



**THE SCHOLAR JOURNAL FOR
SCIENCES & TECHNOLOGY**

Information security and network protection measures

أمن المعلومات و تدابير حماية الشبكة

إعداد



**Researcher/ Aouragh Karim
Cyber Security Management
Charisma University – UK**

Aouragh.karim@yahoo.com

تعد شبكة الإنترنت أحد تقنيات المعلوماتية و الاتصالات في العصر الحالي، لما لها من دور كبير في نشر المعلومات بين البشر في كافة أنحاء العالم. و مع توسع استخدام شبكة الإنترنت ، بدأت تظهر أنماط إجرامية مستحدثة على هذه الشبكة و تتمثل هذه الأنماط الإجرامية في الفيروسات و سرقة الأسرار السياسية و التجارية. في هذا المقال نقوم بدراسة مفاهيم أمن المعلومات و تدابير حماية الشبكة والوقاية من الفيروسات والتغلب على نقاط الضعف.

الكلمات المفتاحية: أمن المعلومات ، حماية الشبكة ، نقاط الضعف، الفيروسات.

Abstract:

The Internet is one of the information and communication technologies in the current era, because of its great role in disseminating information among people all over the world, and with the diversity of the use of the Internet, new criminal patterns began to appear on this network, and these criminal patterns are viruses and theft of political and commercial secrets. In this article, we study information security concepts, network protection measures, virus prevention, and overcoming vulnerabilities.

key words : Information security, network protection, vulnerabilities, viruses

المقدمة:

بالرغم من المزايا التي تحققت ولا تزال تتحقق كل يوم بفضل التطور الهائل في المجال الإلكتروني على جميع الأصعدة في شتى مجالات الحياة المعاصرة، لدرجة حتى أصبحت جميع القطاعات المختلفة تعتمد في أداء عملها بشكل أساسي على استخدام الحاسب الآلي بالدور الأول حيث أصبح العلم قرية صغيرة تربطها شبكات المعلومات. في هذا العصر اعتمدت المؤسسات في تسيير أعمالها على تقنية المعلومات التي أثبتت أنها تسهم في إنجاز الأعمال بسرعة عالية وبدقة متناهية. وحيث أن البيانات والمعلومات تخزن في مخازن معلومات مربوطة مع حاسبات المؤسسة من خلال شبكة الاتصال وغالبا ما تكون متاحة عبر شبكة الانترنت تسهيلات لإجراءات العمل واختصارا للوقت .

ولهذا تطورت طرق معالجة البيانات للتوافق مع بيئة الحاسبات من طرق يدوية إلى طرق آلية منتجة نظم سير العمل الإلكترونية لتصل إلى مفهوم الحكومة الإلكترونية .وبذلك نجد أن تقنية المعلومات قد ساهمت في تسهيل الأعمال الطبية والهندسية والصناعية والمصرفية وأنظمة المكاتب وأعمال المؤسسات التعليمية بل إنها أصبحت سلاحا في المؤسسات العسكرية يستخدم في الأعمال الحربية. إن هذه الشبكات تحتاج إلى حماية تضمن سلامة محتوياتها واستمرارية عملها .حيث وصل الأمر إلى أن الأعمال تتوقف في المؤسسات إذا تعطلت شبكات معلوماتها كشركات الطيران والشركات الكبيرة المنتشرة حول العالم بل إن التوقف القصير لتلك الشبكات يكبد أصحابها أو المستفيدين منها خسائر فادحة، وإن التوقف القصير لشبكات المعلومات الحكومية والوطنية يؤدي إلى تعطيل أعمالها مما ينعكس على انخفاض مستوى الخدمات المقدمة للمواطنين وإرباك في مؤسسات الدولة ذات العلاقة بالشبكات المتعطلة . وتوقف شبكات المؤسسات التجارية يسبب خسائر مالية كبيرة قد تؤدي في كثير من الأحيان إلى الإفلاس وغدت جودة الأعمال ونجاحها يعتمدان على جودة وأداء شبكات الاتصال واستمرارية عمل قواعد البيانات. أصبحت قضية أمن الشبكات تمثل حجر الأساس في بناء أي منظومة شبكية مهما كان حجمها وذلك بسبب تزايد وتنوع التهديدات الجديدة كالإصابة بالفيروسات والبرامج الضارة ومحاولات الاختراق لأغراض سرقة المعلومات أو التخريب أو التعديل والعبث، والتي نجدها دائما في حالة من التطور والتقدم السريع، ولمواجهة هذه التهديدات نحتاج إلى حلول أمنية متطورة والتي لم تعد متوفرة عبر طرق الحماية التقليدية، مما شكل تحدي أساسي في تأمين الحماية اللازمة لأي منظومة شبكية.

مشكلة الدراسة

أدى انتشار شبكات المعلومات الإلكترونية مع كل ما تحتوي من إيجابيات إلى ظهور مخاطر حديثة لم تكن معروفة في السابق ومنها أمن شبكة المعلومات الإلكترونية والمرتبطة بإمكانية التسلل إلى الشبكات وسرقة أسرار الشركات والحكومات والمؤسسات الأمنية والدفاعية، وترويج برامج التخريب والتجسس والقرصنة، وسرقة المواقع وإصابتها بالفيروسات والبرامج الضارة. وبناء على ذلك فإن مشكلة الدراسة يمكن تلخيصها في عدم توفر الوسائل والإجراءات الكافية لمواجهة الاختراق الإلكتروني و حماية الشبكات.

فرضيات الدراسة

1. هل توجد فروق ذات دلالة إحصائية بين الثغرات الأمنية في شبكات المعلومات وبين الإجراءات الوقائية المتخذة لمنع استغلال تلك الثغرات.
2. هل توجد فروق ذات دلالة إحصائية بين الإجراءات اللازمة لتجنب التهديدات وبين الإجراءات المتخذة.

الهدف من الدراسة:

1. التعرف على أمن المعلومات
2. التعرف على المخاطر والثغرات والتهديدات
3. التعرف على الفيروسات
4. تحديد نقاط الضعف في الشبكات المدروسة وتدابير تقويمها
5. التعرف على الإجراءات اللازمة لتحقيق حماية عالية لشبكات المعلومات.

أهمية الدراسة:

تتبع الأهمية النظرية للدراسة من أهمية المحافظة على أمن شبكات الحاسب الآلي الخاصة بالشركات وحمايتها من احتمال لاختراق والقرصنة أو التخريب، مما لها من تأثير على إستراتيجيتها وخططها المستقبلية وبالتالي نموها وتطورها في القطاع التي تنتمي إليه.

مفاهيم أمن المعلومات والشبكات

ظل مجال امن المعلومات والشبكات حتى أواخر سبعينيات القرن الماضي معروفاً باسم أمن الاتصالات Communication Security, COMSEC والذي حددته توصيات أمن نظم المعلومات والاتصالات لوكالة

الأمن القومي بالولايات المتحدة بما يلي:

المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أشخاص غير مخولين عبر الاتصالات وضمان أصالة وصحة هذه الاتصالات وتضمنت النشاطات المحددة لأمن الاتصالات أربعة محاور هي:

1. أمن التشفير security Crypto

2. أمن الإرسال Transmission Security

3. أمن الإشعاع Security Emission

4. الأمن الفيزيائي (المادي) Physical Security

و يتضمن تعريف أمن الاتصالات خاصيتين وهما:

1. السرية Confidentiality: وتعنى بالتأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل

أشخاص غير مخولين بذلك. (الشهري، 2001)

2. الخطر risk : وهو مفهوم يشير إلى التأثيرات السالبة والمحتملة على الأصول والممتلكات القيمة والتي

قد تنتج من عملية حالية أو حدث مستقبلي. بدأت في الثمانينات من القرن الماضي ومع النمو

المضطرد للحواسيب الشخصية واستخداماتها , حقبة جديدة من الأمن وهى حقبة أمن الحواسيب

Computer Security, COMPUSEC, والتي حددتها توصيات أمن نظم المعلومات والاتصالات

وكالة الأمن القومي بالولايات المتحدة بما يلي :

المعايير والإجراءات التي تضمن سرية و كمال وتوفر مكونات نظم المعلومات بما فيها التجهيزات والبرمجيات

والبرمجيات المدمجة firmware والمعلومات التي تتم معالجتها وتخزينها ونقلها. (أبو مدين، 2018)

تضمن أمن الحواسيب خاصيتين إضافيتين وهما:

1- التكاملية وسلامة المحتوى Integrity: وتعنى بالتأكد من أن محتوى الرسائل (المعلومات) صحيح

ولم يتم تعديله أو العبث به. وبشكل خاص لم يتم تدمير المحتوى أو تغييره أو العبث به في أية مرحلة

من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع خلال الإرسال.

2- استمرارية توفر المعلومات أو الخدمة: Availability التأكيد من استمرار عمل نظام المعلومات

والشبكات و استمرار مقدرتها على التفاعل مع المعلومات والمستخدمين وعدم توقف أو حجب الخدمة وعدم إمكانية النفاذ كنتيجة للهجوم عليها أو تدميرها وتخريبها.

لاحقاً وفي التسعينات من القرن الماضي تم دمج مفهومي أمن الاتصالات وأمن الحواسيب لتشكيل ما أصبح يعرف باسم أمن نظم المعلومات.. Information Systems Security –INFOSEC يشتمل مفهوم أمن نظم المعلومات الخصائص الأربع المذكورة مسبقاً ضمن مفاهيم أمن الاتصالات وأمن الحواسيب، وهي السرية والموثوقية والكمال والتوفر، كما أضيفت إليها خاصية جديدة وهي مكافحة الإنكار، أو منع إنكار التصرف المرتبط بالمعلومات ممن قام به، Non-repudiation والقصد هنا هو ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها إنه هو الذي قام بهذا التصرف، بحيث توفر هذه الخاصية المقدرة على إثبات أن تصرفاً ما قد تم من شخص ما في وقت معين . (المنج، 2022)

المخاطر والثغرات والتهديدات

يعرف الأمن بالحماية من المخاطر والفقدان. بصورة عامة مفهوم الأمن شبيه بمفهوم السلامة. الفارق الدقيق بين المفهومين يتمثل في التركيز الإضافي للأمن على الحماية من المخاطر الخارجية المتمثلة في الأفراد والأنشطة التي تنتهك الحماية وتكون مسئولة مباشرة عن خرق الأمن. يستخدم تعبير الأمن بصورة عامة كمرادف لتعبير السلامة ، ولكن من ناحية فنية يعنى تعبير الأمن ليس فقط السلامة بل العمل على توفير السلامة أيضاً.

هناك مفاهيم محددة تتكرر في مجالات الأمن المختلفة منها:

1. **الخطر: risk** وهو احتمال حدوث حدث معين يكون لديه تأثير على إنجاز الأهداف. في مجال العلوم

الهندسية يعرف الخطر كمياً بحاصل ضرب احتمال حدوث الحادثة والخسارة في الحادثة الواحدة.

ويعتبر الخطر مؤشراً للتهديدات ويعتمد على التهديدات والثغرات والتأثير على العمليات وعدم التأكد يوجد العديد من الطرق والأساليب لتقييم وقياس الخطر.

في أمن المعلومات والشبكات يحدد الخطر باستخدام ثلاثة متغيرات (عوامل) وهي:

1- احتمال أن يكون هناك تهديداً.

2- احتمال إن تكون هناك ثغرات .

3- التأثير المحتمل للخطر.

إن أصبحت أي من هذه المتغيرات تساوي صفراً يقترب الخطر الكلي على النظام أو الشبكة من الصفر أيضاً

2. **الثغرات: Vulnerability** (أو عدم التحصين) وبصورة عامة تعرف بالحساسية اتجاه الأذى أو

الهجوم

الجسدي أو النفسي. كما تعني أيضاً عدم توفر الحماية اللازمة للممتلكات والأصول القيمة. في أمن الحاسوب والشبكات يستخدم تعبير الثغرات للإشارة إلى أماكن الضعف في هذه النظم والتي تتيح للمهاجم الاعتداء على سلامة النظام. وقد يتسبب في الثغرات قصور في البرمجيات أو خلل في التصميم، نتيجة لإهمال المبرمج أو المصمم، أو استخدام المهاجم لبرامج خبيثة مثل برامج الفيروسات. يمكن تصنيف الثغرات في أمن الحاسوب والشبكات إلى فئتين:

(1) ثغرات فنية: وتكون نتيجة لضعف التحصين الناتج من التقنيات المستخدمة في النظم والشبكات، في

هذه الحالة يعرف الهجوم على الشبكة بالهجوم التقني.

(2) ثغرات إدارية: وتكون نتيجة لأسباب غير فنية ويعرف الهجوم على الشبكة أو الحاسوب في هذه الحالة

بهجوم الهندسة الاجتماعية. social engineering attack

كما يمكن تقسيم الثغرات من حيث الصعوبة والسهولة إلى فئتين:

أ- ثغرات المستوى الأعلى، High-level Vulnerability، وهو ثغرات سهلة الاستغلال، ومثال عليها كتابه شفرة برنامج لاستغلال تلك الثغرة.

ب- ثغرات المستوى الأدنى Low-level Vulnerability وهذا النوع من ثغرات يصعب استغلاله ويتطلب الكثير من الجهد والموارد من قبل المهاجم.

3. **التهديدات: Threats** وهو احتمال التطفل على الأصول والممتلكات (المعلومات) بدون إذن صاحبها

وقسراً وعبر ثغرة محتملة في النظام، بهدف سرقتها أو تخريبها، وفي حالة حدوثها تمثل التهديدات خطراً على النظام. هناك ثلاثة مكونات أساسية للتهديد وهي:

(1) الهدف: ويمثل في أمن الحاسوب والشبكات المعلومات المخزنة أو المرسلة عبر الشبكات بغرض

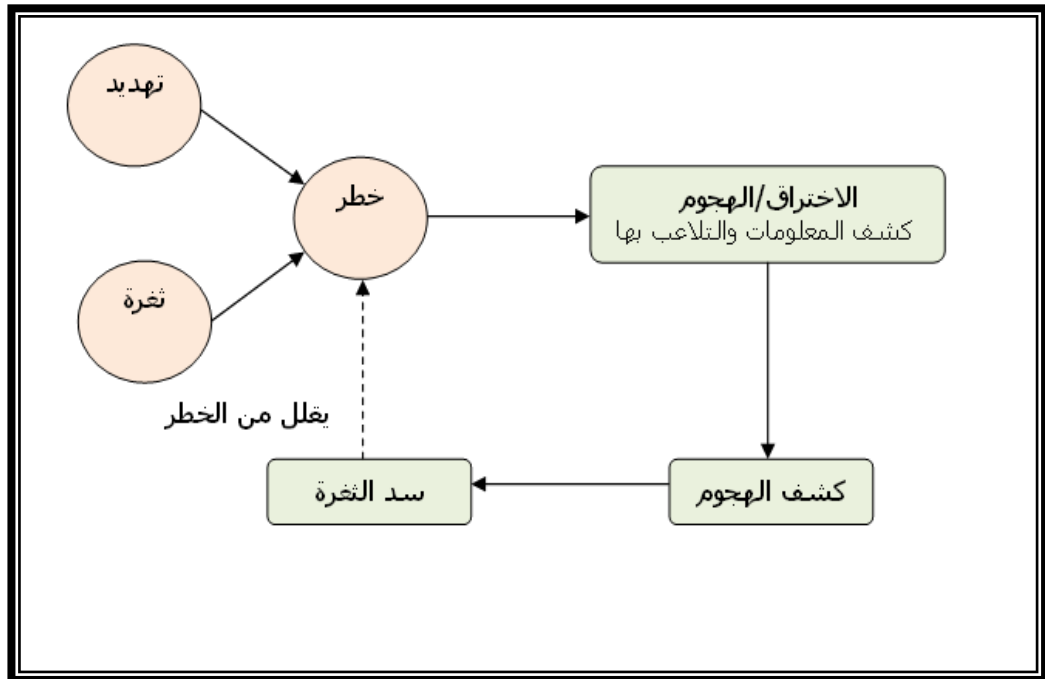
سريتها أو سلامتها أو تواجدها.

(2) العميل: وهي البرامج والأشياء المكونة والمنشأة للتهديد، ويتطلب استخدامها النفاذ إلى الحاسوب أو الشبكات بالإضافة إلى معلومات عن خصائص تشغيلها وآليات الأمن المستخدمة فيها وذلك للبحث عن ثغرة للنفاذ من خلالها إلى النظام أو الشبكة .

(3) الحدث: ويمثل نوعية التأثير لوضعية التهديد ويستخدم لذلك بطرق عديدة من أهمها إساءة النفاذ المخول

Authorized وغير المخول Unauthorized إلى المعلومات أو النظام. ووضع شفرات خبيثة Malicious مثل شفرات الفيروسات في النظام. (مأمون، 2004)

الشكل 1 يوضح العلاقة بين مكونات نظام أمن المعلومات والشبكات وتأثيرها ببعضها البعض.



الشكل 1: يوضح العلاقة بين مكونات نظام أمن المعلومات والشبكات وتأثيرها ببعضها البعض.

عناصر أمن المعلومات

تتمحور عناصر أمن المعلومات في عدة مجالات منها:

- أمن أماكن حفظ البيانات و المعلومات : ويهتم هذا المجال بالعديد من الآليات العلمية والعملية المرتبطة بأماكن حفظ البيانات والبيئة المحيطة بها، وذلك للتأكد من تواجد المعلومات في أماكن آمنة مثل مراكز البيانات، Data Centers، والتي يجب أن تخضع لرقابة دقيقة وإجراءات أمنية مادية عالية في

- الدخول , بحيث لا يصل إلى الأجهزة إلا من هو مصرح له ومن خلال بوابة آمنة والتي قد تعتمد أحياناً على التقنيات المتقدمة مثل قراءة بصمة الإصبع (Printfnger) وقرجية العين (Printeye) أو تردد الصوت أو من خلال الأرقام المتسلسلة أو البطاقات الممغنطة, وغيرها.
- **أمن طريقة حفظ البيانات :** ويتم ذلك من خلال استخدام التقنيات المتقدمة لتشفير المعلومات المحفوظة (Encryption) بمختلف أنواع التشفير المتناظر أو غير المتناظر , وسواء كان معتمداً دولياً أو أسلوب تشفير مطوراً محلياً.
- **أمن وسائط حفظ البيانات :** ويتحقق هذا المحور من خلال الحفظ على الأنسب من الأقراص الصلبة (HDD) أو كروت الذاكرة (CASH) أو الأقراص المدمجة (CD) وغيرها من وسائط الحفظ المناسبة.
- **أمن حماية المعلومة :** ويتم بعدة آليات مثل استخدام برامج الحماية أو الجدران النارية Firewalls للحماية من اختراق الأجهزة المرتبطة بالشبكات واستخدام المرشحات Filters لضمان عدم نقل المعلومات غير المسموح بنقلها , واستخدام برامج مكافحة الفيروسات (Anti-Virus) للحماية من الفيروسات المختلفة والنسخ الاحتياطي (Backup) لمعالجة مشكلة فقدان البيانات الرقمية غير المكتوبة والتي تكون أكثر عرضة من غيرها للتلف أو العطب أو فقدان ويتم ذلك بعدد من الآليات.
- **أمن نقل المعلومات والبيانات :** قديماً كانت تستخدم آليات النقل المادي المباشر للبيانات وتحاط بسرية وحماية هذه الآليات بطيئة نسبياً , والمتأمل حالياً يرى أن تلك الطريقة كانت أكثر أمناً من الطرق الحديثة المعتمدة على التواصل الإلكتروني. وبعد التقدم التقني أصبحت آليات النقل الحديثة بما تميزت به من سرعة النقل والدقة هي الأنسب عند أخذ الاحتياطات الأمنية اللازمة في عمليات نقل البيانات , ولذا نرى بأن هذا المجال يهتم بالبيئات الآمنة لنقل البيانات والمعلومات عبر الشبكات والنفوذ إليها.

- **أمن نظم الاتصالات وبيئات النقل المستخدمة :** وذلك عندما يكون الاتصال مباشراً بواسطة خطوط الهاتف أو بالاتصال المباشر بالأقمار الاصطناعية ,وعندما يكون حجم البيانات متوسطاً نسبياً.

وتكمن الخطورة هنا عند وجود متطفلين يقومون بعمليات بالتطفل Sniffing على خطوط الاتصال وتبرز هنا أهمية تشفير البيانات بقوة وكفاءة عالية والمحافظة على سلامة خط الاتصال من وجود المعترضين أو المتجسسين .(جويل و ماك كلور و كيرتز ، جورج ، 2001).

- **أمن التطبيقات المستخدمة والبروتوكولات :** عندما يكون الاتصال غير مباشر وعبر وسيط مثل الإنترنت أو يكون نقل البيانات لموقع خدمات عالي الأهمية الأمنية مثل المصاريف أو للشراء المباشر

ببطاقات الائتمان الإلكترونية، يمثل التجسس والاختراق أبرز المشاكل الأمنية والتي لا يمكن القضاء عليها بشكل كامل بل يمكن الحد منها بشكل كبير عن طريق استخدام البروتوكولات الآمنة على مستوى طبقة التطبيقات أو طبقة الشبكة، وهنا تظهر أهمية التوقيعات الرقمية والشهادات الإلكترونية للمواقع الآمنة وغيرها من وسائل الحماية.. (طوم، 2004)

- **البحث عن مصادر الخطر المتوقعة على المعلومة لمكافحتها :** تعتبر مصادر الخطر وتهديدات أمن

البيانات والشبكات كثيرة جداً و لعل من أهمها خطورة النفاذ إلى البيانات من قبل أشخاص غير مسموح لهم بذلك وبالتالي يتم تسريب المعلومات أو إتلافها أو تغييرها ويمكن أن يستعين أولئك المهاجمون بالعديد من الوسائل

التي توصلهم للبيانات أو تمكنهم من إتلافها أو تغييرها بعدة طرق . (بسيوني، 2004)

فيروسات الحاسوب

تعريف الفيروسات :

تنتشر فيروسات الحاسب بشكل كبير و تتطور بسرعة كبيرة نظراً للتطور التقني الذي نشهده في حياتنا كل يوم حيث تصاب الآلاف من الأجهزة الحاسوبية بشكل يومي جراء تلك الفيروسات مما يصيب مستخدميها بخسائر مادية و معنوية جسيمة حيث تتم سرقة معلوماتهم الشخصية و من ثم محاولة ابتزازهم مادياً للحصول على الملفات مرة أخرى.

فيروس الحاسوب هو برنامج خارجي صنع عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب و ما شابهها من عمليات. أي أن فيروسات الكمبيوتر هي برامج تتم كتابتها بواسطة مبرمجين محترفين بغرض إلحاق الضرر بكمبيوتر آخر، أو السيطرة عليه أو سرقة بيانات مهمة ، و تتم كتابتها بطريقة معينة.

يتصف فيروس الحاسب بأنه برنامج قادر على التناسخ (Replication) و الانتشار. الفيروس يربط نفسه ببرنامج آخر يسمى الحاضن (host) لا يمكن أن تنشأ الفيروسات من ذاتها. يمكن أن تنتقل من حاسوب مصاب لآخر سليم. (عبدالجابر، 2014) ، (سابا، 2018)

فالفيروس عبارة عن برنامج صمم لينشر نفسه بين الملفات و يندمج أو يلتصق بالبرامج. فعند تشغيل البرنامج المصاب فإنه قد يصيب باقي الملفات الموجودة معه في القرص الصلب أو المرن، لذا يحتاج الفيروس إلى تدخل من جانب المستخدم كي ينتشر، بطبيعة الحال التدخل عبارة عن تشغيله بعد أن تم جلبه من الإيميل أو تنزيله من الإنترنت أو من خلال تبادل الأقراص المرنة.

مكونات الفيروس

يتكون برنامج الفيروس بشكل عام من أربعة أجزاء رئيسية وهي:

(1 The Replication Mechanism :آلية التناسخ و هو الجزء الذي يسمح للفيروس أن ينسخ نفسه.

(2 The Protection Mechanism :آلية التخفي و هو الجزء الذي يخفي الفيروس عن الاكتشاف.

(3 The trigger Mechanism :آلية التنشيط و هو الجزء الذي يسمح للفيروس بالانتشار قبل أن يعرف وجوده كاستخدام توقيت الساعة في الحاسوب كما في فيروس Michelangelo الذي ينشط في السادس من مارس من كل عام.

(4 The Payload Mechanism :آلية التنفيذ و هو الجزء الذي ينفذ الفيروس عندما يتم تنشيطه

كيفية عمل الفيروسات

يقوم من أنشأ الفيروس ببرمجة الفيروس و توجيه الأوامر له حيث يقوم بتحديد الزمان و متى و كيف يبدأ الفيروس بالنشاط و عادة ما تعطى فرصة كافية من الوقت للفيروس حتى يضمن حرية الانتشار دون أن يلفت الانتباه ليتمكن من إصابة أكبر عدد ممكن من المستخدمين، و تختلف الفيروسات من حيث بدأ النشاط فهناك من يبدأ بتاريخ أو وقت محدد و هنالك من يبدأ بالعمل بعد تنفيذ أمر معين في البرنامج

المصاب و هناك من الفيروسات من يبدأ بالنشاط بعد التكاثر و الوصول الى رقم معين من النسخ. و بعد أن ينشط الفيروس يقوم الفيروس بعدة أنشطة تخريبية حسب الغرض من إنشاء ذلك الفيروس فهناك من يقوم بعرض رسالة تستخف بالمستخدم أو تقوم بعرض رسالة تحذيرية عن امتلاء الذاكرة و هناك أنواع أخرى تقوم بحذف أو تعديل بعض

الملفات و هناك من يقوم بتكرار و نسخ نفسه حتى يشل جهازك تماماً و هناك أنواع أشد فتكاً فتقوم بمسح كل المعلومات من القرص الصلب .(حجار ، 2003)

أسباب انتشار فيروسات الحاسوب

- تتنوع أسباب انتشار الفيروسات على أجهزة الحاسب الخاصة بالمستخدمين في العالم و من أهمها:
 - أن تلك الفيروسات تنتشر من خلال البرامج التي يتم تنزيلها من شبكة الإنترنت خاصة حين يتم الاعتماد على مواقع مجهولة المصدر و بمجرد أن يقوم المستخدم بتثبيت البرنامج على الجهاز تنشط تلك الفيروسات لتقوم بدورها في إتلاف الجهاز.
 - يلجأ بعض المستخدمين إلى استخدام ما يسمى بالكراك و هي أداة صغيرة يتم اللجوء إليها لتنفيذ البرامج التي تحتاج إلى أموال لشرائها و إمكانية تثبيتها و تسمى البرامج المدفوعة و تعمل تلك الأداة على تشغيل البرنامج مجاناً و لكنها تحمل في جعبتها العديد من الفيروسات التي تخترق جهاز الحاسوب.
 - تبادل الملفات المصابة بين المستخدمين عن طريق ربط جهازين معاً أحدهما مصاب بالفيروسات فبالطبع يؤثر على الجهاز السليم و تنتقل تلك الفيروسات بسهولة إلى الجهاز الآخر.
 - النقر على روابط مرسله إلى المستخدم دون معرفة من المرسل، فأحياناً يتم إرسال مثل تلك الفيروسات على هيئة روابط إلكترونية و بمجرد الضغط عليها يتم تنزيل الفيروس مباشرة للجهاز
 - انتشار الفيروسات من خلال البريد الإلكتروني، فالغالب اليوم أن يشق الفيروس طريقه إلى كمبيوترك الشخصي من خلال مرفقات البريد الإلكتروني، و بمجرد أن تقوم بفتح الملف المرفق، فإن الفيروس يخرج ليصيب جهازك، و ربما لينسخ نفسه، ناقلاً العدوى إلى جميع العناوين الإلكترونية الموجودة في كتاب

العناوين Address Book

أهم أضرار الفيروسات:

مع تنوع الفيروسات و تكاثرها بشكل مستمر تتنوع الأضرار التي تلحقها بجهاز الكمبيوتر الخاص بك و لكن يمكن إجمال أضرار الفيروسات في عدة نقاط:

تعمل الفيروسات التي تخترق جهاز الكمبيوتر إلى تدمير الجهاز بشكل كامل من خلال الاستقرار في ملفات القرص الصلب بالإضافة إلى ذاكرة التخزين العشوائي و التحكم في إعدادات الجهاز ما يصيب الجهاز بالبطء في النهاية و من ثم تدميره بشكل كامل، كما تعمل الفيروسات التي تلحق بالبرامج المثبتة على جهاز الكمبيوتر بإحداث أعطال في البرامج و منعها من القيام بمهمتها الأساسية. تعمل الفيروسات التي تصيب المواقع الإلكترونية التي تقوم بتصفحها بسرقة البيانات الشخصية الخاصة بك و الاطلاع على ما تقوم بإرساله عبر المواقع المختلفة، حيث تستهدف الفيروسات إحداث ثغرات في جهازك ما يمنع برامج مكافحة الفيروسات من اكتشافها و محاربتها ما يجعل الجهاز بيئة مفتوحة للفيروسات.(المصدر السابق)

النتائج

ان البحث و الدراسة التي سبق استعراضها تشير إلى أنه ينبغي اتخاذ الإجراءات التالية لحماية الشبكة من المخاطر والثغرات والتهديدات:

1. تثبيت جدار الحماية .
2. تثبيت أنظمة الحماية من الفيروسات.
3. تثبيت برنامج مراقبة استخدام الإنترنت.
4. استخدام كلمة مرور بطول 8 أحرف على الأقل.
5. تحديث نظم تشغيل.
6. تحديث برامج الحماية من الفيروسات.
7. تحديث جدران الحماية.
8. تنفيذ اختبار دوري لكشف نقاط الضعف من داخل الشبكة ومن خارجها.
9. استخدام مجموعة متنوعة من التقنيات لتقدير الضعف.

الخلاصة:

لقد واجهت بعض الشركات في الواقع العملي مشاكل بسبب ضعف نظام أمن المعلومات الإلكترونية لديها مما أدى إلى اختراق بياناتها والاحتيايل عليها أو إتلاف بياناتها وبالتالي تكبدها خسائر مالية كبيرة لتعويض هذا الأمر فإن بعض الشركات قد تعاني من ضعف في توفير متطلبات الرقابة على أمن معلوماتها نظراً لضعف أنظمتها للرقابة الداخلية، ومن هنا تأتي هذه الدراسة لتسهم في اكتشاف واقع هذا الأمر ، ويؤمل أن تؤدي هذه الدراسة إل تقديم نتائج وتوصيات مفيدة للشركات أو للعاملين في مختلف القطاعات الأمنية عسكرية كانت أو مدنية والعاملين في المجالات الصناعية والتجارية حكومية كانت أم أهلية تساهم في تحديد بعض نقاط الضعف ضمن مكونات نظم المعلومات الإلكترونية للمحافظة على أمن معلوماتها.

التوصيات:

الإنترنت أصبح يستخدم ويعتمد عليه بشكل هائل وبما يحمله من ملايين الإتصالات , أصبح يشكل تهديد جدي لسلامة البيانات التي تنساب في الشبكات إن معرفة سبل حماية خصوصية معلوماتك وأجهزتك أثناء استخدامك للإنترنت يقلل من احتمال تعرضها لمخاطر الاستخدام غير المشروع، والذي يلحق الضرر بك مادياً أو معنوياً.

المصادر

1. أبو مدين، أنوار أبو بكر (2018). الإنترنت و الحماية من الفيروسات ، الدراسات العليا بقسم الحاسب الآلي ، جامعة طرابلس ، ليبيا.
2. بسيوني، عبد الحميد (2004). الحروب الإلكترونية وقرصنة المعلومات ، دار الكتب العلمية للنشر والتوزيع، القاهرة .
3. جويل ، سكامبراي و ماك كلور ، ستيوارت و كيرتز، جورج (2001). "الهكرز" القرصنة تحت الأضواء ، أسرار وحلول لحماية الشبكات، ط2 ، ترجمة مركز التعريب والترجمة الدار العربية للعلوم ، بيروت.
4. حجار، فادي (2003). تشريح الفيروسات ، شعاع للنشر والعلوم، حلب.
5. سابا ، غسان (2018). أمن الشبكات و البنية التحتية المعلوماتية ، منشورات الجامعة الافتراضية السورية.
6. الشهري، فايز بن عبد الله (2001). استخدامات شبكة الانترنت في مجال الإعلام الأمني العربي ، مجلة البحوث الأمنية ، تصدر عن مركز الدراسات بكلية الملك فهد الأمنية ، الرياض، مج 10 ، ع19.
7. طوم ، توماس (2004). الخطوة الأولى نحو أمان الشبكات ، ترجمة مركز التعريب والترجمة ، الدار العربية للعلوم، بيروت.
8. عبدالجابر، يوسف خليل يوسف. (2014) . مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية، الرسالة الماجستير في المحاسبة قسم المحاسبة والتمويل –كلية الأعمال (جامعة الشرق الأوسط 2014).
9. المنج ،نواف صالح (2022). أمن المعلومات للشبكات الصغيرة و المتوسطة، مكتبة نور.
10. مأمون، نعيم (2004). قرصنة البرامج بلا أقنعة – الأسس النظرية والعملية لكسر حماية البرامج وطرق الوقاية المضادة، دار شعاع للنشر.