وزارة التعليم العالي والبحث العلمي

جامعة ديالى

كلية التربية الاساسية

قسم الحاسبات

دراسة نظرية عن الفيروسات

بحث تقدمت به الطالبتان

زينه طاهر حبيب ايمان محمد سلمان

الى مجلس قسم الحاسبات / كلية التربية الأساسية

استكمالاً لمتطلبات نيل شهادة البكالوريوس في التربية – الحاسبات

اشراف

م.م. شيماء طه

1439هـ 2018م

﴿ هو الذي يصوركم في الارحام كيف يشاء ﴾

صدق الله العظيم

سورة آل عمران: أية (6)

الإهداء

الى من غرس في ذاتي ديمومة الطموح و الاعتماد على الله ثم على النفس ، الى نقش في صدري حب العلم و العطاء و الانفة و علو الهامة و تحدي الذات للوصول الى المبتغى و المرام . . . أبي العزيز

الى من ارضعتني الحب و الحنان ، الى رمز الحب و بلسم الشفاء ، الى القلب الناصع بالبياض . . . . . امي الحبيبة .

الى القلوب الطاهرة الرقيقة و النفوس البريئة الى رياحين حياتي . . . اخوتي

الى كل من ساندني و قدم لي الدعم و المؤازرة و انار لي دروب المعرفة و مسالكها .

الهدى

الى المجتمع الاكاديمي العلمي

شكر وتقدير

في مثل هذه اللحظات يتوقف اليراع قبل ان يخط الحروف ليجمعها في الكلمات تتبعثر الاحرف وعبثا ان يحاول تجميعها في سطور و سطور كثيرة تمر في الخيال ولا يبقى لنا في نهاية المطاف الا قليلا من الذكريات و صور تجمعنا برفاق كانوا الى جانبنا .....

الواجب علينا شكرهم ووداعهم و نحن نخطو خطوتنا الاولى ونخص بجزيل الشكر و العرفان الى كل من اشعل شمعة في دروب عملنا و من وقف على المنابر و اعطانا من بنيات فكرة لينير دربنا الى الاساتذة الكرام في كلية التربية الاساسية قسم الحاسبات .

و نتوجه بالشكر الجزيل الى الاستاذة (م.م شيماء طه التي تفضلت بالاشراف على هذا البحث فجزاها الله عنا كل خير و لها منا كل التقدير و الاحترام.

الباحثة

قائمة المحتويات

الفصل الأول

الاطار العام للبحث

الفصل الاول

الاطار العام للبحث

مقدمة

في عصرنا عصر المعلومات الذي يشهد نموا سريعا في المعلومات والمعارف حيث "تتضاعف كمية المعلومات كل خمس سنوات وتتضاعف قوة الحاسب الآلي كل سنتين وفي هذا العصر نشهد ثورة في المعلومات الذي يقوم فيها الحاسب الآلي بالدور الأول حيث أصبح العلم قرية صغيرة تربطها شبكات المعلومات.

ونظرا لكثرة الأخطار التي تهدد سلامة البيانات التي تنساب في الشبكات أو البيانات المحتضنة في خزائنها وكثرة الأخطار التي تهدد استقرار تلك الشبكات وأمنها كالإصابة بالفيروسات والبرامج الضارة ومحاولات الاختراق الأغراض سرقة المعلومات أو التخريب أو التعديل والعبث، تأتي أهمية الحماية على مدار الساعة لمكونات شبكات المعلومات المادية والبرمجية بتثبيت أجهزة و برامج الحماية في بوابات الشبكات المحلية وداخل تلك الشبكات وإدارة تلك الأجهزة والبرمجيات من الزاوية الأمنية وسد الثغرات أولا بأول لتضييق فرص قراصنة المعلومات والمنافسين والأعداء من التمكن من اختراق أو سرقة أية بيانات من شبكات المعلومات.

بعد انتشار استخدام الحاسبات الآلية على جميع الأصعدة الاقتصادية والاجتماعية والسياسية واستخدام الأفراد لها، ناهيك عن المؤسسات والمنظمات فإن كمية المعلومات المتبادلة والمنقولة عبر شبكات الاتصال ازدادت بشكل مذهل، وانتشرت الشبكات في كل مكان مستخدمة لأشكال متعددة من الوسائط كالكابلات التي تربط المؤسسات والدول على الأرض، والهوائيات والأقمار الصناعية التي تنقل الإشارات اللاسلكية عبر الجو، وقد يكون وسط النقل هجينا يستخدم أكثر من نوع

في آن واحد، كل ذلك لتسهيل انتقال المعلومات وتقصير المسافات. وفي هذا السياق جاءت شبكة الانترنت لتتيح لكل فرد أن يحصل على ما يشاء من المعلومات في مختلف أنحاء الدنيا وفي أي وقت وعلى مدار الساعة. ناهيك عن إتاحة الفرصة لمن يرغب لإضافة بيانات إلى قواعد المعلومات المتاحة في شبكة الانترنت.

مشكلة البحث

لقد توسع مجتمع المعلومات وكثرت التعاملات الالكترونية في العالم ولعل إلقاء نظرة على استخدام البريد الالكتروني الشائع يعطي صورة عن أهمية شبكة الانترنت و شبكات المعلومات عموما ومن ذلك يمكن لنا ان نتخيل مدى ضخامة الشبكات المعلوماتية و استخداماتها و مدى زيادة الاخطار المتلازمة مع زيادة المستخدمين و التي تهدد استقرار شبكات المعلومات و التي يجب حمايتها و ضمان عدم اختراقها و قرصنة محتوياتها و مواردها .

ويترتب على ذلك إنجاز تصميم جيد لشبكات الاتصال الرئيسة وتأمين متطلبات الحماية الفيزيائية لها، ويتطلب الإعداد والضبط الدقيقين لتجهيزات الحماية من حيث إعداد لوائح التحكم بالوصول وضبط صلاحيات تسجيل الدخول والنفاذ إلى تجهيزات الشبكة ومواردها بالإضافة العمليات تثبيت تحديثات مكونات شبكة المعلومات سواء كانت أجهزة أو برمجيات وترقية نظم التشغيل. إن حصر وتوثيق هذه الإجراءات والعمليات ومتابعتها فنيا وإداريا يحتاج لجهود فنية وإدارية تتكامل لتصبح قابلة للتطبيق وتصلح لأي منشأة تعتمد في أعمالها على تقنيات المعلومات بحيث يأخذ بالاعتبار الهيكل التنظيمي لإدارة تقنية المعلومات والمسميات الوظيفية لها والمؤهلات العلمية لشاغلي هذه الوظائف والإجراءات الإدارية والفنية اللازمة لضمان الحماية القصوى للشبكات الرئيسة جميع مواردها.

إن المشكلات الأمنية التي أوجدها شبكات الحاسب و بخاصة شبكة الانترنت والتي تتلخص بتعطيل وتدمير المواقع الحكومية والتجارية، والتسلل إلى الشبكات وسرقة أسرار الشركات والحكومات والمؤسسات الأمنية والدفاعية، وترويج برامج

التخريب والتجسس والقرصنة، وسرقة المواقع وانتهاك حقوق الملكية الفكرية، بالإضافة إلى أن شبكة الانترنت صارت وسيلة اتصال فعالة للعصابات والمجرمين والمخالفين للقانون والأعراف الاجتماعية والأخلاقية السائدة، وتوفر بيئة خصبة للترويج للتجارة المحرمة وغسيل الأموال والجرائم المنظمة، وتشكل ميدانا حديثا من ميادين الحرب الإلكترونية تتسابق فيه الجيوش و مراكز البحوث العسكرية لتطوير تقنيات الدفاع الالكترونية العالية .

فرضيات البحث

1. لا توجد فروق ذات دلالة إحصائية بين كمية الأجهزة والبرامج المستخدمة لحماية الشبكات بإعداد و تحديث تلك الأجهزة والبرامج .
2. لا توجد فروق ذات دلالة إحصائية بين نقاط الضعف الى ستغل لاختراق شبكات المعلومات وبين التدابير الوقائية المتخذة لمنع استغلال تلك النقاط.
3. لاتوجد علاقة ذات دلالة إحصائية بين الهياكل التنظيمية الإدارات تقنية المعلومات وبين توافق الوظائف المستخدمة في مجال حماية شبكات المعلومات.
4. لا توجد علاقة ذات دلالة إحصائية بين إجراءات حماية شبكات المعلومات وبين إتباعها والعمل بهما.
5. لا توجد فروق ذات دلالة إحصائية بين التدابير الاحتياطية اللازمة لتجنب المخاطر التي يمكن أن تؤثر سلبا على أمن شبكات المعلومات، وبين التدابير الفعلية المتخذة للتغلب على تلك المخاطر.

أهمية البحث

1. يؤمن هذا البحث مصدرا مهما للعاملين بمجال التحقيق في الجرائم المستحدثة حيث يستفاد منها بالتعرف على عناصر بناء نظم حماية الشبكات وتفاصيل تثبيتها ومخرجات أجهزتها .

2. يمكن ان تكون مرجعا مهما لإدارات التخطيط والجودة والموارد البشرية فهي تطرح حلولا للهيكل التنظيمي المناسب للأعمال الفنية المطلوبة في إطار الهيكل التنظيمي للمنظمة وتحاول التوصل إلى إجراءات مناسبة.
3. تقدم إجراءات تنظم عملية الحماية لجميع مكونات الشبكات ومواردها للمؤسسات محل الدراسة وتضبط عمليات إضافة أو إزالة مكونات الشبكة، و تنظم العلاقة بين الإدارات ذات الصلة في إطار الصلاحيات المعطاة لمنسوبي تلك الإدارات ويبين هذا البحث إجراءات أمن المعلومات المطبقة على الشبكات و مواردها مع توضيح مواطن الضعف ومواطن القوة فيها، وإيجاد التوصيات التي تفيد في تلافي نقاط الضعف وتحسين نقاط القوة بناء على نتائج التحليل
4. يقدم هذا البحث معلومات مفيدة جدا للراغبين في تصميم الشبكات ومراكز المعلومات أخذين بالاعتبار الاحتياطات الأمنية اللازمة لحماية شبكاقم مختصرين الجهد والمال والوقت.

أهداف البحث

1. حصر الأجهزة والبرامج المستخدمة لحماية الشبكات وطرق إعدادها وتحديثها.
2. تحديد نقاط الضعف في الشبكات المدروسة وتدابير تقويمها.
3. التعرف على مشكلات الهياكل التنظيمية في إدارات تقنية المعلومات، وعلاقتها بالوظائف الفنية والإدارية المطبقة في مجال الحماية، للوصول إلى إجراءات عمل مناسبة لتنفيذ سياسات الحماية.
4. تحديد سياسات الحماية وإجراءات العمل اللازمة لتحقيق حماية عالية لشبكات المعلومات الرئيسة.
5. حصر المخاطر التي يمكن أن تؤثر سلبا على أمن شبكات المعلومات وحصر التدابير الاحتياطية اللازمة لتجنب تلك المخاطر.

تعريف المصطلحات

1. الحاسب الآلي

يُعرف الحاسوب بأنّه آلة مُبرمجة بطريقة مُعيّنة ومُحدّدة تقوم بمُعالجة البيانات وتخزينها ومن ثم إخراجها، وقد ظهرت بوادر ظهور الحاسوب ما بين عامي 1943م و1946م عندما تم تصنيعه لمُساعدة الإنسان في حلّ المسائل والحسابات الطويلة والكبيرة ليُوفّر الوقت والجهد، وكانت بدايات الحاسوب مُميّزة جداً؛ حيث كان حجم جهاز الحاسوب الواحد يُقارب حجم الغرفة المنزليّة، أي أنّ حجمه ووزنه كبيران جدّاً.

يُمكن تعريف الحاسوب في الوقت الحالي بأنه مجموعة من الأسلاك والدوائر الكهربائيّة التي تمثل الهاردويرhardware ، ومجموعة التعليمات والأوامر والبيانات تُسمّى برمجياتSoftware ، ويوجد الكثير من أنواع الحاسوب المُستخدَمة في الوقت الحالي، مثل الحواسيب العملاقة، والحواسيب الشخصيّة، وحواسيب منطقة العمل الخاصة بتشغيل ألعاب الفيديو.[1]

2. الفايروسات

انَّ الفيروس الحاسوبي هو عبارة عن برنامج خبيث يصيب الأجهزة الحاسوبيّة ويغيّر طبيعة عملها دون إذن المُستخدِم أو علمه، ويتكاثر عن طريق نسخ نفسه إلى برنامج آخر أو حتّى إلى ملفّات البيانات إنَّ الهدف من زرع الفيروس في أجهزة الضحيّة يكون غالباً إمّا لإحداث ضرر في الجهاز، أو سرقة المعلومات منه، أو تعديل البيانات المُخزّنة عليه، أو إرسال بريد إلكتروني، أو إظهار رسائل معيّنة للمُستخدِم.[2]

1- Computer", Computer Hope, Retrieved 20-02-2017. Edited.

2- Margaret Rouse, "virus (computer virus)" , Retrieved 12-8-2017. Edited.

الفصل الثاني

نظم المعلومات و حماية الشبكات

الفصل الثاني
نظم المعلومات و حماية الشبكات

تمهيد

يحاول هذا البحث التعرف على طرق ووسائل حماية الحواسيب و الشبكات المستخدمة في المؤسسات التي تستخدم تقنية المعلومات والتعرف على إجراءات الأمان المستخدمة وأساليب إدارة أمن المعلومات تم تحليلها وبناء على النتائج المستخلصة من التحليل يضع الباحث توصيات تفيد تلك المؤسسات في تحسين جودة الحماية الشبكاتها وترقية إجراءات الأمان المطبقة عليها، وتقديم توصيات خاصة بإدارة الحماية للوصول إلى أفضل حماية بظروف وصول مرنة لا تسبب تأخير في تعاملات المستفيدين حيث يتناول الباحث في هذا الفصل نظم المعلومات وأهمية حماية الشبكات.

نظم المعلومات

تكتسب شبكات المعلومات أهميتها من المحتوى الإلكتروني الذي يكون متوفرا في موارد الشبكات مثل أجهزة الخادم (Servers) و مخازن البيانات (Data Storage5) وكذلك من أهمية البيانات المنسابة في خطوط الاتصال وعليه يرى الباحث ضرورة لاستعراض تظم المعلومات وبعض المفاهيم المتعلقة بانواع نظم المعلومات.

تقسم نظم المعلومات إلى نظم المعلومات التقليدية التي تشغل يدويا ونظم المعلومات المرتبطة بالحاسب الآلي والتي تعالج إلكترونية والمهم هنا تلك النظم المرتبطة بالحاسب الألي.

المكونات الأساسية لنظام المعلومات المرتبط بالحاسب الألي [1]

يمكن تحديد هذه المكونات بالأتي:

أ - المدخلات (Inputs): وهي بيانات يتم إدخالها بالنظام بغرض معالجتها.

---

(1) مدحت أبو النصر ، قواعد و مراحل البحث العلمي ،ط1 ، القاهرة ، مجموعة النيل العربية ، 2004م ،ص66-67 .

ب - المعالجة (Processing): وفيها يتم معالجة المدخلات وإنتاج معلومات ذات دلالة مفيدة باستخدام تقنية المعلومات، والتي من عناصرها أجهزة الحاسب الآلي (Hardwvare)، وبرمجيات الحاسب الآلي (software)، وقاعدة البيانات Database)، وإجراءات النظام (procedures)، والأفراد .

ت - المخرجات (outputs): هي النتائج المرجوة من نظام المعلومات في إطار معالجة المدخلات.

ث - التغذية العكسية (Feedback): هي عملية إرجاع نتيجة تقييم المعلومات التي تم الحصول عليها من المخرجات، لاستخدامها في المدخلات بعرض تحسين نوعية المدخلات التي تعطي مخرجات أفضل.

المهام المنفذة بوساطة نظم المعلومات المعالجة إلكترونيا :

تقسم نظم المعلومات المعالجة إلكترونية إلى أربعة أنواع رئيسة هي:

أ- نظم دعم القرارات (DSS)

ب- نظم المعلومات الإدارية (MIS)

ت-نظم المعلومات التشغيلية OIS

ث- نظم المكاتب الألية (A05)

ومن خلال معرفة المهام المنفذة بوساطة نظم المعلومات المرتبطة بالحاسب الألي بالمنشأة يتم معرفة العناصر التي تحتاج للحماية بما يتناسب مع قيمتها المادية أو المعنوية.[1]

أهداف الحماية الأمنية لشبكات الحاسب الآلي

إن الازدياد في اعتماد المؤسسات التجارية والمنشات الوطنية والمنظمات الدولية على تطبيقات شبكات الحاسب والإنترنت بالتوافق مع التطور في تقنيات نقل الصوت مع البيانات، زاد من أهمية بقاء أنقلعة المعلومات قيد التشغيل والعمل بصورة مستمرة (Availability) حيث أن توقفها يؤدي إلى خسائر كبيرة معنوية ومادية، ومهما اختلفت أحباب التوقف عن العمل فهي في النهاية نتيجة لضعف الحماية ضد ما يلي: سرقة المعلومات الخاصة والسرية، الخداع المالي ، الفيروسات

مدحت ابو النصر ، مصدر سابق ، ص70

سوء الاستخدام من قبل المستفيدين داخل الشبكة، التلف والتخريب ، الوصول غير المرخص من قبل القراصنة، سرقة الحواسب المحمولة، هجمات رفض الخدمة، اختراق الأنظمة من خارج المنظمة أو المنشأة وغيرها. ويوجد ثلاثة أهداف رئيسة لحماية الشبكات وهي الخصوصية والتكاملية والاستمرارية. [1]

1- الخصوصية (Confidentiality):

و تهتم بحماية البيانات من الكشف غير المرخص والمسؤول عن حماية خصوصية وسرية البيانات المنشأة التي تمتلك تلك البيانات وخاصة عندما تكون تلك البيانات خاصة بمستفيدين من خارج المنشأة، وعلى جميع العاملين بالمنظمة واجب الحفاظ على سرية بيانات منظمتهم ويعد هذا الواجب من المتطلبات القانونية. ومن المهم جدا عقد اتفاقيات حماية البيانات عند الاشتراك والتعاون في إنجاز الأعمال فيما بين المعلمات لحماية المعلومات المتبادلة وحماية معلومات كل منظمة من قبل الطرف الثاني ويدرج في تلك الاتفاقيات شرط ضرورة معالجة البيانات بطريقة أمنة تحميها من الكشف غير المرخص

2- السلامة (Integrity):

تشير إلى ضمان كمال وسلامة البيانات بالمحافظة عليها من التعديل أو التدريب أو التدمير والله بطريقة غير مرخصة، على سبيل المثال: تكون السلامة مؤمنة عندما تكون الرسالة المسلمة يطابق الرسالة المرسلة، ولا بد من إجراء القياسات اللازمة للتأكد من سلامة كل البيانات بغض النظر عن خصوصيتها أو درجة حريتها.

3- التوفر (Availability) :

تعرف على أنها التشغيل المتواصل لأنظمة الحاسب الآلي، تحتاج التطبيقات مستويات مختلفة للتوفر، تبعا لتأثر العمل (business) سلبا بفترة التوقف، وحتي يستمر تطبيق ما بالتوفر فيجب أن تكون جميع مكونات النظام متوفرة أيضا بحيث تتضمن التطبيق وقاعدة البيانات والخادم وأجهزة التخزين وسلامة الشيكة من البداية إلى النهاية. [2]

---

(1) See: Cisco systems, ic: Indian, Ciscope: Ci0 Letworking academy prograin, first year Coupation uide 2nd ed., 2001) P 32-33

(2) See: Cisco Systems, int: (Ladian, Ciscope, Cisco networking academy program, first year coupation guide 2nd ed., 2001) p12

التوازن في إجراءات الحماية والعناصر الضرورية لحماية الشبكات

1- التوازن بين مرونة الوصول وصلابة الحماية

إن الحماية الأمنية لشبكات المعلومات تصيح تحذية يحتاج كتير من الجهد والمال وخصوصا عند أخذ مخاطر تضرر الأعمال من التوقعات. ويقع على كاهل مهندسي الشبكات مسؤولية إدارة سياسات الأمان للحفاظ على التوازن بين الوصول المرن وصلابة الحماية الأمنية. وعلى مدراء الشبكات أخذ القضايا التالية بالاعتبار بالنسبة للوصول الشفاف (Transparent Acce55) :

أ- استمرارية الاتصال

ب-الأداء

ت-سهولة الاستخدام

ث-قابلية الإدارة

ج- التوفر

وعلى مسؤولي الشبكات أيضا أخذ القضايا التالية بالاعتبار بالنسبة للحماية الأمنية (Security)

أ- إثبات الشخصية

ب-التحويل

ت-المسؤولية

ث-الضمان

ج- الخصوصية

ح- سلامة البيانات

2- ومن العناصر الرئيسة لحماية الشبكة أمنيا[1]

الاستخدام الناجح لتقنيات الشبكات يتطلب حماية البيانات ومصادر المعلومات في الشبكات من التلف ومن الانتهاك والاحتراف، وتتضمن حلول حماية الشبكات خمسة حلول في التعريف بالهوية ، وحماية الحدود، وسرية البيانات، وإدارة الحماية، وإدارة السياسات.

---

(1) See: Cisco systems, inc: (Indiana, Cisco press, Cisco networking academy program first year COLpanion guide 2d ed 2013) p13

أ- التعريف بالهوية (Identity):

يشير مفهوم التعريف بالهوية إلى التعريف الإيجابي الدقيق بهوية مستخدمي الشبكة و تطبيقاتها ومضيفاتها وخدماتها ومصادرها، وتوجد تقنيات معيارية تمكن من تنفيذ تعريف الهوية تتضمن بروتوكولات التحويل مثل خدمة الوصول للمستخدم الداخل من بعيد ونظام التحكم بالوصول القطري المعدل و كيربيروس وأدوات كلمة المرور لمرة واحدة[1]

1. خدمة الوصول للمستخدم المتصل من بعيد (RADIUS) :

تسمح هذه الخدمة لعدد من الأجهزة بالتشارك في قاعدة بيانات التحقق من أصالة هوية المتصل. وتقدم نقطة مركزية لإدارة الوصول البعيد لكل شبكة. وعند ورود طلب من عميل (RADIUS) سيطلب منه اسم مستخدم وكلمة مرور ويتم تحويل هذه البيانات إلى خادم (RADIUS) فإذا كانت صحيحة يجيب الخادم بالموافقة ويسمح بوصول العميل إلى الشبكة، وإن لم تكن صحيحة يجيب الخادم بالرفض وبناء عليه يتم إهمال طلب الوصول. استخدمت هذه الخدمة في بداية الأمر للاتصال البعيد عن طريق المودم وجدران الحماية ومن مساوئها أنها لا توفر خاصية التشفير ولذلك لابد عند اللزوم من توفير خاصية التشفير عن طريق خدمات إضافية.[2]

2. نظام التحكم بالوصول الطرفي المعدل (+TACACS):

تقدم خدمة (+TACACS طريقة بديلة عن خدمة (RADIUS) كأسلوب للوصول المركزي، كما في (RADIUS) فإن هذه الخدمة تجلب تصاريح الوصول من جدران الحماية إلى أجهزة الخادم الأخرى. وهي أيضا طريقة تحقق تستخدم أسماء المستفيدين و كلمات المرور، وبالمقابل فإن (+TACACS تتوافق فقط مع بعض جدران الحماية بالمقارنة مع خدمة (RADIUS الأكثر استخداما [3]

---

(1) OTp: One-Time Password .

(2) See : Chris Brenton , Cameron Hurt Network Security (Manian village Alameda : Sybex 2003) p231.

(3) See : Chris Brenton , Cameron Hurt Network Security (Manian village Alameda : Sybex 2003) p148.

3. كيربيروس (Kerberos):

أتى أصل تسمية كيربيروس من الأساطير اليونانية التي تروي أن كلا ثلاثي الرؤوس بجرس بوابة منوى الأموات الكائن تحت الأرض ويعرف غير ذلك بالحفرة.[1] وفي مجال حماية الشبكات هو حل للتحقق من صحة الهوية وقد تم التقدم تسجيل الدخول من خلال نقطة واحدة إلى بيئة متنوعة. تسمح هذه الخدمة بتحقق متبادل من الصحة مع إمكانية التشفير بين المستخدمين والخدمات. وتعتمد على كل مستخدم لتذكر اسم المستخدم الخاص به مع المحافظة على كلمة مرور فريدة. عندما يتم التحقق من صحة هوية مستخدم في نظام التشغيل المحلي يقوم عميل محلي بإرسال طلب تحقق إلى خادم (Kerbero5)، يقوم الأخير بالاستجابة بإرسال التبوتيات اللازمة مشفرة للمستخدم المعي، والعميل المحلي يحاول فك تشفير التبوتيات مستخدما كلمة المرور التي يمليها المستخدم، إذا كانت كلمة المرور صحيحة يكون المستخدم شرعيا ويعطى بطاقة تصريح بالوصول تسمح بتشفير بيانات جميع جلسات الاتصال. وحالما يتم اعتماد شرعية المستخدم فلا تطلب منه التحقق من الصحة عند محاولة وصوله لخدمات أخرى بالشبكة لأن البطاقة الصادرة بوساطة خادم (Kerberos) تقدم الثبوتيات اللازمة لدخول المستخدم إلى موارد إضافية بالشبكة. ومن أهم الدوافع لاستخدام هذه الخدمة أنفا مجانية ويمكن تنزيل شفرة المصدر مجانا واستخدامها. [2]

ب - حماية حدود الشبكة (Perimeter Security)

تقدم حماية الحدود الوسائل اللازمة لضبط الوصول للتطبيقات الحرجة في الشبكة والبيانات والخدمات للسماح فقط للمستفيدين الشرعيين بتمرير المعلومات عبر

---

(1) See : Chris Brenton , Cameron Hurt Network Security (Manian village Alameda : Sybex 2003) p230.

(2) UTM : Abbreviation of Unified Threat Management

مكونات الشبكة، فيتم إعداد الموجهات والموزعات للقيام بتصفية الحزم وتثبيت جدران الحماية المتخصصة متعددة الوظائف بالإضافة البرامج الحماية من البرامج الضارة والفيروسات والبريد الدعائي وتثبيت برامج إدارة الشبكة ومراقبة حركة حزم البيانات عند منافذ حدود الشبكة.

ت -خصوصية البيانات (Data Privacy) :

عندما تفرض ضرورة العمل حماية البيانات من التسريب يصيح التحقق من هوية المستخدم قضية حرجة ويتوجب على مسؤولي أمن الشبكات أن يفعلوا خصائص التحقق من الهوية المتوفرة في أجهزة الاتصال الشبكية، ويمكن تفعيل خصائص التحقق من الهوية باستخدام تقنية الأنفاق (Tunneling) كتقنية التغليف العام (GRE)[1] أو برتوكول أنفاق الطبقة الثانية (L2TP)[2] التي تساعد على حماية خصوصية البيانات. وإلى جانب التحقق من الصحة تستخدم تقنيات التشفير الرقمية كالحماية اعتمادا على عنوان بروتوكول الإنترنت مثال ذلك (IPSec) وخصوصا عند استخدام الشبكات الافتراضية الخاصة (VPN).

ث - إدارة الحماية الأمنية (Secunty Management) :

من المهم جدا تفقد حالة تدابير الحماية بالمراقبة الدورية للتأكد من بقاء الشبكة محمية بكل فعال، حيث نستعليع ماسحات مواطن الضعف تحديد النقاط الواجب مراعاة تدابير الوقاية لتعزيز الحماية وتستطيع أنظلمة كشف و منع التلصص القيام بالمراقبة وتنفيذ ردود الأفعال المناسبة للحوادث المخالفة للقواعد المحددة في ملف الإعداد. وبذلك يمكن أن تحصل المنظمة على مشهد له معين مفيد لكل من سيل البيانات و حالة حماية الشبكة.

---

(1) GRE: Abbreviation of Generic Routing Encapsulation

(2) L2TP: Abbreviation of Layer 2 Tunneling Protocol

ج - إدارة السياسات (Policy Management) [1]

السياسة الأمنية تذهب بعيدا عن فكرة إبقاء الأشخاص السيئين خارجاً لتصبح وثيقة معقدة تعين بضبط الوصول للبيانات وتصفح الانترنت واستخدام كلمات المرور والتشفير وملحقات البريد الالكتروني وغيرها. تصنف هذه القواعد حسب مجموعات أو أفراد في المنظمة. يجب أن تبقي المستخدمين الماكرين خارجا ولا تأل جهدا في مراقبة وضبط الأشخاص المحتمل أن يكونوا خطرين ضمن المنظمة، والخطوة الأولى لإنشاء السياسة هي إدراك البيانات والخدمات القيمة (ولأي مستخدمين) ، ما احتمالات التعطل وهل يوجد أية حمايات متوفرة مسبقا لمنع إساءة الاستخدام ، يجب أن تملي السياسة الأمنية سماحية الوصول بشكل هرمي بحيث تسمح للمستخدمين بالوصول للموارد الضرورية لإنجاز أعمالهم. و كبداية جيدة يمكن خلال كتابة وثيقة الأمن باستخدام نماذج من موقع معهد المعايير والتكنولوجية الدولي وغيرهما. ويمكن أن تكون السياسات على شكل تعليمات يتم إعدادها على أجهزة شيكية مخصصة لحماية الشبكة بازدياد نمو الشيكات من حيث الحجم والتعقيد، يزداد الاحتياج لأدوات إدارة سياسات مركزية أدوات معقدة يمكنها القيام بتحليل وتفسير وإعداد ومراقبة خصائص الحماية الضرورية. يمكن للأدوات المعتمدة على واجهة متصفح الويب أن سهل الاستخدام وتزيد من فعالية حلول حماية الشبكات.[2]

التوعية بالحماية الأمنية

عادة لا يهتم المستخدم بعينيات الحماية مما يتسبب بنتائج غير مرغوبة حيث تكون شبكات الحاسب الآلي بالنسبة له أداة تساعده لإنجاز متطلبات عمله الوظيفية وحسب

---

(1) See: Cisco systems, Inc. (Indians, Cisco press, Cisco networking academy program, first year coupanion guide 2nd ed., 2001) P 14

(2) https://ar.wikipedia.org/wiki/%D8%A7%D9%84%D8%B9%D8%B1%D8%A7%D9%82

بل علاوة على ذلك غالبا ما يعد إجراءات الحماية الأمنية ضرية من الإزعاج أكثر منه مساعدة ووقاية. ولا بد من إلزام كل منظمة بتقديم التدريب المناسب لموظفيها التعليمهم ما يلزم حول أساسيات الحماية والكثير من المشكلات ذات الصلة بحماية المعلومات. ويجب أن يعتمد ذلك التدريب على سياسة الحماية الأمنية المتبعة في المنظمة. ويجب أن يشمل التدريب كلا من الأفراد العاملين في تصميم أنظمة الشبكات و تركيبها وسيانها. وتتضمن مناهج هذا التدريب المعلومات المتعلقة بالحماية وتقنيات الضبط الداخلية الي يمكن أن تتكامل مع تطوير أجهزة الشبكة و أنظمة تشغيلها وأساليب صيانتها.[1]

ولابد من تدريب الأفراد المسؤولين عن أمن الشبكات تدريبا متعمقا في المسائل التالية:

أ- تقنيات الحماية.

ب-منهجيات تقييم مواطن الضعف والتهديدات الأمنية.

ت-اختيار المعايير والتخطيط للتنفيذ الضوابط الأمنية.

ث-المخاطر الممكنة فيما لو لم يتم اتخاذ تدابير الحماية الأمنية المناسبة.

في المنظمات الكبيرة التي غالبا ما تكون منتشرة على مناطق جغرافية مختلفة تكون شبكة الحاسب كبيرة وتتكون من مجموعة من الشبكات المحلية (LANs) وعند ذلك يكون من الأفضل توظيف مدير شبكة محلية (LAN Administrator) لكل شبكة محلية (LAN) تربط بالعمود الفقري لشبكة المنظمة ويكون هؤلاء المدراء للشبكات المحلية نقطة المركز لإتاحة ونشر المعلومات المتعلقة بنشاطات المنظمة في كل شبكة محلية.

---

(1) See: Cisco systems, Inc: (Indians, Cisco press, Cisco networking academy program, first year COLEpanion guide 2nd ed., 2004)P4

ولا بد من وجود قواعد التنفيذ سياسات الحماية الأمنية قبل القيام بتوصيل الشبكة المحلية إلى العمود الفقري لشبكة المنظمة، ومن تلك القواعد :

أ. توفير سياسية للحماية الأمنية موحدة وموثقة بشكل جيد.

ب. توفير ضوابط تنزيل البرامج

ت. توفير التدريب الكافي للمستخدمين.

ث. توفير خطة طوارئ الاستعادة عند الكوارث وتكون موثقة توثيقا جيدا.

ويكون التدريب ضروريا أيضا للأفراد المسؤولين عن توزيع كلمات المرور فعلى هؤلاء الأفراد التأكد من تقديم المستفيد الذي يطلب كلمة مرور عند النسيان إثباتات كافية قبل إعادة تهيئة كلمة مرور جديدة.

التهديدات ومواطن الضعف في الشبكات

1. التهديدات والثغرات الأمنية (Security Threats and Vulnerabilities)

يوجد ثلاثة مواطن ضعف أساسية تزيد من التهديدات الأمنية هي:

أ- نقاط ضعف تكنولوجية

ب-نقاط ضعف الإعدادات

ت-نقاط الضعف في سياسات الحماية

وتعد نقاط الضعف الثلاث مصدرا مهما لأناس يبحثون عنها ويتلهفون للوصول إليها لاستغلالها بانتهاك خصوصية الشبكات والتلذذ بشوة الانتصار باختراق الإجراءات الدفاعية لشبكات ضحاياهم .[1]

---

(1) See: Cisco systems, Inc: (Indians, Cisco press, Cisco networking academy program, first year coinpanion guide 2nd ed., 2001) p 15.

٢. مواطن الضعف في حماية الشبكة (Network Secunty Weaknesses)

حتى يتم إكمال الاتصال من خلال الشبكة، يجب تمكين خدمات محددة وتشغيلها، وتتكون الشبكة النموذجية من بروتوكولات ونظم تشغيل مكتبية وأجهزة شبكية تستخدم لتمرير البيانات عبر الشبكة. و كل من مكونات الشبكة تحوي مواطن ضعيفة قابلة للاستغلال. ويمكن ذكر مواطن الضعف المشهورة التالية:

أ- نقاط ضعف بروتوكول TCP / IP وتشمل (HTTP) و (ICMP) و(SNMP) و (Dos).

ب-نقاط ضعف نظم التشغيل وتشمل (UNIX) و (Ms-Windows) و (OS/2).

ت- نقاط ضعف عتاد الشبكة وتشمل حماية كلمات المرور وعدم وجود خصائص التحقق من الصحة وبروتوكولات التوجيه والإعداد السيئ لبروتوكولات التوجيه.

٣. التهديدات الرئيسة للشبكات (Primary Network Threats)[1]

يمكن حصر تمديدات الشبكات في مجموعة من العناوين الكبيرة كالتالي:

أ- تهديدات غير منظمة: تتضمن بشكل رئيس أفراد غير متوقعين يستخدمون أدوات قرصنة سهلة تتوفر على شبكة الانترنت في مواقع كثيرة كأدوات كسر كلمات المرور والنصوص المغلفة .

مع أن التهديدات غير المنظمة يمكن أن أحصل عند تشغيل أدوات القرصنة السهلة فإنها تظل مصدر خطر يمكن أن يؤدي الشبكة المعتدى عليها بأضرار خطيرة تزيد بازدياد مهارة هؤلاء الأفراد وقوة الأدوات

---

(1) See: Cisco systems, Inc: (Indians, Cisco press, Cisco networking academy program, first year coinpanion guide 2nd ed., 2001) p 20.

المستخدمة، فعند اختراق موقع منظمة ما على الانترنت يكون ركن السلامة أحد أركان الحماية الأمنية غير محققا و حتى لو كان الموقع المخترق محميا من الشبكات الخارجية بجدار حماية فعال فإن مصداقية المنظمة تنخفض لدى الأطراف الأخرى ويعدون ذلك الموقع بيئة غير أمنة وبالتالي تتأثر أعمال المنظمة سلبا، ويكون الأثر أكثر سلبية إذا كان الموقع خاص بجهات وطنية دفاعية متصلة بقواعد بيانات عسكرية أو أمنية.

ب- تهديدات منظمة: تأتي من قراصنة مندفعين بشدة يحفزهم التنافس التنفي، يعرفون ثغرات نظم التشغيل ويمكنهم فهم النصوص البرمجية والشفرات واستغلالها. و يفهمون ويطورون ويستخدمون تقنيات القرصنة المعقدة في اختراق مواقع الشركات والمؤسسات غير المحمية عن جهل وقلة خبرة. هذه المجموعة من القراصنة غالبا ما تكون متورطة في معظم قضايا الاحتيال والسرقة التي يتم إخبار الجهات الأمنية عنها.

ت-تهديدات خارجية هي تلك التهديدات التي يسببها أفراد أو منظمات يعملون من خارج المنظمة ولا يملكون حق الوصول إلى شبكة الحاسب العائدة لتلك المنظمة. تؤدي هذه المجموعة من الأفراد أو المنظمات العمل عن طريق دخولها الشبكات بشكل رئيس من الإنترنت أو خطوط الهاتف من خلال خدمة الطلب الهاتفي .

ث- تهديدات داخلية: يمكن حصول هذا النوع من التهديدات عندما يكون لشخص ما حق الوصول لشبكة المنظمة سواء حساب مسجل مسبقا (اسم مستخدم وكلمة مرور) أو بالدخول الفيزيائي الأماكن وجود أجهزة ومعدات الشبكة.

الفصل الثالث

البرامج الخبيثة

(انواعها و اضرارها)

الفصل الثالث

البرامج الخبيثة (أنواعها و أضرارها)

إنَّ البرنامج الخبيث (Malware) هو أي برنامج يؤدّي إلى إحداث ضرر معيَّن لمستخدم الحاسوب، ويندرج تحته الفيروسات والتي تُعد أشهر أنواع البرامج الخبيثة، بالإضافة لدودة الحاسوب وأحصنة طروادة وبرامج التجسُّس وبرامج الفدية والتي تصيب أجهزة الحاسوب وتقوم بتشفير جميع البيانات الموجودة عليه، وغير ذلك من البرامج المضرّة.

يهدف مطوِّرو البرامج الخبيثة إلى نشر برامجهم عبر الأجهزة والشبكات بجميع الوسائل المتاحة، فيمكن أن ينتقل البرنامج من خلال شبكة الإنترنت عن طريق تحميلها إلى جهاز المستخدم دون علمه أو إذنه، أو عن طريق زيارة المستخدم لمواقع إلكترونيّة زائفة، أو فتحه لرسائل بريد إلكتروني تحتوي على فيروسات، كما يمكن أن تنتقل هذه البرامج إلى النظام من خلال الذاكرات الوميضيّة USB : بالإضافة لوسائل أخرى عديدة.[1]

الفيروس

فيروس الحاسوب هو عبارة عن برنامج خبيث يتكاثر في الجهاز المستهدف عن طريق نسخ نفسه في برامج أخرى، أو في قطاع الإقلاع أو حتّى في ملفّات وثائقيّة، وذلك يتم دون علم مستخدم الحاسوب أو إذنه؛ حيث يقوم شخص ببدء نشر الفيروس على الجهاز، وقد يكون هذا الشخص جاهلاً بالأمر بحيث ينشر الفيروس دون دراية. قد ينتشر الفيروس بعدّة طرق، فيمكن ذلك من خلال فتح المستخدم لرسالة

---

(1) Margaret Rouse, "malware (malicious software)" ،TechTarget, Retrieved 26-8-2017. Edited

بريد إلكتروني تحتوي على فيروسات، أو تشغيل برنامج معيّن، أو زيارة موقع ما، أو حتّى من خلال معدّات التخزين المتنقّلة كالذاكرة الوميضيّة، أو غير ذلك.

يقوم الفيروس بتغيير آلية عمل الحاسوب، فتأثيره على الجهاز المصاب قد يكون بحذف أو تشفير البيانات والملفّات الموجودة على الجهاز، أو نسخها، أو التأثير على برامج أخرى، أو التعديل على برامج النظام أو تعطيلها عن العمل .إنَّ العديد من الفيروسات تتميَّز بكونها قادرة على تفادي البرامج المضادّة للفيروسات فيكون من الصعب كشفها .

أنواع الفيروسات

1. توجد العديد من أنواع الفيروسات تختلف من حيث تأثيرها على الجهاز المصاب، ومنها ما يلي[1]
2. الفيروسات التي تصيب الملفّات؛ فهذا النوع يربط نفسه بالبرامج، وعادةً التي تحمل امتداد ".EXE" أو ".COM"
3. الفيروسات المتحوّلة Polymorphic viruses : فهذا النوع من الفيروسات له القدرة على تغيير الكود الخاص به دون تغيير آليّة عمله؛ وذلك لتفادي كشفه من قبل البرمجيّات المضادّة للفيروس، خصوصاً تلك التي تعتمد على كشف الفيروسات بواسطة تحليل البصمة .
4. الفيروسات المُقيمة Resident viruses : وهي التي تُخزِّن وتُخفي نفسها في ذاكرة الوصول العشوائي للنظام، فيستطيع الفيروس أن يُصيب الملفّات والبرامج الأخرى الجديدة حتّى وإن تمَّ حذف الملف الأصلي للفيروس. عادةً ما يبدأ هذا النوع من الفيروسات بالعمل عند تفعيل نظام التشغيل لبرنامج ما أو بدء عمل مُعيَّن.

---

(1) Margaret Rouse, "virus (computer virus)" ،TechTarget, Retrieved 26-8-2017. Edited.

5. فيروسات الروتكيت Rootkit viruses : وتقوم بتنصيب روتكيت وهي برامج تسمح بتنفيذ وتفعيل أوامر إداريّة في الحاسوب على الجهاز المُستهدف، فتستطيع تعديل أو تعطيل برامج النظام أو وظائفه. هذا النوع من الفيروسات قادر على تفادي معظم البرامج المضادّة للفيروس خصوصاً تلك التي تفتقر لعمل مسح على برامج الروتكيت الموجودة على الجهاز.
6. الفيروسات التي تصيب قطاع الإقلاع فهذا النوع من الفيروسات يقوم بتنصيب نفسه في أماكن معيّنة على القرص الصلب أو الذاكرة الوميضيّة بحيث تبدأ بالعمل فور تفعيل هذه الأجهزة .

و هناك نوعان رئيسيان للفيروسات و هما :

1. فيروسات الـ Software : و هي الفيروسات المختصة في ضرب و تعطيل المكونات البرمجية للحاسوب و تسمى ايظا الفيروسات البرمجية .
2. فيروسات الـ Hardware : و هي الفيروسات المختصة في ضرب و تعطيل المكونات المادية للحاسوب .

من أخطر الفيروسات على الحاسوب [6]

فيروس تشيرنوبيل

فيروس تشيرنوبيل CIH Virus : هو فيروس تمَّ انتشاره عام 1998م، وكان يقوم بعمل تخريبي في كل عام تمرّ ذكرى انفجار المفاعل النووي في روسيا؛ حيث كان يمسح جميع البيانات الموجودة على القرص الصلب، بالإضافة لتعديل البرنامج المخصَّص بتشغيل الجهاز، والموجود على شريحة مثبّتة فوق اللوحة الأمّ وذلك يؤدّي إلى منع الحاسوب من العمل إلى حين استبدال اللوحة الأم.

---

(1) Lauren Sporck (26-5-2017), "Update: Most Destructive Malware of All Time" ، OPSWAT, Retrieved 26-8-2017. Edited

دودة ميليسا

انتشرت دودة ميليسا Melissa Worm :عام 1999م، وقد أدّت إلى خسائر تُقدَّر بملايين الدولارات. تمَّ نشر الفيروس بواسطة البريد الإلكتروني وذلك من خلال رسالة بريد إلكتروني مزيّفة تقوم بإرسال نفسها إلى 50 بريد إلكتروني آخر عند فتحها.

دودة ستكسنت

انتُشرت دودة ستكسنت Stuxnet Worm :في عام 2010م، وقد كانت تنتشر عبر أجهزة اليو إس بي USB drives :عند وصلها بجهاز الحاسوب، ولم يكن يتطلَّب وجود اتصال بشبكة الإنترنت ليتمكَّن من الانتشار .أصاب الفيروس محطّات توليد الطاقة النووية بالإضافة لمحطّات تخصيب اليورانيوم في إيران.

برنامج فدية واناكراي

انتُشِر فيروس فدية واناكراي WannaCry Ransomware :في عام 2017م، وقد أصاب أكثر من 100000 مُنظّمة في أكثر من 150 دولة، من ضمنها شركات كُبرى بالإضافة للدوائر الحكوميّة. كان الفيروس ينتشر بواسطة البريد الإلكتروني، ويستغلّ ثغرة موجودة في أنظمة تشغيل الويندوز وقد أصاب الفيروس 16 مستشفى في المملكة المتّحدة.

أضرار الفيروسات و تاثيرها على الحاسوب[1]

1- إبطاء عمل جهاز الحاسوب، وحدوث أخطاء مجهولة عند تشغيل البرامج وتنفيذ أوامرها.

---

(1) Stallings, William (2012). Computer security : principles and practice. Boston: Pearson. p. 182

2- توسيع حجم الملفات وزيادتها، وكما يزيد من المدة التي يتم بها تحميل البرامج والملفات إلى ذاكرة جهاز الحاسوب.
3- ملاحظة وجود تأثير غير مسبوق ورسائل على الشاشة.
4- ظهور رسالة FATALI/o ERROR عند بدء قراءة الأقراص وزيادة المدة الزمنيّة في قراءتها في حال كانت محميّة.
5- ملاحظة المستخدم صدور نغمات موسيقية غير مألوفة له. إحداث تغييرات في تواريخ تسجيل الملفات.
6- اختلال عمل لوحة المفاتيح.
7- تراجع المساحة المتوفرة في ذاكرة الجهاز، نظراً لما يشغله الفيروس من مساحة كبيرة.
8- إظهار رسائل تكشف عن عدم وجود ذاكرة كافية لتحميل البرامج والملفات.
9- عدم صلاحيّة بعض المساحات للتخزين في القرص الصلب.
10- إلحاق الضرر بالنظام من خلال تعطيل BOOT Sector.
11- تعرض البيانات والملفات للإتلاف.

البرنامج المضاد للفيروس

برنامج مضاد الفيروسات: هو برنامج له القدرة على كشف ومنع وتعطيل البرامج الخبيثة التي قد تصيب أجهزة الحاسوب[1]

---

(1) Margaret Rouse, "antivirus software" ،TechTarget, Retrieved 26-8-2017. Edited.

التجسس

التجسس بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف وبطبيعة الحال هي سمة سيئة يتسم بها المخترق لقدرته على دخول أجهزة الأخرين عنوه ودون رغبة منهم وحتى دون علم منهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها سواء بأجهزتهم الشخصية او بنفسياتهم عند سحبة ملفات وصور تخصهم وحدهم [1].

برامج التجسُّس

يتم تنصيب برامج التجسُّس على الجهاز الهدف بغرض التجسُّس عليه وانتهاك خصوصيّته واستغلالها. قد يتم استخدام هذه البرامج لأغراض غير مضرّة بالمستخدم، كتنصيب الأهل لها على أجهزة أبنائهم لكشف أنشطتهم على شبكة الإنترنت، أو من قِبَل الشركات على أجهزة الموظّفين للتأكُّد من المواقع التي يتصفّحونها خلال العمل، وغير ذلك.[2]

أسباب التجسس و دوافعه

لم تنتشر هذه الظاهرة لمجرد العبث وإن كان العبث وقضاء وقت الفراغ من أبرز العوامل التي ساهمت في تطورها وبروزها الي عالم الوجود . و من ابرز الدوافع الرئيسية للتجسس اوجزها هنا على النحو التالي[3]

- الدافع السياسي والعسكري ممالاشك فيه أن التطور العلمي والتقني أديا الي الأعتماد بشكل شبة كامل على أنظمة الكمبيوتر في أغلب الاحتياجات التقنية والمعلوماتية. فمنذ الحرب البارردة والصراع المعلوماتي والتجسسي بين

---

(1) http://rap-syr.mam9.com/t23-topic

(2) Margaret Rouse, "spyware" ،TechTarget, Retrieved 26-8-2017. Edited.

(3) مروة الاسدي ، سباق التجسس الالكتروني و زعزعة النظام العالمي ، مقال (شبكة النبأ المعلوماتية) ، 20 كانون الاول 2017 .

الدولتين العظميين على أشده. ومع بروز مناطق جديده للصراع في العالم وتغير الطبيعة المعلوماتيه للأنظمة والدول ، اصبح الأعتماد كليا على الحاسب الألي وعن طريقة اصبح التجسس من اجل الحصول على معلومات سياسية وعسكرية واقتصادية مسالة أكثر أهمية.

- الدافع التجاري من المعروف أن الشركات التجارية الكبرى تعيش هي ايضا فيما بينها حربا مستعرة وقد بينت الدراسات الحديثة أن عددا من كبريات الشركات التجارية يجرى عليها أكثر من خمسين محاولة تجسس لشبكاتها كل يوم.
- الدافع الفردي بداءت اولى محاولات التجسس الفردية بين طلاب الجامعات بالولايات المتحدة كنوع من التباهي بالنجاح في تجسس اجهزة شخصية لأصدقائهم ومعارفهم ومالبثت أن تحولت تلك الظاهرة الي تحدي فيما بينهم في تجسس الأنظمة بالشركات ثم بمواقع الأنترنت. ولايقتصر الدافع على الأفراد فقط بل توجد مجموعات ونقابات اشبة ماتكون بالأنديه وليست بذات أهداف تجارية. بعض الأفراد بشركات كبرى بالولايات المتحدة ممن كانوا يعملون مبرمجين ومحللي نظم تم تسريحهم من اعمالهم للفائض الزائد بالعمالة فصبوا جم غضبهم على انظمة شركاتهم السابقة مفتحمينها ومخربين لكل ماتقع ايديهم علية من معلومات حساسة بقصد الأنتقام . وفي المقابل هناك هاكرز محترفين تم القبض عليه بالولايات المتحدة وبعد التفاوض معهم تم تعيينهم بوكالة المخابرات الأمريكية الس أي اي وبمكتب التحقيقات الفيدرالي الأف بي أي وتركزت معظم مهماتهم في مطاردة الهاكرز وتحديد مواقعهم لأرشاد الشرطة اليهم

أنواع التجسس

يمكن تقسيم التجسس من حيث الطريقة المستخدمة الي ثلاثة أقسام[1]

1. تجسس المزودات او الأجهزة الرئيسية للشركات والمؤسسات او الجهات الحكومية وذلك بتجسس الجدران النارية التي عادة توضع لحمايتها وغالبا مايتم ذلك باستخدام المحاكاة Spoofing وهو مصطلح يطلق على عملية إنتحال شخصية للدخول الي النظام حيث أن حزم الـ IP تحتوي على عناوين للمرسل والمرسل اليه وهذة العناوين ينظر اليها على أنها عناوين مقبولة وسارية المفعول من قبل البرامج وأجهزة الشبكة . ومن خلال طريقة تعرف بمسارات المصدر Source Routing فإن حزم الـ IP قد تم اعطائها شكلا تبدو معه وكأنها قادمة من كمبيوتر معين بينما هي في حقيقة الأمر ليست قادمة منه وعلى ذلك فإن النظام إذا وثق بهوية عنوان مصدر الحزمة فإنه يكون بذلك قد حوكي (خدع) وهذة الطريقة هي ذاتها التي نجح بها مخترقي الهوت ميل في الولوج الي معلومات النظام قبل شهرين.
2. تجسس الأجهزة الشخصية والعبث بما تحوية من معلومات وهي طريقة للأسف شائعة لسذاجة اصحاب الأجهزة الشخصية من جانب ولسهولة تعلم برامج التجسسات وتعددها من جانب اخر.
3. التعرض للبيانات اثناء انتقالها والتعرف على شيفرتها إن كانت مشفرة وهذة الطريقة تستخدم في كشف ارقام بطاقات الأئتمان وكشف الأرقام السرية للبطاقات البنكيه ATM وفي هذا السياق نحذر هنا من امرين لايتم الأهتمام بهما بشكل جدي وهما عدم كشف ارقام بطاقات الأئتمان لمواقع التجارة الألكترونية إلا بعد التأكد بألتزام تلك المواقع بمبداء الأمان . أما الأمر الثاني فبقدر ماهو ذو أهمية أمنية عالية إلا أنه لايؤخذ مأخذ الجديه . فالبعض

---

(1) http://redirect.viglink.com

4. عندما يستخدم بطاقة السحب الألي من مكائن البنوك النقدية ATM لاينتظر خروج السند الصغير المرفق بعملية السحب او انه يلقي به في اقرب سلة للمهملات دون ان يكلف نفسه عناء تمزيقة جيدا . ولو نظرنا الي ذلك المستند سنجد ارقاما تتكون من عدة خانات طويله هي بالنسبة لنا ليست بذات أهمية ولكننا لو أدركنا بأن تلك الأرقام ماهي في حقيقة الأمر الا إنعكاس للشريط الممغنط الظاهر بالجهة الخلفية لبطاقة الـ ATM وهذا الشريط هو حلقة الوصل بيننا وبين رصيدنا بالبنك الذي من خلالة تتم عملية السحب النقدي لأدركنا اهمية التخلص من المستند الصغير بطريقة مضمونه ونقصد بالضمان هنا عدم تركها لهاكر محترف يمكنه استخراج رقم الحساب البنكي بل والتعرف على الأرقام السرية للبطاقة البنكية ATM .

طرق الحماية من التجسس

للحماية من الاختراقات والتجسس هناك عدة طرق تستخدمها برامج الحماية لأداء مهامها ويمكن تصنيف هذه الطرق الي اربعة على النحو التالي: [1]

1- تخزين قاعدة بيانات بالبرنامج تخزن فيه عدد كبير من اسماء احصنه طرواده ويتم عمل مسح لكافة الملفات الموجودة بجهاز المستخدم ومطابقتها مع الموجود بقاعدة البيانات تلك للتعرف على الملفات المطابقه . يتم تحديث قاعدة البيانات دوريا اما من خلال الاقراص اللينه التي تحدث اولا بأول كما كانت تفعل سابقا شركة مكافي ببرنامجها الشهير انتي فيروس او يتم ذلك مباشرة من خلال الانترنت كما يفعلا نورتون ومكافي في الوقت الحالي .

2- البحث عن وجود تسلسل محدد من الرموز التي تميز كل ملف تجسسي

(1) How to Keep a Smartphone From Being Hacked", www.techlife.samsung.com, Retrieved 15-1-2018. Edited.

والتي تميز احصنه طروادة وغيرها وهذا الملف يعرف تقنيا بأسم Signature وايضا هذة الطريقة تحدث دوريا كما تم شرحه اعلاه .

3- الكشف عن التغيرات التي تطرأ على ملف التسجيل Registry وتوضيح ذلك للمستخدم لمعرفة ان كان التغيير حصل من برنامج معروف او من حصان طرواده.

4- مراقبة منافذ الاتصالات بالجهاز (اكثر من 65000 منفذ) لأكتشاف اي محاولة غير مسموح بها للأتصال بالجهاز المستهدف وقطع الاتـصال تلقائيا واعطاء تنبيه بذلك في حالة وجود محاولة للأختراق .

الاستنتاجات

و

التوصيات

الاستنتاجات

من خلال اتمام هذا البحث استنتج الباحث ان الفيروسات عبارة عن برامج يتم صنعها و برمجتها حيث يقوم من أنشأ الفيروس ببرمجة الفيروس و توجيه الأوامر له حيث يقوم بتحديد الزمان و متى و كيف يبدأ الفيروس بالنشاط وعادة ما تعطى فرصة كافية من الوقت للفيروس حتى يضمن حرية الإنتشار دون أن يلفت الإنتباه ليتمكن من إصابة أكبر عدد ممكن من المستخدمين ، و تختلف الفيروسات من حيث بدأ النشاط فهنالك من يبدأ بتاريخ أو وقت محدد و هنالك من يبدأ بالعمل بعد تنفيذ أمر معين في البرنامج المصاب وهناك 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 انشاء ذلك الفيروس فهنالك من يقوم بعرض رسالة تستخف بالمستخدم أو تقوم بعرض رسالة تحذيرية عن امتلاء الذاكرة وهناك انواع اخرى تقوم بحذف أو تعديل بعض الملفات وهناك من يقوم بتكرار ونسخ نفسه حتى يشل جهازك تماما و هناك انواع اشد فتكا فتقوم بمسح كل المعلومات من القرص الصلب .

التوصيات

1. لكي احمي النظام الخاص بالحاسوب يجب توفر عدة شروط منها:
2. وضع كلمة سر او الرمز أو الرقم الشخصي
3. برامج مكافحة الفيروسات
4. مراعاة الإجراءات الأمنية لحماية الدخول إلى الشبكة
5. حماية مواقع التجارة الإلكترونية
6. إعتماد بصمة الأصبع او العين أو الصوت
7. تحديد نطاق الاستخدام Authorization
8. إجراء النسخ الإحتياطيBackup

المصادر

المصادر

- **المصادر العربية**

1. مدحت أبو النصر ، قواعد و مراحل البحث العلمي ،ط1 ، القاهرة ، مجموعة النيل العربية ، 2004م
2. مروة الاسدي ، سباق التجسس الالكتروني و زعزعة النظام العالمي ، مقال (شبكة النبأ المعلوماتية) ، 20 كانون الاول 2017 .

- **المصادر الاجنبية**

1. Chris Brenton , Cameron Hurt Network Security (Manian village Alameda : Sybex 2003)
2. Cisco systems, inc: (Indiana, Cisco press, Cisco networking academy program first year COLpanion guide 2d ed 2013)
3. Cisco systems, Inc: (Indians, Cisco press, Cisco networking academy program, first year coinpanion guide 2nd ed., 2001)
4. Cisco Systems, int: (Ladian, Ciscope, Cisco networking academy program, first year coupation guide 2nd ed., 2001)
5. Computer", Computer Hope, Retrieved 20-02-2017. Edited.
6. GRE: Abbreviation of Generic Routing Encapsulation
7. How to Keep a Smartphone From Being Hacked",
8. L2TP: Abbreviation of Layer 2 Tunneling Protocol
9. Lauren Sporck (26-5-2017), "Update: Most Destructive Malware of All Time" ،OPSWAT, Retrieved 26-8-2017. Edited
10. Margaret Rouse, "antivirus software" ،TechTarget, Retrieved 26-8-2017. Edited.
11. Margaret Rouse, "malware (malicious software)" ،TechTarget, Retrieved 26-8-2017. Edited

12. Margaret Rouse, "spyware" ،TechTarget, Retrieved 26-8-2017. Edited.
13. Margaret Rouse, "virus (computer virus)" , Retrieved 12-8-2017. Edited.
14. Margaret Rouse, "virus (computer virus)" ،TechTarget, Retrieved 26-8-2017. Edited.
15. OTp: One-Time Password .
16. Stallings, William (2012). Computer security : principles and practice. Boston: Pearson
17. UTM : Abbreviation of Unified Threat Management

- **المواقع الالكترونية**

1. https://ar.wikipedia.org/wiki/%D8%A7%D9%84%D8%B9%D8%B1%D8%A7%D9%82
2. http://rap-syr.mam9.com/t23-topic
3. http://redirect.viglink.com
4. www.techlife.samsung.com