات الأخرى لتجاوز المصادقة الثنائية، وقد يقومون أيضًا بتوجيه الضحايا إلى مواقع الويب الضارة على هواتفهم، كما يمكن أيضًا استخدام صورة أخرى من هذا النمط وهي الرسائل المسجلة حيث يتم إخبار المستلمين بأن حساباتهم المصرفية قد تعرضت للاختراق ومن ثم يُطلب منهم إدخال البيانات عبر لوحة مفاتيح

الهاتف، وبالتالي يمكن الوصول إلى حساباتهم المصرفية. (IT Governance Ltd، ٢٠٠٣-٢٠٢٠).

ج/ الاصطياد Baiting:وهذا النوع يتم استخدامه في العالمين الرقمي والمادي، ويختلف عن سابقيه في الوسيلة حيث يعتمد على ترك محركات الأقراص(USB) في مناطق معينة كالمكتبات ومحطات المترو وخلافة ، وذلك بغرض من جذب فضول الأفراد؛ وهنا يقوم المستخدم باستخدام الأداة المتروكة وبمجرد توصيلها بجهازه يتم تنزيل البرامج الضارة على القرص الصلب، ومن ثم تبدأ هذه البرامج بممارسة عملها أيًا كانت طبيعتها سواء أكانت برامج تجسس أو غيرها مرسلة البيانات مباشرةً إلى المتسلل؛ ومن ثم إتاحة الفرص له بالوصول إلى مو اقع الويب والحسابات (phoenixnap، ٢٠٢٠).

وقد يأتي الاصطياد الرقمي في صورة إعلانات مغرية، أو عناصر مجانية يكون الهدف من ورائها توجيه المستخدمين إلى مو اقع الويب التي تؤدي إلى تنزيل البرامج الضارة. كما قد يتم إخفاء برامج التجسس، والبرامج الضارة في صورة تحديثات برامج أو برامج تقليدية (phoenixnap، ٢٠٢٠).

د/ المقايضة quid pro quo يقدم هذا النوع من الهجمات كخدمة فنية في المقابل للحصول على المعلومات. يتمثل التهديد الشائع في قيام المهاجم بانتحال شخصية ممثل لتكنولوجيا المعلومات وتقديم المساعدة للضحية التي قد تواجه تحديات تقنية (conteh و Schmick، ٢٠١٦). "على سبيل المثال، قد يتلقى المستخدم النهائي مكالمة هاتفية من المتسلل الذي يقدم، بصفته خبيرًا تقنيًا، مساعدة مجانية لتكنولوجيا المعلومات أو تحسينات تقنية في مقابل بيانات اعتماد تسجيل الدخول" (HEINBACH, 2020).

هـ/ التتبع Tailgating: وهذا النوع من الهجوم يستخدم خاصية الرجوع إلى الخلف والوصول إلى المناطق المحظورة. فقد ينتحل شخصية موظف التوصيل أو غيره ممن قد يحتاجون إلى وصول مؤقت (conteh و Schmick، ٢٠١٦).

و/ التصيد بالرمح: شكل أكثر تعقيدًا من التصيد الاحتيالي حيث يتعرف المهاجم على الضحية وينتحل شخصية شخص يعرفه ويثق به (TAYLOR, 2020).

ثانيًا: هجمات معتمدة على العامل البشري: -

وهذه الأنواع بخلاف سابقتها فهي تعتمد على الإنسان فهي تتم من الإنسان إلى الإنسان دون تدخل التقنية كما سيتضح فيما يلي:

أ/ الإقناع: عن طريق التحدث مع الشخص المطلوب استدراجه وتشجيعه للإفصاح بالمعلومات سواء أكانت هذه المعلومات سرية أولها علاقة بهدف المخترق، وذلك من خلال ترك انطباع جيد لدى الضحية من خلال أساليب عدة للإقناع، كي يتمكن المخترق من الحصول على المعلومات التي يريدها (إبراهيم، ٢٠١٩).

ب/ الهندسة الاجتماعية المعاكسة: تتم عن طريق الإيحاء للضحية بأنك شخص مهم أو ذو صلاحيات عليا بحيث يقوم المهاجم بإعطاء معلومات يريدها الضحية وإذا ما نجح الأمروسارت الأموركما خُطط لها فقد يحصل المهاجم على فرصة أكبرللحصول على معلومات ذات قيمة كبيرة من الضحية، وهذا الأسلوب معقد نسبياً كونه يعتمد على مدى التحضيرالمسبق وحجم المعلومات التي بحوزة المهاجم (الهندسة الاجتماعية Social engineering و أساليب الإختراق، ٢٠١٦)، وهذا الأسلوب يشبه أسلوب المقايضة كما في أنواع الهندسة الاجتماعية التي تعتمد على التقنية.

ج / الانتحال:وغالبًا ما تتم عن طريق الهاتف فهي لا تستدعي الحضوروجهًا لوجه، بينما تتطلب بعض المعلومات كالاسم وتاريخ الميلاد... (إبراهيم، ٢٠١٩).

د/ التجسس والتصنت: حيث يمكن استخدامهما عند مر اقبة الضحية حين كتابة معلومات مهمة أو التصنت عليها عند إجراء مكالمة هاتفية، والحصول على كلمات المرور(إبراهيم، ٢٠١٩).

٣/٢/٢ هجمات الويب Web Attacks:

١/٣/٢/٢ المقصود بهجمات الويبWeb attacks :يمكن تعريف هجمات الويب على أنها: تلك الهجمات التي يكون الهدف منها تطبيقات الويب والتي تُعد أحد أكبر التهديدات لأمن المؤسسات، وأمن البيانات، والتي من الممكن أن تؤدي إلى مجموعة واسعة من العو اقب المدمرة من انقطاع الخدمة وإغلاقها إلى سرقة المعلومات والتلاعب بالبيانات (pentasecurity، ٢٠٢٠).

كما تعرف على أنها: قدرة المهاجمين على الوصول المباشر إلى قواعد البيانات، بهدف تغيير البيانات الحساسة أو خرقها، كما قد يكون الهدف تشويه وذلك من خلال نقاط الضعف الناجمة عن الترميزغيرالمناسب أونقاط الضعف العامة (acunetix، ٢٠٢٠).

وتتبنى الدراسة التعريف الأول لهجمات الويب لسببين:

- الأول: أنه قد جاء معممًا لكافة التطبيقات.

- الثاني: أنه قد جاء مشتملًا على بعض الصور التي تتم من خلالها تلك الهجمات.

٢/٣/٢/٢ أنواع هجمات الويب Web attacks:

أ- حقن SQL ويُعرف أيضًا باسم SQLI، وهو نوع من الهجمات التي تستخدم تعليمات برمجية ضارة للتعامل مع قواعد البيانات الخلفية للوصول إلى المعلومات التي لم يكن الغرض منها عرضها. ويشتمل ذلك على العديد من العناصر بما في ذلك قوائم المستخدمين، أو تفاصيل العملاء الخاصة، أو بيانات الشركة الحساسة، كما قد ينتج عنها حذف جداول بأكملها، وعرض غير مصرح به لقوائم المستخدمين، ورغم أن هذا الهجوم يستخدم لمهاجمة قاعدة البيانات إلا أن الجناة عادةً ما يستهدفون مواقع الويب (phoenixnap، ٢٠١٩).

ب- هجوم رفض الخدمة الموزع (DDoS) يهدف هذا الهجوم إلى إغلاق شبكة أو خدمة، مما يجعل الوصول إليها غير ممكن للمستخدمين المقصودين (phoenixnap، ٢٠١٩). وذلك من خلال ارسال عدد كبير من الأوامر والرسائل مثل أمر (Ping) باستخدام أدوات معينة ترسل عبر الإنترنت إلى جهاز الضحية بهدف إغراقه في معالجة هذه الطلبات، وبالتالي التوقف عن أداء الخدمة، ومن ثم يمكن استغلال الثغرات في وقت توقف الجهاز للوصول غير المصرح به للبيانات، و إتلافها، وتعطيل الخدمة ومنع المستخدمين الشرعيين من الوصول إليها (جوهري و طه، ٢٠٢٠).

ج - هجوم حقن أوامر نظام التشغيل OS command injection attack وهذه العملية تتم عندما يقوم المهاجمون بإدخال أوامر نظام التشغيل (OS) في الخادم الذي يقوم بتشغيل تطبيق الويب. وهذه تختلف عن حقنة SQL لأنها تدخل من جانب الخادم بدلاً من جانب التطبيق. ورغم ذلك، إلا أن العواقب تشبه إلى حد كبير هجوم حقن SQL، حيث يستطيع المهاجم التحكم الكامل في التطبيق، أو إصدار أوامر للتطبيق لعرض معلومات حساسة، تعديل البيانات أو حذفها، استغلال التطبيق للسيطرة على أجزاء أخرى من شبكة المؤسسة مما يؤدي إلى مزيد من الهجمات بداخلها. (pentasecurity، ٢٠٢٠).

د- هجوم البرمجة النصية عبر المواقع Cross site scripting attack(XSS) يحدث هجوم البرمجة النصية عبر المواقع عندما يكون موقع الويب به ثغرة أمنية تسمح بإدخال البرامج النصية. فيستغل المهاجم هذه الثغرات الأمنية ويقوم بحقن جافا سكريبت ضار في قاعدة بيانات موقع الويب. عندما يطلب المستخدم هذه البيانات في وقت لاحق، سيقوم متصفح

الويب الخاص بالمستخدم بتنفيذ جافا سكريبت الضار، مما يتيح للمهاجم الفرصة بسرقة ملفات تعريف الارتباط للمتصفح لاختطاف الجلسة يمكن للمهاجمين بعد ذلك استخدام معلومات الجلسة لاستغلال نقاط الضعف الإضافية، وربما الحصول على معلومات الشبكة والتحكم في كمبيوتر المستخدم. وتضح أهميته بشكل خاص لبيئة الشركة لأن هجوم البرمجة النصية عبر المواقع واحد يمكن أن يعرض الشبكة بالكامل للخطر (pentasecurity، ٢٠٢٠).

هـ- هجوم حقن injection attack LDAP " بروتوكول الوصول الخفيف إلى الدليل (LDAP) هو بروتوكول يستخدم في الغالب لشبكات الإنترانت الخاصة بالشركات. إنه يمكّن أي شخص على الشبكة من العثور على موارد من دليله، مثل الأفراد الآخرين، والأجهزة، والملفات، بالإضافة إلى أسماء المستخدمين وكلمات المرور كجزء من نظام الدخول الموحد (SSO). يحدث هجوم حقن LDAP عندما تسمح الثغرة الأمنية للمهاجمين بإرسال استعلامات دون التحقق المناسب من الصحة. يمكن للمهاجمين بعد ذلك تغيير الاستعلامات للوصول إلى الموارد الهامة، مما يؤدي إلى عواقب وخيمة". (pentasecurity، ٢٠٢٠)

و- هجوم كلمة المرور أي محاولة فك تشفير كلمة مرور المستخدم أو الحصول عليها بنوايا غير شرعية، عادةً ما يتم تنفيذ هجمات كلمات المرور من خلال استعادة كلمات المرور المخزنة أو المصدرة من نظام كمبيوتر. فغالبًا ما يتم استعادة كلمة المرور عن طريق التخمين المستمر لكلمة المرور بواسطة خوارزمية الكمبيوتر (phoenixnap، ٢٠١٩).

ز- هجوم التنصت: تبدأ هجمات التنصت باعتراض حركة مرور الشبكة، ويعد خرق التنصت، المعروف أيضًا باسم التطفل أو الاستنشاق، هجومًا لأمن الشبكة ويقوم فيه المهاجم بسرقة المعلومات التي ترسلها أو تستقبلها الهواتف الذكية وأجهزة الكمبيوتر والأجهزة الرقمية الأخرى. يستفيد هذا الاختراق من عمليات إرسال الشبكة غير الآمنة للوصول إلى البيانات التي يتم إرسالها. (phoenixnap، ٢٠١٩)

هذه الهجمات يكون هدفها عمليات الإرسال الضعيفة بين العميل والخادم بحيث يستطيع المهاجم تلقي عمليات إرسال الشبكة. ومن م تثبيت شاشات الشبكة على الخادم أو الكمبيوتر لتنفيذ هجوم تنصت واعتراض البيانات أثناء إرسالها. ويعد أي جهاز داخل شبكة الإرسال والاستقبال نقطة ضعف، بما في ذلك الجهاز الطرفي والأجهزة الأولية نفسها (phoenixnap، ٢٠١٩).

٤/٢/٢ دوافع القيام بالهجمات السيبرانية/ الهندسة الاجتماعية/ الويب:

إن الهجمات بأنواعها سواء أكانت هجمات سيبرانية أو هجمات هندسة اجتماعية أو خلاف ذلك فإن دوافعها كدوافعها من الجرائم التي تتم في الصرح المعلوماتي والرقمي، ومن ثم يمكن عرض الدوافع الكامنة وراء هذه الهجمات في النقاط التالية:

١/٤/٢/٢ دوافع الاقتصادية: وهي تتدرّج من تأمين الحاجات المالية الفردية إلى المعارك التنافسية بين المؤسسات التجارية، حيث بات عدد كبير من الشركات التجارية يستخدم الهجمات لسرقة معلومات تتعلَّق بأعمال شركات منافسة وعملائها وموظفيها ومناقصاتها للإيقاع بالمنافس أو القضاء عليه (ضوميط وصقر، ٢٠١١).

٢/٤/٢/٢ دوافع سياسية وأمنية: حيث تسعى بعض الدول إلى الحصول على الأسرار العسكرية والأمنية لدول أخرى عن طريق التجسُّس الإلكتروني، ما يتيح لها معرفة خططها العسكرية والاستراتيجية وإحباطها إذا ما اضطرت إلى ذلك. (ضوميط وصقر، ٢٠١١).

٣/٤/٢/٢ دوافع عقائدية :حيث يقوم بعض المجموعات التي تتبنَّى فكرة الإصلاح، بعملية رقابة أخلاقية أو اجتماعية أو دينية، فتتجسّس على المواقع التي تقدِّم خدمات أو معلومات تتعارض مع قناعاتها، وتعمل على كشف أسرارها أو حتى تدميرها (ضوميط وصقر، ٢٠١١)

٤/٤/٢/٢ حب التعلم: حيث يعتقد المهاجم أن أجهزة الحاسوب والأنظمة هي ملك للجميع وأن المعلومات ليست حكرًا على أحد وعلى الجميع الاستفادة منها (فاروق وخديجة، ٢٠١٥).

٥/٤/٢/٢ التسلية واللهو: فكثير من المهاجمون يعتبرون عملهم هذا مجرد وسيلة للتسلية والمرح (فاروق وخديجة، ٢٠١٥).

٦/٤/٢/٢ الرغبة الشخصية: وقد تكون بسبب المشاكل التي يواجهها المهاجم أو ظروف البيئة المحيطة به حيث تزرع بداخله رغبة الانتقام ووجود مثل هذه الأنظمة الإلكترونية تسهل له القيام برغباته فيعبث بمحتوياتها إلى درجة التخريب، أو يكون بدافع التحدي وإثبات الجدارة أمام الأخرين بقدرته على اختراق أنظمة الحاسوب والمساس بها (فاروق وخديجة، ٢٠١٥).

٣/ النظافة الرقمية:

ترى الدراسة أن النظافة الرقمية بمثابة نموذج جيد لتقليص تكلفة الأمن السيبراني فهي تعمل على تعزيز قيمته دون الحاجة إلى تكاليف باهظة، فهي تعمل علة تقليل عمليات التسلل للأنظمة والشبكات من خلال اتباع نموذج جيد من ممارساتها، وبالتالي تقليل عمليات الاختراق. وفي هذا الصدد قد أفادت جارتنرGartner " أن متوسط الإنفاق السنوي على الأمن السيبراني لكل موظف قد تضاعف، من ٥٨٤ دولارًا في عام ٢٠١٢ إلى ١١٧٨ دولارًا في عام ٢٠١٨". ومع زيادة الإنفاق، نلاحظ أن المؤسسات لديها أدوات أمن إلكتروني جديدة أكثر فعالية وبالتالي فهي أكثر أمانًا، ولكن ليس بالضرورة أن زيادة الإنفاق تؤدي إلى زيادة الأمان فإن هذا لا يعالج المشكلة، ومن ثم بحثت الشركات طويلًا عن كيفية إدارة هذه الأدوات والمعدات بالشكل الأمثل لضمان نجاحها وتحقيق الغاية المرجوة منها وهذا الأمر الذي تقوم به النظافة الرقمية (merlin، ٢٠١٩).

١/٣ نشأة النظافة الرقمية:

لقد تم استخدام مصطلح Cyber Hygiene لأول مرة بواسطة Vint Cerf في عام ٢٠٠٠، وأشار إليه على أنه "الخطوات التي نعلم أنه يمكن اتخاذها لتحسين الأمن والمرونة" (merlin، ٢٠١٩)، ويقال أنه صاغ مصطلح "النظافة الرقمية " أثناء التفكير في تنظيف الأسنان. ورأى أوجه التشابه بين العناية الوقائية بالفم والأمن السيبراني الوقائي (CYBER HYGIENE: A COMPLETE GUIDE, 2020).

وفي الآونة الأخيرة، أطلق مركز أمن الإنترنت (CIS) ومجلس الأمن السيبراني (CCS) حملة نظافة الإنترنت وقاموا بتقسيم هذه الخطوات إلى "خمس أولويات قصوى". وهما (merlin، ٢٠١٩).

- العد: ينبغي التعرف على ما هو موجود في الأنظمة الحالية وما هو بحاجة إلى حماية.
- التكوين: إدارة الأنظمة باستمرار باستخدام تكوينات "جيدة معروفة"
- التحكم: معرفة وتحديد من لديه الامتيازات الإدارية لإعدادات الأمان.
- التصحيح: من حيث تحديث البرامج والأجهزة للحماية من الثغرات الأمنية المعروفة.
- التكرار: حيث أن الأمن السيبراني عملية تكرارية وليست نهائية.

وبالنظر إلى كلمة النظافة سنجد أنها كلمة يونانية قديمة، ووفقًا لمنظمة الصحة العالمية، فهي تشمل ممارسات النظافة الشخصية التي تمنع انتشار الأمراض للكائنات الحية. وتشمل أنواع مختلفة من ممارسات النظافة الصحية مثل غسل اليدين والاستحمام إلى طب الأسنان أو صحة الفم، نظافة النوم، نظافة الطعام ...وغيرها، والملاحظ أن هناك ثلاث جوانب حول كيفية تفسير النظافة في أدبيات الصحة العامة (Vishwanatha، Neob، و Gohb، ٢٠١٩).

أولاً: النظافة هي مفهوم متعدد الأبعاد، مع العديد من الجوانب الأساسية التي تحكم العناصر الفرعية المختلفة التي تشكل كليًا نظافة الشخص (Vishwanatha، Neob، وGohb، ٢٠١٩).
ثانيًا: عادة ما تكون النظافة بمثابة دليل، حيث ينصب التركيزعلى ما يجب أن يفعله شخص ما ويجب أن يكون على دراية به. على سبيل المثال، يعتبرغسل اليدين إجراءً شاملاً يتوقع أن يكون كثيرمن الناس على دراية به والانخراط فيه، بصرف النظرعما إذا كان الناس يستوعبون عملية انتقال المرض (Vishwanatha، Neob، وGohb، ٢٠١٩).
ثالثًا: أن معظم ممارسات النظافة متجذرة في الوقائع السياقية والثقافية، فعادة ما يتم تعريف النظافة على نطاق واسع، فمثلًا، على سبيل المثال، قد يغسل الأشخاص الذين يعملون في أماكن الرعاية الصحية أيديهم بشكل متكرر، حتى باستخدام مواد كيميائية أكثر قسوة وتطهير، في حين أن الأشخاص الذين لا يعملون في مثل هذه الأماكن قد يقومون بذلك ببساطة عدة مرات باستخدام الصابون والماء (Vishwanatha, Neob, & Gohb, 2019).
فغالبًا ما تتم مقارنة النظافة الرقمية بالنظافة الشخصية فكما يمارس الأفراد النظافة الشخصية للحفاظ على حالة جيدة من الصحة، فكذلك ممارسات النظافة الرقمية يمكنها أن تحافظ على المعلومات والبيانات آمنه ومحمية بشكل جيد، الأمر الذي يحمي الأجهزة من الهجمات الخارجية، ويجعلها تعمل بشكل صحيح (Brook، ٢٠١٨).
ومن ثم يمكن ترجمت الجوانب الثلاث السابقة لكي تعكس التصور حول النظافة الرقمية للمستخدم باعتبارها "ممارسات الأمن السيبراني التي يتبعها المستخدمين عبر الإنترنت لحماية وسلامة معلوماتهم الشخصية على أجهزتهم التي تدعم الاتصال بالإنترنت ضد أي هجمات" ، وتماشيًا مع تعريف النظافة في مجال الصحة العامة يمكن تعريف النظافة الرقمية على أنها: تلك العملية التي تشمل حماية المعلومات والأجهزة التي توجد للاستخدام من قبل العاملين بالمنظمة، وتحت إشرافهم والموكلة إليهم من قبل هذه المنظمة، وتحديد دور الموظفين تجاه هذه العملية (Vishwanatha، Neob، وGohb، ٢٠١٩).
والملاحظ أن هذا التعريف قد جاء وفقًا لطبيعة العمل بالمنظمات، وأنه يتسم بالمرونة لكونه قادرعلى الاستجابة للتغيرات التي تحدث في البيئة التكنولوجية مع مرور الزمن، وتتفق الدراسة الحالية مع الدراسة التي أجراها كلًا من Arun Vishwanath, Loo Seng Neo, Pamela Goh, Seyoung Leec, Majeed Khader, Gabriel Ong, Jeffery Chin من حيث أن هذا التعريف قابل للتطويروالتطبيق على نطاق واسع عبر

المنتجات التكنولوجية لكونه لم يقم بتحديد نوع الجهاز أو نظام التشغيل أو بيئة الاستخدام، ومن ثم فإن هذا التعريف المفاهيمي قادر على استيعاب مجموعة واسعة من المستخدمين والتقنيات والممارسات ذات الصلة والتغيرات التي من الممكن أن تطرأ فيما بعد.

٢/٣/٢ تعريف النظافة الرقمية:

لقد جاءت كلمة " hygiene " في كلًا من موقع word reference ، قاموس أوكسفورد oxford، قاموس مريام وبستر merriam-webster، ومعجم المعاني بمعنى " النظافة"، كما جاءت كلمة "cyber " في كلًا من القواميس السابقة بمعنى (إلكتروني أو سيبراني أو عبر الإنترنت)، وكلمة "Digital " بمعنى رقمي أو إلكتروني.

هناك عدة تعريفات اصطلاحية للنظافة الرقمية ومنها:

أنها: مصطلح له خصائص محددة للغاية مذكورة في العديد من الوثائق المنشورة المختلفة، ولكن ليست بشكل واضح، والتي منها الأمان وكلمات المرور... (Chak، ٢٠١٥)

والملاحظ من خلال هذا التعريف أنه استند في مدلوله على عدد من ممارسات النظافة الرقمية كما عرفها Brook على أنها:" الممارسات والخطوات التي يتخذها مستخدمو أجهزة الكمبيوتر والأجهزة الأخرى للحفاظ على صحة النظام وتحسين الأمان عبر الإنترنت، وعادةً ما تكون هذه الممارسات جزءًا من روتين لضمان سلامة الهوية والتفاصيل الأخرى التي يمكن سرقتها أو إتلافها (Brook، ٢٠١٨).

وترى الدراسة أن هذا التعريف بخلاف سابقه فقد ذكر أجهزة الكمبيوتر ولكنه عاد ليعمم التطبيق على الأجهزة الأخرى، وذكر الهدف منه وهو الحفاظ على صحة النظام، كما حدد طبيعة هذه الممارسات في كونها جزء من الإجراءات الروتينية لحفظ إجراءات العمل.

وعرفها كلًا من Maennel, M¨ ases, & Meannel على أنها: " مجموعة من الممارسات التي تهدف إلى الحماية من التأثير السلبي على الأصول والحياة البشرية من المخاطر المتعلقة بالأمن السيبراني (Maennel, M¨ ases, & Maennel, 2018)"

وقد عرفها كلا من (Maennel، M¨ ases، و Maennel، ٢٠١٨) بأنها: " تنفيذ وفرض سياسات وإجراءات وضوابط أمان البيانات والخصوصية للمساعدة في تقليل الأضرار المحتملة وتقليل فرص اختراق امن البيانات"

ويتضح من خلال هذا التعريف عملية مزج إجراءات الأمن السيبراني داخل السياسة التنظيمية بالعمل.

كما يمكن تعريفها على أنها: تدريب ذاتي على التفكير بشكل استباقي في أمن الشخص الرقمي، لمقاومة التهديدات السيبرانية وقضايا الأمان عبر الإنترنت (norton، بلا تاريخ).

كما تعرف على أنها: الخطوات التي يتخذها المستخدمون للحفاظ على صحة أجهزة الكمبيوتر والأجهزة الخاصة بهم وتحسين الأمن عبر الإنترنت لمنع سرقة البيانات أو تلفها (turremgroup، ٢٠١٩).

والبعض يرى أنها: هي الأمن السيبراني المكافئ لمفهوم النظافة الشخصية في أدبيات الصحة العامة (turremgroup، ٢٠١٩).

كما يمكن تعريفها على أنها: مجموعة من الممارسات لإدارة مخاطر أمن البيانات الأكثر شيوعًا وانتشارًا والتي تواجهها المؤسسات. بهدف التخفيف من الأسباب الجذرية الشائعة المسؤولة عن العديد من حوادث الأمن السيبراني، بما فيها عدوى البرامج الضارة وخروقات البيانات (RSI, 2019).

وقد عرفها (SEAL, 2020) بأنها: أفضل ممارسات الأمن السيبراني الأساسية التي يمكن لممارسي ومستخدمي الأمن في المؤسسة القيام بها.

ويتضح توافق وجهات النظر بين آخر تعريفين فقد ذكرو أنها مكافئة للأمن السيبراني أو أنها أفضل ما به من ممارسات، رغم أن التعريف الأخير قد حصر نطاق تطبيقها على المؤسسة، وبالتحديد ممارسو الأمن السيبراني بها، وهذه الرؤية الأخيرة تختلف عن رؤية Vishwanatha,Arun وزملاؤه من حيث أن تعريفهم قد جاء مُعممًا لجميع الموظفين وليس فقط متخصصي الأمن في المنظمة أو المؤسسة ومن ثم يتضح أن تعريف Vishwanatha,Arun وزملاؤه أكثر مرونة من غيره وبالأخص هذا الأخير.

وهناك من يعرفها على أنها: " مصطلح عام يشير إلى أفضل الممارسات والأنشطة الأخرى التي يمكن لمسؤولي ومستخدمي أنظمة الكمبيوتر القيام بها لتحسين أمنهم السيبراني أثناء الانخراط في أنشطة مشتركة عبر الإنترنت، مثل تصفح الويب، البريد الإلكتروني والرسائل النصية وما إلى ذلك" (CyberSecurity FAQ - What is cyber hygiene?، ٢٠٢٠).

ويوضح موقعdigitalhygiene.net أن النظافة الرقمية هي: " مجموعة من الإرشادات لمساعدة الناس على الحفاظ على صحة حياتهم الرقمية "صحية" (How NOT to become a victim of cybercrime?، ٢٠٢١)

وبعد عرض كلًا من المفهوم اللغوي والاصطلاحي لـ مصطلح النظافة الرقمية Digital Hygiene يتضح أن كلا المعنين قد جاء مترابطًا من حيث إن المفهومين قد اتفقا على أن معنى المصطلح ينصب على النظافة عبر الإنترنت سواء أكانت رقمية أو إلكترونية، وأن غالبية التعريفات قد قامت على القياس مع النظافة الشخصية، أو النظافة الصحية...

وتتبنى الدراسة التعريف الذي قد ذكره Chris, Brook: " الممارسات والخطوات التي يتخذها مستخدمو أجهزة الكمبيوتر والأجهزة الأخرى للحفاظ على صحة النظام وتحسين الأمان عبر الإنترنت، وعادةً ما تكون هذه الممارسات جزءًا من روتين لضمان سلامة الهوية والتفاصيل الأخرى التي يمكن سرقتها أو إتلافها" (Brook، ٢٠١٨). وذلك لعدة نقاط:

١- بكونها الممارسات والخطوات التي يتخذها مستخدمو أجهزة الكمبيوتر والأجهزة الأخرى، فهو هنا حدد طبيعتها، بالإضافة إلى أنه لم يحصر استخدامها على الحاسوب فقط، و إنما ذكر الأجهزة الأخرى وتركها مفتوحة، فالعلم والتكنولوجيا في تقدم مستمر الأمر الي يجعل هذا التعريف يشمل ما نعرفه من الأجهزة ومالم نسمع عنه.

٢- أنه جاء محددًا للهدف من تطبيق هذه الممارسات وهو: للحفاظ على صحة النظام وتحسين الأمان عبر الإنترنت، فهو هنا قد حدد المحافظة على صحة النظام، ثم عاد ليعمم الهدف في تحسين الأمان عامة عند الاتصال بالإنترنت (فهو هنا تركها مفتوحة بما يحمله الإنترنت من معنى وشبكات ومو اقع وما إلى ذلك).

٣- أنه ذكر أن هذه الممارسات جزء من إجراءات العمل الروتينية: أي أنه حتمًا ولابد من تو افرها لضمان سلامة العمل والحماية من الانتهاكات. فهو هنا عكس في طيات تعريفه الهدف من النظافة الرقمية، وكذلك قيمة ممارساتها.

٣/٣ أهداف النظافة الرقمية ومزاياها:

يمكن إبراز الأهداف المرجوة من وراء تحقيق النظافة الرقمية في النقاط التالية:

أ- استكشاف الطرق التي يمكن للمرء أن يخفف من خلالها اختراق شبكات الكمبيوتر عن طريق الاستفادة من ميول المستخدمين النهائيين (Chak, 2015).

ب- أنها تسعى إلى تعزيز الأمن السيبراني من خلال دمج إدارة سلوك المستخدم النهائي بدلاً من الاعتماد المفرط على التكنولوجيا الآلية (Chak، ٢٠١٥).

ج- أنه من خلال ممارسات النظافة الرقمية والتي قد تبدو صغيرة وغير مهمة من قبل المستخدمين النهائيين الفرديين إلا أنها تزيد من الصعوبة ومقدار الوقت الذي يقضيه المهاجمون في عمليات التسلل، وبالتالي إعاقة تلك العمليات (Chak، ٢٠١٥).

د- تحسين الأمن العام وسلامة الشبكات سواء كانت خاصة بمؤسسة، أو منظمة، أو شركة... وما إلى ذلك.

٤/٣ فوائد ومميزات النظافة الرقمية:

ينبغي فهم ممارسات النظافة الرقمية الأساسية ودورها في حماية أنظمة وأجهزة تكنولوجيا المعلومات وصيانتها. وبالتالي الاستجابة بشكل أفضل للحوادث وتوفير دفاعات فورية وفعالة ضد الهجمات، حيث أن هناك الكثير من عمليات الاختراق، فوفقًا لتقرير تكلفة خرق البيانات لعام ٢٠١٩ الصادر عن معهد Ponemon و IBM Security، فقد نما متوسط التكلفة العالمية لخرق البيانات بنسبة ١٢٪ في السنوات الخمس الماضية إلى ٣,٩٢ مليون دولار (Tunggal، ٢٠٢٠). ومن ثم تظهر حاجتنا إلى إتباع ممارسات النظافة الرقمية، والتي يمكن إبراز فوائدها ومزاياها فيما يلي:

١ – إن عملية الصيانة ضرورية لأجهزة الكمبيوتر والبرامج لتعمل بأقصى كفاءة. وقد تصبح الملفات مجزأة والبرامج قديمة، الأمر الذي يزيد من مخاطر التعرض لنقاط الضعف. وهنا يأتي دور النظافة الرقمية حيث أن الإجراءات والممارسات التي يتم اتخاذها يمكن من خلالها اكتشاف المشكلات مبكرًا، أيضًا منع حدوث مشكلات خطيرة. فليس من المعقول أن النظام الذي يتم صيانته جيدًا يكون عرضة لمخاطر الأمن السيبراني (Brook، ٢٠١٨).

٢ – أن إتباع ممارسات النظافة الرقمية يُمكن الأفراد من التنبؤ بالتهديدات التي من المحتمل حدوثها ليس فقط، بل ومنعها من الحدوث (Brook، ٢٠١٨).

٣ – خلق وضعية أمنية قوية وفقًا لتصنيف الأمان، فكلما ارتفع تصنيف الأمان لدى المؤسسة أو الأفراد كلما كانت ممارسات الأمان أفضل لديهم (Tunggal، ٢٠٢٠).

٤ – منع خروقات البيانات، والتصيد الاحتيالي، البرامج الضارة بأنواعها، منع الهجمات السيبرانية وخلافه (Tunggal، ٢٠٢٠).

٥- أنها تشتمل أجهزة الأفراد والموظفين والبنية التحتية لتكنولوجيا المعلومات، والتدريب على التوعية بالأمن السيبراني، وبالتالي حماية الأفراد والمؤسسات ككل (Tunggal، ٢٠٢٠).

٦- تشغيل الأجهزة والبرامج بأقصى كفاءة ممكنه بل، وتعمل على تحسين الوظائف الحالية، أو تقديم وظائف جديدة، إضافة إلى تصحيح الثغرات التي من الممكن أن تكون قابلة للاستغلال (Tunggal، ٢٠٢٠).

٧- أن الأشخاص الذين يمارسون النظافة الرقمية لديهم المزيد من الثقة بأنفسهم بشأن التعامل مع القضايا التكنولوجية المتعلقة بالأمن السيبراني (Vishwanatha، Neob، و Gohb، ٢٠١٩).

٥/٣ مشكلات النظافة الرقمية:

تمتلك المؤسسات العديد من العناصر والتي بحاجة إلى النظافة الرقمية، ومن ثم ينبغي تضمين كافة الأجهزة من أجهزة حاسب آلي، الهواتف، والأجهزة المتصلة، بالإضافة إلى البرامج والتطبيقات عبر الإنترنت والتي تستخدم ضمن أعمال الصيانة المنتظمة والمستمرة، وبطبيعة الحال فكلًا من هذه الأنظمة لديها نقاط ضعف محدده يمكن أن تؤدي إلى مشاكل مختلفة، والتي بالطبع تنعكس على النظافة الرقمية وتعترضها وهذه المشاكل يمكن عرضها فيما يلي (Brook، ٢٠١٨):

أ- فقدان البيانات: حيث يمكن قرصنة، وخرق وتسريب البيانات الحساسة التي لا يتم نسخها احتياطيًا أو صيانتها والتي يتم تخزينها على محركات الأقراص الثابتة أو من خلال التخزين السحابي عبر الإنترنت وتطبيقات SaaS التي تخزن البيانات (Tunggal، ٢٠٢٠).

ب- تغير مكان البيانات: فاتباع نظام سيء من ممارسات النظافة الرقمية سيؤدي إلى فقدان البيانات بطرق أخرى. قد لا تكون المعلومات تالفة أو تختفي إلى الأبد، فمع وجود أماكن عديدة لتخزين البيانات، قد يؤدي إلى وضع الملفات في غير موضعها (Brook، ٢٠١٨).

ج- تهديدات الأمان: حيث أن هناك العديد من التهديدات المستمرة لجميع بيانات المؤسسة (Brook، ٢٠١٨)، وهذه التهديدات التي سبق وتناولنها كالهجمات السيبرانية وهجمات الهندسة الاجتماعية وهجمات الويب بأنواعهم.

د- تقادم البرامج: جميع تطبيقات البرامج المستخدمة من قبل بعض المؤسسات قديمة الأمر الذي يجعل بها ثغرات، وللك ينبغي تحديث تطبيقات البرامج بانتظام، مع ضمان استخدام أحدث تصحيحات الأمان، وأحدث الإصدارات من خلال المؤسسة (Brook، ٢٠١٨).

هـ- برامج الأمان المستخدمة المتقادمة: فينبغي تحديث برامج مكافحة الفيروسات، وبرامج الأمان الأخرى لمواكبة مشهد التهديدات المتغيرة باستمرار (Tunggal، ٢٠٢٠).

ترى الدراسة أنه لتحقيق الإفادة من فوائد ومزايا النظافة الرقمية ينبغي العمل على تلافي المشكلات التي تعترضها حتى يمكن تحقيق الغاية المرجوة منها حيث لابد من القيام بعمليات النسخ الاحتياطي للبيانات سواء باستخدام التخزين السحابي أو الهاردات الخارجية أو أي وسيلة أخرى من وسائل التخزين والنسخ وذلك لتلافي مشكلة فقدان البيانات. العمل على حفظ البيانات بعناية وذلك حتى لا تتعدد أماكن حفظها وبالتالي صعوبة استرجاعها نظرًا لتغير أماكن حفظها من الحين للآخر كذلك مراعاة الالتزام بممارسات الأمان حتى يمكن تفادي مشاكل البرامج الضارة وهجمات الهندسة الاجتماعية وهجمات حقن SQL. العمل على تحديث البرامج والتطبيقات المستخدمة على الأجهزة وغيرها من برامج الأمان كبرامج مكافحة الفيروسات وذلك لمجابهة الثغرات الأمنية والحماية من التعرض للاختراقات وبتحقيق هذه العوامل تتحقق الفائدة المرجوة من تطبيق النظافة الرقمية.

٦/٣ النظافة الرقمية وعلاقتها بالأمن السيبراني والذكاء الاصطناعي

(The Networking & Information Technology R&D Program, June 2020):

والجدير بالذكر أن هناك علاقة ما بين والنظافة الرقمية والأمن السيبر اني والذكاء الاصطناعي حيث يُمكن تعزيز عمليتي الأمن السيبر اني والنظافة الرقمية من خلاله وذلك للأسباب التالية:

١- الهدف من الأمن السيبر اني، والنظافة الرقمية هو تمكين العمليات المستمرة للشبكات والأنظمة من مواجهة الهجوم والتسوية. الذكاء الاصطناعي لديه القدرة على تحقيق هذه الأهداف بشكل كبير، من خلال زيادة الوعي والاستجابة للمخاطروالتغيرات في البيئة بسرعة تقارب سرعة الأسلاك.

٢- يمكن لأنظمة الذكاء الاصطناعي تحديد نقاط الضعف و إنشاء طرق للمراقبة، والاستعداد لحملات الهجوم السيبر اني المستقبلية، كذلك لتصنيف أنواع مختلفة من الهجمات و إبلاغ الاستجابات التكيفية.

٣- تستهدف العديد من الهجمات أخطاء بسيطة نسبيًا، مثل التهيئة الخاطئة للأنظمة، والتي تكون مخفية في كمية البيانات الصحيحة من أقاست Avast. تعد أنظمة الذكاء الاصطناعي القائمة على المنطق جيدة بشكل استثنائي في ملاحظة هذه الأنواع من التناقضات ومعرفة كيفية إصلاحها.

٤- يمكن أن يتيح استخدامه توفير مستويات مماثلة من الحماية في كل مكان مع توفير الخبرة في اللازمة لمعالجة جوانب أخرى، مثل (قيود جودة الخدمة وسلوكيات تدهور النظام، تعزيز مصداقية الأنظمة).

٥- هناك استخدامات دفاعية محتملة للذكاء الاصطناعي في جميع مراحل تطوير البرامج (والأجهزة) ودورات الحياة التشغيلية. يسمى أحيانًا "الشفرة الكبيرة"، يتضمن الاستفادة من الذكاء الاصطناعي، لاكتشاف الأخطاء في البرامج، والتحقق من أفضل الممارسات، والبحث عن الثغرات الأمنية.

٦- يمكن لتقنيات الذكاء الاصطناعي أيضًا تجميع التعليمات البرمجية عالية التأكيد تلقائيًا من المواصفات الرسمية. بالنسبة للكود القديم، يمكن للذكاء الاصطناعي استنتاج المزيد من المواصفات الرسمية لأتمته التحديث والتشديد الأمني.

ومن خلال ما تم عرضه في هذه النقطة يتضح مدى الترابط بين المجلات الثلاث النظافة الرقمية، الأمن السيبراني، الذكاء الاصطناعي، حيث أن عملية النظافة الرقمية هي جزء رئيسي من الأمن السيبراني كما أنه يُمكن تعزيز الأمن السيبراني والنظافة الرقمية من خلال المقومات والمزايا التي يقدمها الذكاء الاصطناعي في هذا الإطار والتي سبق تناولها في النقاط سالفة الذكر وبهذا تتحقق علاقة الترابط بينهما فلا غنى للأمن السيبراني عن النظافة الرقمية ولا يمكن للإثنين الاستغناء عن الذكاء الاصطناعي للتطوير منهم.

النتائج:

١- أن هناك اختلاف بين الأمن السيبراني والنظافة الرقمية من حيث الطبيعة والتطبيق.

٢- أن عملية النظافة الرقمية جزء أساسي في محور الأمن السيبراني.

٣- أن هناك مجموعة من الهجمات والمشكلات التي تعترض كلًا من الأمن السيبراني والنظافة الرقمية، والتي ينبغي العمل على علاجها حتى يمكن تحقيق الغاية المُثلى من الأمن السيبراني والنظافة الرقمية.

٤- أنه يُمكن الاستفادة من تطبيقات الذكاء الاصطناعي لتعزيز عمليتي الأمن السيبراني والنظافة الرقمية.

التوصيات:

١- زيادة الوعي بمفهوم الأمن السيبراني والنظافة الرقمية والتفريق بينهما.

٢- العمل على مجابهة المشكلات التي تقف حائلًا ضد تطبيق الأمن السيبراني والنظافة الرقمية بنجاح.

٣- العمل على الإستفادة من تطبيقات الذكاء الاصطناعي لتعزيز عمليتي الأمن السيبراني والنظافة الرقمية.

قائمة المراجع:

١- الهيئة الوطنية للأمن السيبراني .(2018) . :الضوابط الأساسية للأمن السيبراني Retrieved from . https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf

٢- إبراهيم, مهاأحمد .(2019) .الهندسة الإجتماعية وشبكات التواصل الإجتماعي وتأيرها على المجتمع العربي.٢- الملجلة الدولية لعلوم المكتبات والمعلومات.218-195 ,

٣- البعلبكي, م .(2004) .قاموس المورد(انجليزي-عربي) .بيروت: دار العلم للملايين.

٤- البكر(2018) .سبتمبر٢٦ .(الأمن السيبراني مفهومه-وأهدافه .Retrieved from .الجزيرة : http://www.al-jazirah.com/2018/20180926/ar6.htm

٥- جوهري, طه(٢٠٢٠). إبريل مج١،ع١٦ .أمن المعلومات الرقمية وسبل حمايتها في ظل التشريعات الراهنة .المجلة المصرية لعلوم المعلومات.62 .p , .

٦- خميس .(2018) .القرصنة الإلكترونية .Retrieved from https://cutt.ly/RBTCxeM الشاهد.

٧- الرابغي ,2020) .فبراير ١٢ .(الأمن السيبراني والثورة الصناعية الرابعة :okaz from Retrieved . https://www.okaz.com.sa/articles/authors/2010045

٨- غسان ,2019) .أكتوبر ١٩ .(الأمن السيبراني وإدارة مخاطره في مجال الأعمال .Retrieved from .الغد : https://cutt.ly/gBTCv7U

٩- فاروق, ع & .,خديجة, ع .(2015) .القرصنة الإلكترونية في الجزائر و أثرها على المستخدم .مستغانم: جامعة عبد الحميد ابن باديس.

١٠- ضوميط .(2011) .إمبراطورية الإنترنت وفرسان القرصنة والحقيقة .Retrieved from https://cutt.ly/vBTCn6z

١١- المجدوب .(2017) .مفهوم القرصنة الإلكترونية .Retrieved from .ليبيا المستقبل : https://cutt.ly/YBTCQBr

١٢- Almaany (٢٠٢٢) .ترجمة و معنى الهندسة الاجتماعية في قاموس الكل عربي انجليزي :Almaany from Retrieved . https://cutt.ly/qBTCEBp

١٣- المعجم الوسيط .Retrieved from (2020) .تعريف ومعنى الهجمات السيبرانية : https://cutt.ly/YBTCTtf

١٤- الموسوعة السياسية. (٢٠٢٠). الأمن السيبراني - Cyber Security. تم الاسترداد من الموسوعة السياسية: https://cutt.ly/CBTCUh6

١٥- الهيئة المنظمة للإتصالات .(2008) .لمحة عامة حول الأمن السيبراني from Retrieved . http://www.tra.gov.lb/Cybersecurity-in-few-words-AR

16- A., B., & M., H. (2017). What Is Malware? Windows, Virus and Malware Troubleshooting. Retrieved from http://08102xj8u.1105.y.https.link.springer.com.mplbci.ekb.eg/content/pdf

١٧-Benarous, L., Leila, B., & Nouridane, A. (2017). A Survey on CyberSecurity Evolution and Threats Biometric Authentication Solutions. Retrieved from https://link.springer.com/content/pdf/10.1007%2F978-3-319-47301-7_15.pdf

١٨-Brook, C. (2018, ٥ ديسمبر). What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More. Retrieved from digitalguardian: https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more

١٩-Chak, S. (2015). MANAGING CYBERSECURITY AS A BUSINESS RISK FOR. Baltimore, Maryland.

٢٠- conteh, N., & Schmick, P. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. nternational Journal of Advanced Computer Research, 9.

٢١- kaspersky. (2020). What is Cyber Security? Retrieved from kaspersky: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

٢٢- Maennel,Kaie&M¨ ases,Sten&Maennel,Olaf. (2018). Cyber Hygiene: The Big Picture. Estonia: TalTech University.

٢٣- merlin. (2019, September 4). Mo Money, Mo [cyber] Problems. Retrieved from merlin: https://merlincyber.com/blog/mo-money-mo-cyber-problems

٢٤-norton. (n.d.). Good cyber hygiene habits to help stay safe online. Retrieved from norton: https://us.norton.com/internetsecurity-how-to-good-cyber-hygiene.html

٢٥- phoenixnap. (2019). phoenixnap. Retrieved from 17 Types of Cyber Attacks To Secure Your Company From in 2020: https://phoenixnap.com/blog/cyber-security-attack-types

٢٦-RSI. (2019, December 20). CYBER HYGIENE: A COMPLETE GUIDE. Retrieved from RSI: https://blog.rsisecurity.com/cyber-hygiene-a-complete-guide/

٢٧-SEAL, R. (2020). CYBER HYGIENE WITH REDSEAL. Retrieved from redseal.net: https://www.redseal.net/cyber-hygiene/

٢٨- Schmitt, M. N. (1998– 1999, Vol. 37,). Computer network attack and the use of force in international law: Thoughts on a normative framework. Columbia,journal of transnational law, P58.

٢٩- TAYLOR, H. (2020, 22 Jan). What Are Cyber Threats and What to Do About Them. Retrieved from prey: https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/

٣٠- Tunggal, A. (2020, ٢٥ مـايـو). What is Cyber Hygiene and Why is it Important? Retrieved from upguard: https://www.upguard.com/blog/cyber-hygiene

٣١-turremgroup. (2019). What is Cyber Hygiene and why is it important? Retrieved from turremgroup: https://www.turremgroup.com/what-is-cyber-hygiene-and-why-is-it-important/