IJSSP

المجلة الدولية لنشر الدراسات العلمية
المجلد الأول – العدد الثالث – البحث الثاني (ص: 9 - 15)

15 – أيلول – 2017 م

www.ijssp.com International Journal of Scientific Studies Publishing

[أمن المعلومات وحمايتها]

[الباحثة: فرح محمد فوزي]

[بكالوريس – نظم المعلومات الحاسوبية – الجامعة الأردنية– المملكة الأردنية الهاشمية] 2017 – 2018 م

[farah181198@gmail.com]

الملخص للدراسة

تناول هذا البحث أمن المعلومات ومفهومها وطرق الحفاظ عليها وحمايتها من البرامج الضارة كالفيروسات أو السرقة، وقد تم توضيح أهمية أمن المعلومات لحماية الشركات أو حتى الأفراد من المتطفلين و الذين يريدون أذية الغير.

إن وجود شبكة الانترنت في حياتنا سهل علينا الكثير في الحصول على ما نريد من بيانات وبرامج أو غيرها، لكن هذا الأمر لم يكن له ايجابيات فقط، بل له سلبيات خطيرة قد تهدد الحياة الخاصة للبعض، فمحاولتنا الحصول على بعض البرامج عبر الانترنت من صفحات غير موثوقة كان من المحتمل وجود روابط غير آمنة أو مدسوسة بمجرد فتحها تسرق البيانات المتواجدة لدى الشخص، كذلك الأمر لدى الشركات أو المؤسسات التي من السهل يصبح اختراقها والدخول إلى قاعدة بياناتها وإحداث أعطال قد تؤثر على عمل الشركة كلها.

لقد تم تقديم البحث ببعض من المعلومات التي قد تفيد في حماية البيانات ومكافحة البرامج الخطيرة والضارة، على الرغم من وجود طرق أخرى كثيرة للعمل على حماية المعلومات، إلا أننا نامل بأن يكون قد قدم فائدة.

مصطلحات البحث: أمن المعلومات، حماية البيانات، حماية المعلومات.

Abstract

This research dealt with information security, its concept, methods of preserving and protecting it from harmful programs such as viruses or theft. The importance of information security has been clarified to protect companies or even individuals from intruders who want to harm others.

The presence of the Internet in our lives is easy for us a lot in obtaining what we want from data, programs or others, but this matter did not only have positives, but also has serious negatives that may threaten the private life of some, so our attempt to obtain some programs via the Internet from unreliable pages It was possible that there were insecure or tied links as soon as they were opened, stealing the information available to the person, as well as companies or institutions that could easily become penetrated and enter its database and cause malfunctions that may affect the work of the whole company.

The research has been presented with some information that may be useful in protecting data and fighting dangerous and harmful programs, although there are many other ways to work to protect information, but we hope that it has provided a benefit.

Keyword: Information Security, Data Protection, Information Protection.

المقدمة

انتشرت الأنظمة والأجهزة الرقمية في عصرنا الحاضر بشكل كبير، ويقصد بالنظام الرقمي، النظام الثنائي الذي يعتمد على تمثيل البيانات فيه وفق النظام الثنائي للعد، الذي يتكون من رقمين، هما الصفر والواحد. ويمكن تمثيل أي رقم أو حرف أو رمز من خلال النظام الثنائي، كما هو الحال في نظام (كود) الآسكي (ASCII). إذاً يمكن القول إن البيانات هي مجموعة الأرقام الثنائية، سواءً أكانت تمثل أرقاماً أم حروفاً أم رموزاً أم أي خليط منها، ومن الامثلة على البيانات ما يرسل عبر الشبكات من أرقام ثنائية على شكل سيل من البيانات (صفر، واحد) تتعامل معها الأجهزة فقط، ولا يستطيع أن يتعامل معها الإنسان. (القحطاني،2015م)

إن موضوع الأمن المعلوماتي يرتبط ارتباطاً وثيقاً بأمن الحاسوب فلا يوجد أمن للمعلومات إذا لم يراع أمن الحاسوب، وفي ظل التطورات المتسارعة في العالم التي أثرت على الامكانات التقنية المتقدمة المتاحة والرامية إلى خرق منظومات الحاسوب بهدف السرقة أو تخريب المعلومات أو تدمير أجهزة الحاسوب، كان لا بد من التفكير الجدي لتحديد الإجراءات الدفاعية والوقائية وحسب الإمكانات المتوفرة لحمايتها من أي اختراق أو تخريب، فكان على المنظمات أن تتحمل مسؤولية ضمان خلق اجواء أمنية للمعلومات تتضمن الحفاظ عليها.(الموسى،2010)

أمن المعلومات:

مراحل تطور مفهوم أمن المعلومات:

مر مفهوم أمن المعلومات بمراحل تطور متلاحقة، ففي الستينات كانت أجهزة الحاسوب وعملها هي شغل العاملين في أقسام المعلومات، وكان همهم هو كيفية تنفيذ البرامج والأنشطة المحوسبة ولم يكونوا مشغولين بأمن المعلومات بقدر انشغالهم بعمل الأجهزة وكان مفهوم الأمن يدور حول تحديد الوصول أو الاطلاع على البيانات من خلال منع كل غريب من التلاعب في الأجهزة لذلك ظهر مصطلح من الحاسوب والذي يعني حماية الحواسيب وقواعد البيانات، ونتيجة للتوسع في استخدام أجهزة الحاسوب وما تؤديه من منافع تتعلق باتساع أحجام معالجة البيانات، تغير الاهتمام ليمثل السيطرة على البيانات وحمايتها، و في السبعينات تم الانتقال إلى مفهوم أمن البيانات ورافق ذلك استخدام كلمات السر البسيطة للسيطرة على الوصول للبيانات لإضافة إلى وضع إجراءات الحماية لمواقع الحواسيب من الكوارث واعتماد خطط لتخزين نسخ إضافية من البيانات والبرمجيات بعيداً عن موقع الحاسوب، وفي مرحلة الثمانينيات والتسعينيات ازدادت أهمية استخدام البيانات، وساهمت التطورات في مجال تكنولوجيا المعلومات بالسماح لأكثر من مستخدم للمشاركة في قواعد البيانات، كل هذا أدى إلى الانتقال من مفهوم أمن البيانات إلى أمن المعلومات، وأصبح من الضروري المحافظة على المعلومات وتكاملها وتوفرها ودرجة موثوقيتها، حيث ان الإجراءات الأمنية المناسبة يمكن أن تساهم في ضمان النتائج المرجوة وتقلص اختراق نظم المعلومات والتلاعب بها.(الدنف،2013م)

مفهوم أمن المعلومات:

اختلف في تحديد مفهوم أمن المعلومات، فقد عرفه (الزغبي،2004م) أن أمن المعلومات هو اختصار الطرائق والوسائل المعتمدة للسيطرة على أنواع ومصادر المعلومات كافة وحمايتها من السرقة والتشويه والابتزاز والتلف والضياع والتزوير، والاستخدام غير المرخص وغير القانوني.

أما (الحميدي،2009م) فقد عرفها على أنها تشير إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات ويشمل أمن المعلومات الخصائص الخمسة التالية (السرية، الكمال، التوفير، التحقق من الهوية، مكافحة الإنكار).

مكونات ومحاور أمن نظم المعلومات:

إن بيئة نظام أمن المعلومات تتكون من أربع مكونات أساسية، وهي:(الهادي،2006م)

- التكنولوجيا.
- العمليات.
- البشر.
- الثقافة.

عناصر أمن المعلومات:

ذكر (القحطاني،2015م) أن عناصر أمن المعلومات: هي مجموعة العناصر الواجب توافرها لحماية المعلومات الثابتة والمنقولة، بحيث يغطي كل عنصر من هذه العناصر جانباً من جوانب الحماية المطلوبة، أي أنها تتكامل مع بعضها لتوفر الحماية المطلوبة.

فقد حدد الاتحاد العالمي للاتصالات في توصيته (X 800)، أن لأمن المعلومات عناصر يمكن حصرها في سبعة عناصر أساسية، وهي

- التحقق من الهوية: وتعني الخدمة التي يمكن من خلالها التحقق من هوية الشخص أو الجهة، وأنه الشخص المعني لا غيره. أي أن التحقق يبدأ بالتعريف بالهوية أو تحديد الهوية من خلال مثلاً اسم مستخدم وكلمة مرور أو رقم حساب. أحياناً تكون صعبة التحديد وذلك إذا تكررت في أكثر من مجال، وقد حُدد شقين رئيسين للتحقق من الهوية هما (التحقق من هوية الشخص أو الجهة، والآخر التحقق من أصل منشأ المعلومة)، ومن الأمثلة على الخروقات الممكنة التي يمكن أن تتم إذا لم يتوفر هذا العنصر: إمكانية دخول شخص غير مصرح له الدخول إلى شبكة المنشأة أو أنظمتها الداخلية.
- التحكم بالوصول: يأتي هذا العنصر بعد التحقق من الهوية، فبعد تحديد الهوية ويسمح بدخول الشخص إلى شبكة الحاسب مثلاًن فإنه يجري التحكم باستخدامه لموارد محددة من الشبكة، وليس جميع الموارد عن طريق التحكم بالوصول، حيث تحدد الأشخاص المصرح لهم فقط باستخدامها، ويشمل ذلك منع الاستخدام الغير مرخص لأي معلومة، وتحديد صلاحيات للأشخاص المصرح لهم بالوصول إلى المعلومات لاستخدامها والاطلاع عليها تحت شروط محددة. من الأمثلة على الخروقات التي ممكن حدوثها لعدم توفر

هذا العنصر: إمكانية طباعة بعض المستخدمين _ممن لديهم صلاحية الاطلاع على المعلومات المهمة_ بعد دخوله النظامي إلى شبكة المنشأة وثائق مهمة وحساسة على ورق، ومن ثم اطلاع أي شخص عليها.

- السرية: وتعين الحفاظ على المعلومات من أن يطلع عليها غير الأشخاص المصرح لهم فقط، فعندما ترسل رسالة سرية فإن ذلك يتطلب ألا يراها إلا المرسِل والمرسَل إليه فقط، فإن استطاع أحد الاطلاع عليها فإنه لا يستطيع أنيفهم محتواها، أي يجب أن تكون غير مفهومة. هناك العديد من الطرق لتوفير السرية تتراوح بين حجب المعلومة يدوياً، وعدم تسليمها إلا للأشخاص المصرح لهم فقط، إلى طرق التشفير الحديثة التي تعتمد على خوارزميات رياضية معقدة يصعب فكها. من الأمثلة على الخروقات الممكنة التي تحدث في حال عدم وجود هذا العنصر وهي: إمكانية الاطلاع على معلومات مهمة وحساسة من قبل أي أحد إذا ما وضعت هذه المعلومات وسط تخزين خارجي وهي غير مشفرة.
- سلامة المعلومة وتكاملها: تعني الحفاظ على المعلومات من الإضافة أو الحذف أو التعديل، أو إعادة التركيب، أو إعادة التوجيه. وهذا مهم لضمان الثقة في المعلومة و أنها أصلية دون زيادة أو نقصان. ومن الأمثلة على الخروقات الممكنة حال عدم توافره: أخطاء المستخدمين التي ينتج عنها التعدي على سلامة المعلومة أو الأنظمة المعالجة لها.
- عدم الإنكار: وتعني منع أي شخص أو أي جهة من إنكار أي معلومة قاموا بها وكشفهم، فمثلاً إذا منحت جهة معينة الصلاحية لجهة أخرى لشراء منتج معين ثم أنكرت بعد ذلك أنها منحت هذه الصلاحية لتلك الجهة فإن خدمة عدم الإنكار ستكشف ذلك. وتشمل أيضاً إثبات وقوع العمليات والإجراءات الإلكترونية في أوقات وتواريخ معينة عن طريق إلحاق بصمة التاريخ والوقت بالعملية نفسها، ومن الأمثلة على الخروقات الممكن حدوثها حالة عدم توفر عنصر عدم الإنكار: إمكانية التنصل من مسؤولية وثيقة معينة جرى تصديقها إلكترونياً من قبل أحد الأشخاص.
- توافر أو ديمومة المعلومة: أي أن تكون الشبكة والأجهزة والأنظمة والبرامج والخدمات متاحة في جميع الأوقات التي يحتاج إليها المستخدم وأن توفر لها الحماية مما قد يتسبب في عطل أو عدم توفر أي منها، وفي حال حدوث الأعطال أو الكوارث المعلوماتية يجب أن تكون هناك شبكة وأنظمة وبرامج بديلة، ومن الأمثلة على الخروقات الممكن حدوثها حالة عدم توفر عنصر ديمومة المعلومة: إمكانية تدمير أنظمة المنشأة باستخدام برنامج تدميري أو فيروس حديث الانتاج.
- المتابعة أو التدقيق: تهدف إلى متابعة عمليات المستخدمين والتحقق من فرض سياسات أمن المعلومات، وأنها تطبق بشكل صحيح ودقيق. وتعتمد على تسجيل أنشطة المستخدمين والأنظمة والبرامج التطبيقية بشكل مستمر.

المخاطر التي تتعرض لها الشبكات:

تتعرض الشبكات للكثير من المشكلات والمخاطر التي قد تؤثر على حفظ البيانات، ومن أبرز هذه المخاطر:(بامفلح،2002م)

- اقتحام الهاكرز والكراكرز للشبكة مما يؤدي إلى تفشي أسرار العمل والعاملين، أو تخريب البيانات وإتلافها، وذلك على اعتبار أن وصول أشخاص غير مصرح لهم إلى ملفات البيانات قد يعرض البيانات للتغيير أو التعديل أو المسح وبالتالي يؤدي إلى تحريف البيانات أحياناً وإلى سرقتها في أحيان أخرى.

- تعليق شخص لمعدات معينة على الكابلات بغرض التنصت عليها.
- مراقبة خطوط الهاتف والتجسس على مستخدمي الشبكة.
- اقتحام الفيروسات للشبكة سواء كانت فيروسات مزعجة فقط أم مدمرة تعرض أجهزة الشبكة وبياناتها للتلف أو الفقد.
- إطلاع الأشخاص المصرح لهم باستخدام الشبكة على معلومات غير مصرح لهم بالاطلاع عليها.
- التشويش على الإشارات المنقولة عبر الكابلات.
- تعطيل أحد الأشخاص لنظام الأمن الخاص بالشبكة أو كشفه لإجراءات الحماية المتبعة.

أنواع الهجوم على البيانات والمعلومات:

يقسم الهجوم إلى أربعة أقسام:(أبو سعد،2005م)

1- هجوم التنصت على الرسائل: وتقوم فكرته على أن المهاجم يراقب الاتصال بين المرسل والمستقبل للحصول على المعلومات السرية وهو ما يسمى بالتنصت على الاتصال.

2- هجوم الإيقاف: ويعتمد على قطع قناة الاتصال لإيقاف الرسالة أو البيانات من الوصول إلى المستقبل وهو ما يسمى أيضاً برفض الخدمة.

3- هجوم يعدل على محتوى الرسالة: وهنا يتدخل بين المرسل والمستقبل (يعتبر وسيط بين المرسل والمستقبل) وعندما تصل إلى المهاجم فإنه يقوم بتغيير محتوى الرسالة ومن ثم إرسالها إلى المستقبل، والمستقبل لا يعلم بتعديل الرسالة من قبل المهاجم.

4- الهجوم المزور أو المفبرك: وهنا يرسل المهاجم رسالة مفادها أنه صديقه ويطلب منه معلومات أو كلمات سرية خاصة بالشركة مثلاً.

الفيروسات و أنواعها:

في عام 2000م تم إجراء مسح لعدد كبير من الشركات وجِد أن 99.67% منهم قد تعرضوا على الأقل لفيروس واحد. فالفيروسات الجديدة كل يوم يتراوح عددها ما بين 10-20 فيروساً جديداً، بل إن شركة F-Secure المتخصصة في مكافحة الفيروسات أضافت 1418 تعريفاً لفيروسات جديدة خلال شهر نوفمبر 2004م، ويقدر عدد الفيروسات المعروفة بقرابة 100000 فيروس. إن للفيروسات أنواع منها:

- الفيروسات: هي برامج حاسوبية خبيثة مضرة بالحواسيب وتنتقل بينهم بعدة طرق، وتتكاثر بالاعتماد على ملفات أخرى، ولها أنواع كثيرة منها ما يبدأ عمله بوقت معين، ومنها ما يكون مكون من أجزاء متعددة، وغيرها.
- الديدان: برامج حاسوبية خبيثة ومضرة، تنتقل بين الحواسيب بعدة طرق، وتمتاز عن الفيروسات باعتمادها على نفسها لتتكاثر وبسرعة الانتقال وصغر حجمها، لكنها لا تقوم بحذف بيانات وإنما تؤثر سلباً على فعالية الحاسوب وشبكة المعلومات.
- البلاغ الكاذب: يبدأ من شخص يريد الضرر وينتشر بواسطة أناس صدقوا الكذبة ونشروا الخبر بغرض المساعدة في التصدي للفيروس أو الدودة، وممكن أن تكون على شكل بريد كاذب. (الغثبر و القحطاني،2009م)

مكافحة البرامج الضارة:

يمكن مكافحة الرامج الضارة باستخدام حزمة برامج واحدة لمكافحة كل من الفيروسات والديدان وغيرها في آن واحد، لذا لا بد من تثبيت برنامج مكافحة جيد وتحديثه دورياً لتوفير الحماية المطلوبة، ولا بد أن تشتمل برامج الحماية ليس فقط على كشف الإصابات وإنما إزالتها أيضاً، وهناك عدة برامج مشهورة لمكافحة البرامج الضارة يمكن الاعتماد عليها، أشهرها:(القحطاني،2015م)

- حزمة برامج مكافي(McAfee)
- حزمة برامج سيمانتك(Symantec)
- حزمة برامج كاسبر سكاي(Kasper SKY)
- حزمة برامج نورتون(Norton)

وفي جميع الحالات لا بد من اتباع خطوات للمكافحة، وهي:

- تحديث برامج المكافحة آليا ودورياً.
- تحديث نظام التشغيل آلياً ودورياً من خلال التحديث التلقائي.
- تحميل ملفات الاصلاح الأمنية الخاصة بأنظمة التشغيل وبعض البرامج التطبيقية الأخرى كحزمة برامج الأوفيس.
- عدم فتح مرفقات البريد الالكتروني التي لها الامتدادات التشغيلية مثل (vbs) (exe) (scr) أو التي لها أكر من امتداد مثل (txt.vbs).

الخاتمة

بات الآن من أكثر المشاكل التي تتعرض لها شبكات الحاسب الآلي ومستخدميها هو امن المعلومات وطرق حمايتها، وخصوصاً في ظل تزايد استخدام شبكة الانترنت كناقل رئيس للبيانات، وقد تطرقنا في هذا البحث إلى أهمية تفعيل برامج أو حزم للحفاظ على البيانات او المعلومات من المخاطر التي قد تتعرض لها وتؤثر على عملها.

وقد بيّنا عدة طرق للتعامل مع بعض المشاكل كالفيروسات والديدان وطرق الوقاية منها باستخدام برامج وحزم المكافحة كالمكافي والكاسبر سكاي وغيرها، إضافة إلى أنه تم توضيح وذكر طرق الحفاظ على فعالية عملها بالشكل السليم والمطلوب.

إن الحديث عن أمن المعلومات وطرق الحماية للأنظمة والبيانات لا يتوقف عند هذا الحد، وخصوصاً أنه علم يتجدد ويتطور بتطور البيانات وأنظمة الحواسيب وما تتعرض له باستمرار من تجديد ودخول لبرامج جديدة عليها، كما أن وجود البرامج المتنقلة عبر الانترنت له دور كبير في انتقال البرامج الضارة والفيروسات عبر الروابط الكاذبة أو إرسال رسائل مكذوبة تحتوي على برامج تسرق البيانات دون علم المستخدم.

المراجع

مراجع اللغة العربية

القحطاني، ذيب(2015م)، "أمن المعلومات"، مكتبة الملك فهد الوطنية، الرياض-السعودية.

الموسى، عبد الله(2010م)، "مقدمة في الحاسب والانترنت"، منظمة الأمم المتحدة للتربية والعلوم والثقافة، جامعة الملك فيصل بالأحساء، الطبعة السادسة.

بامفلح، فاتن(2002م)، "حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى_ دراسة حالة"، جامعة الملك عبد العزيز، المجلد(9)، العدد(18)، السعودية.

الحميدي، نجم(2009م)، "نظم المعلومات الإدارية – مدخل معاصر"، الطبعة الانية، دار اليازوري للنشر والتوزيع، عمان-الأردن.

الزعبي، هيثم(2004م)، "نظم المعلومات الإدارية"، الطبعة الأولى، دار صفاء للنشر والتوزيع، عمان-الأردن.

أبو سعد، وليد(2005م)، " أمن المعلومات Security"، الموسوعة العربية للكمبيوتر والانترنت.

الدنف، أيمن(2013م)، "واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها"، رسالة ماجستير غير منشورة، الجامعة الإسلامية –غزة-فلسطين.

الغثبر، خالد، والقحطاني، محمد(2005م)، "امن المعلومات بلغة ميسرة"، مكتبة الملك فهد الوطنية، الرياض-السعودية.