متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الالكترونية

الاستاذ الدكتور علي عبد الصمد ال فرهاد

الباحثة مريم هاشم طه

قسم المعلومات و تقنيات المعرفة / كلية الآداب / جامعة البصرة

المستخلص

تهدف الدراسة الى التعرف على ما هيه الأمن السيبراني و الأخطار السيبرانية و التعرف ايضا على اهم متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الالكترونية . و ابرز المخاطر التي تواجها انظمة المعلومات الالكترونية , اعتمدت الدراسة على المنهج الوثائقي بالاعتماد على المصادر و الدراسات العربية و الاجنبية التي تناولت متغيرات الدراسة والمتوفرة بشكلها الورقي و الالكتروني على شبكة الأنترنت , و توصلت الدراسة لعدد من الاستنتاجات نذكر منها :

١- يساهم الأمن السيبراني في الحفاظ على سرية المعلومات و البيانات داخل الانظمة .

٢- يساعد الأمن السيبراني على صد الهجمات الخارجية في شبكة الأنترنت فضلا عن التصدي للدخول غير المصرح به من قبل الاشخاص غير المخول لهم بالدخول .

كلمات مفتاحية: أمن المعلومات , الأمن السيبراني , انظمة المعلومات .

تاريخ الاستلام: ٢٠٢٣/٠٩/١١ **تاريخ القبول:** ٢٠٢٣/١٠/١

Cybersecurity Requirements for Electronic Information Systems

Prof.Dr. Ali Abdul-Samad Al-Farhad
Res.Mariam Hashim Taha
Department of Information and Knowledge Technologies / College of Arts /University of Basrah

Abstract

The study aims to identify what cyber security and cyber dangers are, and also to identify the most important requirements for achieving cyber security for information systems . The most prominent risks facing electronic information systems, the study relied on the documentary approach, relying on Arab and foreign sources and studies that dealt with the variables of the study: which are available in both paper and electronic form on the Internet. The study reached a number of conclusions, including:

1- Cybersecurity contributes to maintaining the confidentiality of information and data within systems.

2- Cybersecurity helps against external attacks on the Internet, as well as repelling unauthorized entry by unauthorized persons.

Keywords:information security, cyber security, information systems .

Received: 11/09/2023 **Accepted: 1/10/2023**

اولا : الإطار العام للدراسة

١- مشكلة الدراسة

أن استخدام أنظمة المعلومات و الانترنت تزيد و توسع من عمليات الاختراق التي تتنوع طرقها و آثارها , ففي السابق كان آثر الاختراق أبسط من الأن مثل اختراق البيانات الشخصية و غيرها الا انه اصبحت هذه الاختراقات و الهجمات تؤثر بشكل كبير على الانظمة و المؤسسات التي تعتمد على الانترنت مما تؤدي الى عمليات اختراق تدمر الانظمة الالكترونية او اخذ المعلومات السرية او التجسس لهذا لا بد من حماية هذه الأنظمة و المعلومات و هذا جزء من الأمن السيبراني الذي من خلاله يتم حماية الشبكات و الأنظمة و الأجهزة و البرمجيات و كل ما تتضمن من الاختراق أو التعطيل أو التعديل او حتى الدخول غير المصرح به و الاستغلال ومن هنا تنطلق مشكلة الدراسة التي تتمثل في معرفة متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الالكترونية .

٢- أهمية الدراسة

للدراسة أهمية واضحة من خلال ما تتناوله في موضوعها و هو الأمن السيبراني الذي يعد من أبرز النظم التي تعمل على الحماية و الدفاع عن المعلومات و الأنظمة و البيانات من الهجمات و الاختراقات و التزييف , لذا من المتوقع ان تسهم هذه الدراسة في زيادة التركيز و الانتباه إلى أهمية حماية انظمة المعلومات في الجامعات .

٣- أهداف الدراسة

تهدف الدراسة الى :

٣-١ التعرف على ما هيه الأمن السيبراني و الأخطار السيبرانية .

٣-٢ التعرف على اهم متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الالكترونية .

٣-٣ التعرف على المخاطر التي تواجها انظمة المعلومات الالكترونية و ما أهم انواعها .

٤- تساؤلات الدراسة

لأجل تحقيق أهداف الدراسة تم وضع التساؤل التالي :

ما المتطلبات التي من خلالها يمكن تحقيق الأمن السيبراني لأنظمة المعلومات الالكترونية ؟

٥- حدود الموضوعية للدراسة

تقتصر الحدود الموضوعية على تحديد ما هيه الأمن السيبراني و أهميته لأنظمة المعلومات الالكترونية .

٦- منهج الدراسة

اعتمدت الدراسة على المنهج الوثائقي بالاعتماد على المصادر و الدراسات العربية و الاجنبية التي تناولت متغيرات الدراسة والمتوفرة بشكلها الورقي و الالكتروني .

٧- الدراسات السابقة

تمثل الدراسات السابقة الإطار المرجعي الأساس إلى أي دراسة وهنا سوف نستعرض بعض الدراسات السابقة التي تناولت متغيرات الدراسة المتغير المستقل (الأمن السيبراني) و المتغير التابع (أنظمة المعلومات الالكترونية) وكما يأتي :

٧-١ نبيلة محمد الحداد .متطلبات تحقيق الأمن السيبراني في المكتبات الجامعية اليمنية دراسة حالة ._مجلة جامعة البيضاء ._مج٤ , ع٢ ,ص٧٠٣_ص٧١٥ .٢٠٢٢ متاح على
https://baydaauniv.net/buj/index.php/buj/article/view/287/277

تهدف دراسة الباحثة نبيلة محمد الحداد الى التحقق من متطلبات تحقيق الأمن السيبراني في المكتبات الجامعية اليمنية و كذلك التعرف على واقع الأمن السيبراني في تلك الجامعات و اتبعت الباحثة المنهج الوصفي التحليلي دراسة حالة , و توصلت الدراسة لعدد من النتائج من أبرزها : يسهم الأمن السيبراني في المحافظة على أمن البيانات و المعلومات في المكتبات و سريتها و يساعد على التصدي للهجمات الالكترونية و توصلت الباحثة إلى عدد من التوصيات منها تأهيل كوادر بشرية في مجال تكنولوجيا المعلومات في الجامعات اليمنية .

٧-٢ الجوهرة بنت عبدالرحمن المنيع .متطلبات تحقيق الأمن السيبر اني في الجامعات السعودية في ضوء رؤية ٢٠٣٠ ._المجلة العلمية ._ مج٢٣ ,ع١ , ص ١٥٥ - ص ١٩٤ متاح على
http://www.aun.edu.eg/faculty_education/arabic

هدفت دراسة الباحثة الى التعرف على واقع تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠ و كذلك التعرف على متطلبات تحقيق الأمن السيبراني في الجامعات السعودية و الكشف عما أذا كان هنالك فروق ذات دلالة احصائية لمتغيرات دراستها , اتبعت الدراسة المنهج الوصفي التحليلي وشمل مجتمع الدراسة الموظفين التقنيين لثلاث جامعات في السعودية لجمع المعلومات المطلوبة حول الدراسة من خلال عينة عشوائية بلغت (٢١٠) . و توصلت الدراسة لعدد من النتائج منها تدني مستوى الخبرة لدى موظفين الجامعات السعودية في مجال الأمن السيبراني و الضعف في التعاون بين موظفي التقنيات في الجامعة و كذلك وجود اتفاق بدرجة كبيرة حول على ضرورة تحقيق متطلبات الأمن السيبراني في الجامعات السعودية . كما و خرجت الدراسة بعدد من التوصيات منها توعية الموظفين بالمخاطر السيبرانية و منح الحوافز المادية و المعنوية التي تشجع الموظفين المبدعين في مجال الأمن السيبراني .

٧-٣ مني عبدالله السمحان . متطلبات تحقيق الأمن السيبر اني لأنظمة المعلومات الإدارية بجامعة الملك سعود ._ مجلة كلية التربية ._ع١١١ ,ص١_ص٢٩ .٢٠٢٠ متاح على
http://search.mandumah.com/Record/1120017/Details

تهدف دراسة الباحثة إلى التعرف على متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود شمل مجتمع الدراسة العاملين في جامعة الملك سعود و اعتمدت الباحثة على الاستبانة كاداة

لجمع المعلومات من العاملين للتعرف على وجهة نظرهم حول كيفية تحقيق الأمن السيبراني بالجامعة و توصلت لعدد من التوصيات نذكر منها :التأكد على ضرورة اهتمام جامعة الملك سعود بمتطلبات حماية الأنظمة المعلوماتية الادارية و تشجيع البحوث و الدراسات في مجال الأمن السيبراني و توعية العاملين بكافة مؤسسات الدولة و تنمية المعايير المهنية لديهم و ارساء بنية تحتية للدخول في صناعة البرمجيات العالمية و منافسة البرامج المستوردة .

٨- مصطلحات الدراسة

تشمل هذه الفقرة مفاهيم لمصطلحات الدراسة و المرتبطة بمتغيرتها وكما يلي :

٨-١ الأمن السيبراني : جميع الإجراءات التي تهتم بحماية شبكات المعلومات ضد كافة الأعمال و المماراسات التي تهدف إلى التلاعب بالمعلومات و ألحاق الأذى بالمستخدمين أذ تعمل هذه الإجراءات على الحماية ضد الاختراقات و البرمجيات الخبيثة و الفايروسات و الوصول غير المصرح به و غيرها من الممارسات السلبية . (الحداد، ٢٠٢٢)

٨-٢ الفضاء السيبراني :هو فضاء الكتروني يمثل مجال عالمي داخل بيئة المعلومات يتكون من شبكة مترابطة من البنى التحتية لأنظمة المعلومات بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة المعلومات ووحدات التحكم المدمجة . (cyberspace, 2012)

٨-٣ الجريمة السيبرانية : من وجهة نظر الباحثة تعرف الجريمة السيبرانية على أنها افعال و أعمال غير قانونية تهدف إلى ألحاق الضرر بأجهزة الحاسوب و انظمة المعلومات و شبكات الاتصال .

٨-٤ أنظمة المعلومات الالكترونية : هي مجموعة المكونات و الاجراءات التي تقوم على جمع وخزن و معالجة البيانات للحصول على مخرجات . و النظم المعلومات في أي مؤسسة يشمل على المكونات المادية و البرمجيات و البيانات و الموارد البشرية و الاتصالات التي تعمل على تحقيق اهداف المؤسسة . (قنديلجي و السامرائي، ٢٠٣٣)

٨-٥ أنظمة المعلومات المكتبية : هي مجموعة من الموارد البشرية و الحواسيب التي تتحد مع بعضها البعض لتنفيذ مجموعة من العمليات المتتالية أذ تقوم على جمع و معالجة و خزن و بث و استرجاع المعلومات و من ثم توظيفها لتقديم خدمات المكتبة للمساعدة في تقديم خدمات أكثر كفاءة و بأقل جهد و اسرع وقت للمستفيدين . (عبدالقادر، ٢٠٢١)

٨-٦ أنظمة المعلومات الإدارية : هي نظم متكاملة تختص في المجالات الإدارية في المؤسسة أذ تعمل على تقديم المعلومات لغرض التخطيط و التنظيم و الرقابة . (النجار، ٢٠١٣)

ثانيا : الإطار النظري للدراسة

١- الأمن السيبراني , النشأة , المفهوم , الأهداف , الأهمية

نشأة الأمن السيبراني

نشأ الأمن السيبراني ضمن الثورة الصناعية الرابعة و هي التسمية التي اطلقها المنتدى الاقتصادي العالمي عام ٢٠١٦ في سويسرا على الحلقة الأخيرة من سلسلة الثورات الصناعية و يلحظ من الشكل رقم (١) أن الثورة الصناعية الثالثة بدأت بالتشغيل الآلي و الالكتروني مروراً بوقتنا الحاضر الثورة الصناعية الرابعة التي تضم الأنترنت و الأمن السيبراني و الذكاء الاصطناعي و المجالات المستقبلية الاخرى التي سوف يشهدها العالم.

شكل (١)نبذه عن الثورات الصناعية

أن الثورات السابقة مهدت بشكل كبير في ظهور الأمن السيبراني أذ شهد عام ١٩٦٧ أهم الأحداث في تاريخ الأمن , ففي ذلك الوقت دعت شركةIBM بعض الطلاب للتحقق من جهاز كمبيوتر تم إنشاؤه حديثًا في مكاتبهم و تم تدريب الطلاب على نظام الكمبيوتر هذا ,أذ تمكنوا من الدخول إلى العديد من مكونات النظام بطريقة غير شرعيه وهو ما يعرف بالقرصنة الأخلاقية و نتيجة لذلك ، اكتسبت شركة IBM المعرفة حول نقاط الضعف في النظام ,و بدأت فكرة تنفيذ تدابير أمنية دفاعية على أجهزة الكمبيوتر لردع المتسللين , وخلال العام ١٩٨٣ ظهر مصطلح حصان طروادة و فيروس الكمبيوتر لأول مرة خلال الحرب الباردة و ازداد خطر التجسس السيبراني و يعتبر عام ١٩٨٣ بداية تاريخ جرائم الكمبيوتر و الأنظمة , وفي عام ١٩٨٧على الرغم من ادعاء العديد من الأشخاص أنهم أنشأوا أول برنامج مضاد فيروسات قبل ذلك ، فقد شهد عام ١٩٨٧ بداية برامج مكافحة الفيروسات التجارية بإصدار Anti4us و Flushot Plus. (Bhadwal، ٢٠٢٣).

*المخطط من عمل الباحثة

مفهوم الامن السيبراني

السيبرانية هي كلمة مشتقة من اللغة اليونانية و تعني السيطرة و التوجيه و تستخدم مجازا للمتحكم و بذلك يمكننا القول ان مصطلح السيبرانية تعني التحكم عن بعد ,اما الامن فتعني السلامة و هي مصدر الفعل أمن امنا و اماناً اي الاطمئنان و زوال الخوف من هنا جاء مصطلح (الأمن السيبراني) (جيجان ، ٢٠٢١) و يمكننا القول ان الابتكارات التكنولوجية و التقنيات الحديثة في كافة شؤون الحياة ساهمت في تغير المفاهيم التقليدية لأمن و حماية المعلومات , و من خلال الثورة التكنولوجية الحديثة التي ادت الى ظهور التهديدات و المخاطر الالكترونية ومنها الابتزاز و الاحتيال و النصب و السرقة , الامر الذي ادى الى تطور لمفاهيم و استراتيجيات متطورة تلائم مفاهيم الامن السيبرانية , ومنها يعرف " (حامد و عبداللة ، ٢٠٢٠) الأمن االسيبراني " بأنه عبارة عن مجموعة الوسائل التقنية و التنظيمية و الادارية التي يتم استخدامها لحماية

الشبكات و الاجهزة و البرامج و البيانات من الهجمات او الاضرار او الوصول غير المصرح به و سوء الاستغلال" . و عرف ايضا على انه "عبارة عن مجموعة من التقنيات والعمليات المصممة لحماية أجهزة الكمبيوتر والشبكات وقواعد البيانات والتطبيقات من الهجمات أو الوصول غير المصرح به أو التغيير أو يمكن أن يكون التدمير أيضًا جزءًا مهمًا في تطوير المعلومات التكنولوجيا وكذلك خدمات الإنترنت" (AL Wally & M. Nema, 2019)

من خلال ما سبق يمكن القول أن الأمن السيبراني هو المجال الذي يرتبط بإجراءات و معايير الحماية الواجب اتخاذها للدفاع عن البرامج و الشبكات و انظمة المعلومات إذ أن الهدف من الأمن السيبراني هو سرية و سلامة المعلومات و مواجهة التهديدات الالكترونية الداخلية و الخارجية والحد و التقليل من المخاطر السيبرانية التي تمتاز بالسرعة الهائلة و الغموض , و تتحقق هذه الأهداف حال توفر مجموعة من العناصر التي تعد اساسية للحفاظ على أنظمة المعلومات وهي كما يأتي : (آمنة، ٢٠٢١).

١-١ التكنولوجيا : تتمثل في الأدوات و المعدات اللازمة لحماية الأنظمة

١-٢ الأشخاص : وهم مستخدمي الأنظمة والبرامج الذين يتطلب عليهم استخدام مبادئ الحماية مثل تحديد كلمة مرور و تفادي فتح الروابط المهمة و المرفقات عبر البريد الالكتروني فضلا عن عمل النسخ الاحتياطية للبيانات .

١-٣ العمليات : تتمثل في مجموعة من الإجراءات التي من خلالها يتم توظيف الاشخاص و التقنيات للقيام بالعمليات و الانشطة و تسييرها مع أسس الأمن السيبراني التي من شأنها التصدي للهجمات الالكترونية .

أهداف الأمن السيبراني

هناك العديد من الأهداف التي يتمتع بها الأمن السيبراني وكما يأتي :

١- تعزيز حماية أنظمة المعلومات في كافة مكوناتها من برمجيات و أجهزة و تقنيات و لكل ما تقدمه من خدمات و ما تتضمن من بيانات .

٢- التصد للهجمات وحوادث أمن المعلومات التي غالبا ما تستهدف الأجهزة الحكومية و المؤسسات .

٣- اتاحة بيئة آمنه و موثوقة للتعامل مع المجتمع المعلوماتي .

٤- ثبات البنى التحتية الحساسة للهجمات الالكترونية .

٥- سد الفجوات في انظمة المعلومات

٦- التخلص من نقاط الضعف في أنظمة الحاسوب الالية و الاجهزة بجميع انواعها .

٧- مقاومة البرمجيات الخبيثة التي تحدث أضرار بالغة للمستخدمين .

٨- الحد من عمليات التجسس و التخريب الالكتروني و الدخول غير المخول به من قبل المتطفلين .

٩- اتخاذ الإجراءات اللازمة لحماية المستخدمين من المخاطر المحتملة في مجالات الأنترنت المختلفة .

١٠- تدريب الأفراد على الإجراءات و الاليات الجديدة لمواجهة التحديات الخاصة باختراق اجهزتهم بقصد الضرر بمعلوماتهم بالأتلاف او بقصد السرقة .

اضافة الى ما سبق ترى الباحثة أن الأمن السيبراني يهدف الى وضع القواعد و الاجراءات لضمان سرية المعلومات أي حمايتها وعدم الاطلاع عليها من قبل الافراد الغير مخولين بذلك , ونزاهة المعلومات و رصانتها , اضافة الى أتاحه المعلومات عن طلبها .

أهمية الأمن السيبراني

من خلال ما جاء في أهداف الأمن السيبراني يمكن القول أن أهمية الأمن السيبراني تنبع من الحاجة للحفاظ على أمن المعلومات و البيانات و الأنظمة ففي وقتنا الحاضر يقوم الأفراد بتخزين كميات هائلة من البيانات و المعلومات على الأجهزة و الخوادم المتصلة او غير المتصلة و التي تكون حساسة جداً , و إذا تمكن مجرمي الإنترنت من الوصول لهذه المعلومات و البيانات فيمكن ان يتسبب في الخراب و مشاركة المعلومات الحساسة او حتى استخدام كلمات المرور و تغير البيانات , لهذا تحتاج المؤسسات و الجامعات الى حلول أمنية تمكنها من اتاحة بيئة آمنه ذات موثوقية عالية , من خلال اتاحة برامج الدفاع السيبراني و الذي تتمثل أهميته في الحفاظ على المعلومات و سلامتها و توفير المعلومات و البيانات و قت الحاجة إليها , حماية الأجهزة و الأنظمة و البيانات من الدخول غير المصرح به و تكوين درع واقٍ , استكشاف نقاط الضعف و الثغرات في أنظمة و معالجتها .

٢- المخاطر السيبرانية على أنظمة المعلومات الالكترونية

المخاطر السيبرانية يقصد بها المخاطر التشغيلية التي تؤثر على أصول المعلومات و التكنولوجيا مما تسبب عواقب على سرية و سلامة أنظمة المعلومات (Hartmann & Carmenate, 2022)و تضم المخاطر السيبرانية ثلاثة انواع وهي كالآتي :(Caliyurt, 2018)

٢-١ مخاطر تتعلق باستمرارية الأداء : تتمثل في تعطل أو التوقف عن أداء الاشغال الواجب العمل بها .

٢-2 مخاطر تتعلق بسرية المعلومات : و يمكن أن تنشئ هذه المخاطر عند الافصاح عن المعلومات الخاصة داخل المؤسسة الى أطراف ثالثة في حالة حدوث اختراق البيانات .

٢-٣ مخاطر تتعلق بالرصانة : و تتمثل في إساءة استخدام الأنظمة و استخدامها بطرق غير دقيقة .

٣- الهجمات السيبرانية و أنواعها

الهجوم السيبراني هو فعل متعمد يقوم به واحد أو أكثر من مجرمي الإنترنت لسرقة البيانات أو تزوير المعلومات أو تعطيل الأنظمة الرقمية لفرد أو مؤسسة بأكملها. تسمح الهجمات السيبرانية لمجرمي الإنترنت بالحصول على وصول غير قانوني وغير مصرح به إلى جهاز كمبيوتر واحد أو أكثر لاستخدامه لاحقًا وفقًا لأهدافهم الإجرامية والتي تؤدي الى عواقب عديده منها سرقة الهوية , الابتزاز , التلاعب بالأجهزة , سرقة الملكية الفكرية , التزييف , و البرمجيات الضارة (حمود، ٢٠٢١) وفيما يلي أبرز انواع الهجمات السيبرانية .

٣-١ الهندسة الاجتماعية Social Engineering : الهندسة الاجتماعية او ما تسمى بـ فن اختراق العقل هي مجموعة من التقنيات المستخدمة لجعل الأفراد يفعلون شيئًا ما أو يكشفون عن معلومات سرية, تستخدم

الهندسة الاجتماعية أحيانًا في الاحتيال عبر الإنترنت لتحقيق الغرض المقصود من الضحية ، حيث أن الهدف الأساسي لهندسة الاحتيال الاجتماعي هو طرح أسئلة بسيطة أو تافهة على سبيل المثال انتحال شخصية عميل مهم عبر مكالمة هاتفية تسمح له بسحب معلومات حساسة من خلال طرح اسئلة بطريقة مباشرة او غير مباشرة دون أثارة الشك (European Union Ageny For Cyberecurity, 2023) .

3-2 الدخول غير المصرح به Unauthorized Access :ويقصد به محاولة التحايل على أليات الأمان الخاصة بنظام المعلومات للوصول بطريقة غير مُصرّح بها إلى الأنظمة أو البرامج أو قواعد البيانات،, عن طريق الحصول على اسم المستخدِم أو كلمة السر بطريقة غير مشروعة (Al-Rawashdeh, 2018)

٣-٣ التجسس Espionage :التجسس الإلكتروني هو نوع من الهجمات الالكترونية التي يحاول فيها مستخدم غير مصرح له الوصول إلى معلومات و بيانات حساسة أو سرية لتحقيق غاياته , كالتجسس على المؤسسات الحكومية و الشركات الكبيرة و مراكز الفكر و المنظمات الاخرى او الافراد . (Gary، ٢٠١٦)

٣-٤ البرامج الضارة Malware Attacks :هجمات البرامج الضارة هي أي نوع من البرامج الضارة أشهرها (الفيروسات)التي صممت لإحداث ضرر أو تلف لجهاز كمبيوتر أو خادم أو عميل أو شبكة دون معرفة المستخدم النهائي ,إذ يصنع المجرمون عبر الإنترنت البرامج الضارة ويستخدمونها أو يبيعونها لأسباب مختلفة، ولكن في العادة يتم استخدامها لسرقة المعلومات الشخصية أو التجارية على الرغم من اختلاف دوافعهم، يركز مجرمو الانترنت دائماً على الوصول إلى بيانات المهمة لتنفيذ غايتهم.

٣-٥ برامج الفدية Ransomware :تعد واحدة من أخطر الهجمات السيبرانية في عصرنا ، أذ تعمل على تقيد الوصول الى جهاز الكمبيوتر و يطالب بدفع فدية و بالتالي يقوم بتشفير الملفات الموجودة في النظام و يتركها غير صالحة للاستخدام إما بشكل دائم عند رفض دفع الفدية أو موقتاً حتى يتم الدفع , ولهذا اطلق عليه برامج الفدية . (حمود، ٢٠٢١) .

وهناك العديد من الهجمات السيبرانية التي تشكل خطر على الأنظمة الالكترونية والتي يكون غالبيتها الهدف منها الوصول الى المعلومات و البيانات المهمة أو أحداث ضرر أو تلف في النظام فضلا عن الاهداف المادية ومن هذه الهجمات (الهاكرز , حصان طروادة , هجمات الذكاء الاصطناعي , التصيد الاحتيالي ,هجمات رجل في الوسط , التلاعب بـ URL , هجمات البرمجية النصية عبر المواقع CROSS-SITE- SCRIPTING)

ثالثا : المتطلبات الاساسية لتحقيق الأمن السيبراني لأنظمة المعلومات الالكترونية

١- الخطوات الأساسية للحفاظ على أعلى مستوى من السلامة و الأمان لأنظمة المعلومات الالكترونية .

من وجهة نظر الباحثة من الضروري أن تتبع المؤسسة عدد من الخطوات لضمان حماية و سلامة أنظمتها في الفضاء السيبراني و كما يأتي :

١-١ استخدام المواقع الموثوقة خاصة عند تقديم معلومات شخصية مع ضرورة التحقق من عناوين الـ URL , فإذا تضمن الموقع على https في بدايته فيعني هذا أنه موقع آمن , أما إذا كان عنوان URL يحتوي على http بدون حرف الـ s يجب الحذر و عدم أدخال أي معلومات هامة و سرية .

١-٢ النسخ الاحتياطي للملفات بانتظام خاصة الملفات التي تشكل أهمية كبيرة للمؤسسة .

١-٣ التحديث بشكل دوري للأنظمة أذ باتت المؤسسات تتعرض إلى الهجمات الالكترونية بشكل مستمر و بهذا لا يمكن أن تتغاضى المؤسسات عن وجود الثغرات في أنظمتها مهما تكن نسبة الحماية متوافرة , و لتقوم المؤسسات في تأمين لأنظمتها لا بد من الاعتماد على تحديث هذه الأنظمة بشكل دوري , أذ تعمل التحديثات عادة على سد الثغرات و أضافة جدار جديد من الحماية لهذه الأنظمة .

١-٤ عدم فتح مرفقات البريد الالكتروني أو الضغط على الروابط من المصادر غير الموثوقة , أذ تعد رسائل البريد الالكتروني من الطرق الاشهر في تنفيذ عمليات الاختراق و السرقات من خلال الرسائل المتخفية على أنها مرسلة من جهات موثوقة .

١-٥ تنصيب برامج مكافحة الفيروسات أذ تساعد هذه البرامج في مكافحة الفايروسات وإبقاء اجهزة الكومبيوتر في حالة دفاع عن الأنظمة الخاص بها ضد الفيروسات .

٢- المتطلبات الأساسية لتحقيق الأمن السيبراني لأنظمة المعلومات الالكترونية

هناك متطلبات يجب توفرها عند تنصيب برامج الأمن السيبراني وكما يأتي :

٢-١ متطلبات ادارية

تتمثل المتطلبات الإدارية في وضع خطة استراتيجية يتم من خلالها الاتي : (الحداد، ٢٠٢٢)

- وضع سياسات و تشريعات يتم اتباعها عند العمل على شبكة الأنترنت
- تشريع الأنظمة و الإجراءات الواضحة لتحقيق الامن السيبراني
- تشفير البيانات و أنظمة المعلومات
- توفير الحماية الكاملة للبيانات و المعلومات الادارية
- تخصيص القوانين الملائمة التي تخص الامن السيبراني
- توفير المتطلبات المالية و البشرية و المادية
- تزويد الموظفين بمعلومات أكثر حول الأمن السيبراني و هم تطوراته

٢-٢ متطلبات مادية

ترى الباحثة أن من أهم متطلبات تحقيق الامن السيبراني هي توفر المتطلبات المادية والتي تتمثل في توفير الأجهزة و تزويدها بالبرامج الخاصة بالوقاية واكتشاف المخاطر السيبرانية اضافة الى ربط جميع الاجهزة و

الحاسبات بقاعدة بيانات مؤمنة, توفير خوادم قوية و محمية فضلاً عن توفير برامج مضادة للفيروسات و كذلك تنصيب اجهزة حائط النار .

٢-٣ متطلبات بشرية

تتمثل المتطلبات البشرية في اختصاصيين في مجال تكنولوجيا المعلومات و كذلك الموظفين العاملين في مجال انظمة المعلومات و تحديد مسؤوليات العمل و المتابعة و التدقيق فضلا عن ذلك تأهيل الموظفين و توعيتهم بأهمية الأمن السيبراني .

٢-٤ متطلبات تقنية

و تشمل البرامج المضادة للفيروسات و الجدران نارية و كذلك تطبيقات حماية قوية , توفير كاميرات المراقبة و كذلك مراقبة الدخول إلى المواقع و العمل على مكافحة الفيروسات الخبيثة , فضلا عن توفير اجهزة و حاسبات حديثة و كذلك التحديث المستمر للأنظمة و البرامج و الاجهزة .

الاستنتاجات

١- يساهم الأمن السيبراني في الحفاظ على سرية المعلومات و البيانات داخل الانظمة .

٢- يساعد الأمن السيبراني على صد الهجمات الخارجية في شبكة الأنترنت فضلا عن التصدي للدخول غير المصرح به من قبل الاشخاص غير المخول لهم بالدخول .

٣- للأمن السيبراني دور كبير في التفادي لكثير من الجرائم الالكترونية .

٤- يمكن أن يساهم الأمن السيبراني في فتح مجالات تكنولوجية مختلفة في الجامعة .

التوصيات

١- توفير الدعم المالي من قبل المؤسسة المسؤولة لتحقيق الأمن السيبراني .

٢- إقامة دورات تدريبية للموظفين و العاملين على أنظمة المعلومات حول مفهوم الأمن السيبراني .

٣- تأهيل اختصاصيين في مجال الأمن السيبراني و تكنولوجيا المعلومات.

٤- توفير كوادر بشرية للقيام بمهام الأمن السيبراني .

٥- تشجيع مجالات البحث العلمي و الابتكار في مجالات الأمن السيبراني .

٦- نشر ثقافة الاستخدام الأمن لشبكة الأنترنت و التطبيقات الرقمية الجديدة .

٧- توعية الموظفين بمخاطر استخدام الأجهزة الشخصية مثل الهاتف الشخصي لنقل و تخزين المعلومات الهامة و السرية الخاصة بالجامعة .

٨- من الضروري تحديد المسؤوليات وصلاحيات الوصول لكل موظف .

٩- التحديث المستمر للاجهزة و الأنظمة المعلوماتية باستمرار بشكل يتيح التعرف على ادق التقنيات التي تساعد على كشف الجريمة و مرتكبها .

المصادر

1-*cyberspace*. (٢٠١٢). تاريخ الاسترداد ٢ ٣, ٢٠٢٣، من NIST.

2-Akhil Bhadwal. (٢٠٢٣). *[The History of Cyber Security: A Detailed Guide [Infographic*. تاريخ الاسترداد ٢٦ ٢, ٢٠٢٣، من https://www.knowledgehut.com/blog/security/history-of-cyber-security

3-Brown Gary. (٢٠١٦). ?Spying and Fighting in Cyberspace: What is Which *JOURNAL OF NATIONAL SECURITY POLICY_V6 & LAW*، الصفحات ٦٢١-٦٣٥.

4-C. Hartmann، و J Carmenate. (٢٠٢٢). Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy, and Research *American Accounting Association.vol15,No.2*، الصفحات ٩-٢٣.

5-European Union Ageny For Cyberecurity. (٢٠٢٣). *"What is "Social Engineering?* تاريخ الاسترداد ١٥ ٣, ٢٠٢٣، من /enisa: https://www.enisa.europa.eu

6-Hanan Abed AL Wally، و M. Nema Bashar. (٢٠١٩). Cybersecurity Risks Detection and Prevention *Al-Mansour Journa.- no.31*، الصفحات ٦٥-٨٦.

7-Kahyaoglu S.B and K. Caliyurt. (٢٠١٨). Cyber security assurance process from the internal audit perspective *managerial auditing*، الصفحات ٣٦٠-٣٧٦.

8-Sami Hamdan Al-Rawashdeh. (٢٠١٨). Illegal Access to Information Systems in the Qatari Criminal Law: A Comparative Study *Kuwait International Law School Journal - Volume 6 - Issue 1 - Ser. No. 21*، الصفحات ٣٣-٩٢.

٩-احمد حامد، و سعاد عبداللة . (٢٠٢٠). الامن السيراني في دول مجلس التعاون لدول الخليج العربية بمنظور جيوبولتيكي معاصر . *مجلة اجامعة الانبار للعلوم الانسانية .- مج١ , ع٣* ، صفحة ٣٧٣.

١٠ اسراء شريف جيجان . (٢٠٢١). الامن السيبراني الصيني : دراسة في الدوافع و التحديات. *قضايا سياسية ._ ع٦٥* ، الصفحات ٣٣-٤٦.

١١- آمنة محمد منصور. (٢٠٢١). تأثير الامن السيبراني على الرقابة الداخلية و انعكاساتها على الوحدة الاقتصادية _ دراسة استطلاعية لاراء عين من المدققين و المحاسبين في وزارة التعليم العالي و البحث العلمي. *مجلة الادارة و الاقتصاد*، الصفحات ٢٢٣-٢٣٨.

١٢- رؤى حمود. (٢٠٢١). *أبرز أنواع الهجمات السيبرانية حتى عام ٢٠٢١* . تاريخ الاسترداد ١٥ ٣, ٢٠٢٣، من رينا د المجد لتقنيات المعلومات RMG: https://www.rmg-sa.com

١٣-عامر ابراهيم قنديلجي، و ايمان فاضل السامرائي. (٢٠٣٣). *حوسبة اتمته المكتبات*. عمان: دار المسيرة للنشر و التوزيع.

١٤-فايز جمعة النجار. (٢٠١٣). نظم المعلومات الإدارية : منظور اداري. عمان: دار الحامد للنشر و التوزيع.

١٥-نبيلة محمد الحداد. (٢٠٢٢). متطلبات تحقيق الأمن السيبراني في المكتبات الجامعية اليمنية دراسة حالة. *مجلة جامعة البيضاء ,ع٢ ,مج٤*، الصفحات ٧٠٣-٧١٥.

١٦- نضال نعمة عبدالقادر. (٢٠٢١). *نظم المعلومات الآلية المستخدمة في مكتبات جامعة البصرة :دراسة مسحية /أشراف هالة غالب الناهي*. جامعة البصرة :كلية الآداب قسم المعلومات و المكتبات.