الأكاديمية العربية الدولية

المملكة العربية السعودية

بحث في بكالوريوس IT Information

Technology بعنوان

برامج مكافحة الفيروسات

للطالب/ فائق ابراهيم جواد آل مريبط

فهرس البحث

ملخص البحث

يتناول هذا البحث شرح مشتملات برامج مكافحة الفيروسات على أجهزة الحاسب الآلي، من نواحٍ عديدة. بداية من التعريف الكامل للبرنامج الإليكتروني وأنواعه وعناصر التكوين ومعايير التصميم الأساسية للبرنامج، ثم ينتقل إلى ماهية فيروسات الحاسوب العائق الأكبر لجميع أجهزة الحاسوب بشكل عام لكونها في النهاية عبارة عن برامج عادية لكنها ذات وظائف خبيثة. وتوضيحها بشكل تفصيلي ودورة عملها في تدمير الجهاز وسرقة بياناته بشكل غير قانوني، وتم استعراض تاريخ فيروسات الكمبيوتر وأهم خصائصها وآلية عملها، واستعراض أنواعها وأشهر الفيروسات التي تصيب الأجهزة وأكثرها خطورة.

بعد ذلك ننتقل برنامج مكافحة الفيروسات Antivirus وهي برامج متخصصة في مكافحة الفيروسات بالتحديد، وكيفية عملها في اكتشاف الفيروسات والقضاء عليها بمعنى أكثر دقة تعطيلها عن العمل، وختامًا للبحث نستعرض أهم أشهر أنظمة الحماية الواجب تفعيلها في الجهاز للحماية ضد أي هجوم فيروسي أو اختراق عبر شبكات الانترنت قدر الإمكان.

المقدمة

في العصر الحالي أصبح مجتمعنا واقتصادنا ومعظم محاور الحياة يعتمد إلى حد كبير على التقنيات التكنولوجية المتمثلة كثيرا في أجهزة الكمبيوتر وتكنولوجيا المعلومات (and Pati, 2017 Xavier)، لقد استطاعت شبكات الإنترنت حول العالم أن تعقد بين المجتمعات بل جعلته في كيانات موحدة من نواحٍ عديدة، كما فتح لنا أيضًا تأثيرات لم تكن من قبل بهذا التنوع والتحدي من قبل. مع نمو الأمن بسرعة.

ومع التطور المذهل نما عالم القرصنة بشكل أسرع هناك طريقتان للنظر في مسألة أمن المعلومات والبيانات. أحدها هو أن الشركات التي توفر الحوسبة السحابية تفعل ذلك وفقط لذلك سيتم تأمين هذه الشركات بشكل جيد للغاية باستخدام أحدث تقنيات التشفير المتطورة (Seemma et al., 2018) وعلى الرغم من ذلك أصبح الإنسان معرضًا للكثير من المخاطر بسبب الجوانب السلبية التي تأخذ غالباً الهجمات الإلكترونية، حيث تعد الهجمات الإليكترونية التي يتعرض لها الحاسوب من أكبر المشاكل كارثية، وتزداد نسبة الخطورة مع زيادة اعتمادنا على تكنولوجيا المعلومات and Pati, 2017 Xavier).

وفقًا لتقرير Symantec cybercrime عن الجرائم الإلكترونية الذي نُشر في أبريل 2012 فإن الهجمات الإلكترونية 114 تكلف مليار دولار سنويًا، وترتفع إلى 385 مليار دولار بسبب تكاليف الصيانة الأضرار الناجمة وحماية الإليكترونية، كما يتزايد عدد ضحايا الهجمات الإلكترونية بشكل ملحوظ وذلك استنادًا إلى الدراسة الاستقصائية التي أجرتها شركة cybercrime Symantec والتي تضمنت إجراء مقابلات مع العديد من المستخدمين 24 دولة حول العالم، وقد أفاد 69٪ أنهم تعرضوا لهجوم إلكتروني في حياتهم، حسبت الشركة أن 14 شخصًا بالغًا يقعون ضحية لهجوم إلكتروني كل ثانية (Jang and Nepal, 2014).

المحور الأول: البرنامج الإليكتروني

مفهوم البرنامج الإليكتروني

يُعرف البرنامج الإليكتروني اصطلاحًا بأنه عبارة عن بيئة إلكترونية رقمية متكاملة تعرض الدورات عبر الشبكات الإلكترونية، وتوفر التوجيه والإرشاد، وتنظم الاختبارات وكذلك إدارة وتقييم الموارد و العمليات(Al-Noori and Jabar, 2020).

وعرف الباحث (Hindle et al., 2016) البرنامج الإليكتروني بمفهوم أكثر تخصصًا وهو " يتم تعريف البرنامج بشكل عام على أنه مجموعة من التعليمات ، أو مجموعة من الوحدات أو الإجراءات، التي تسمح بنوع معين من تشغيل الكمبيوتر. غالبًا ما يستخدم المصطلح أيضًا بالتبادل مع مصطلحات مثل "تطبيق برمجي" و "منتج برمجي".

أنواع البرامج الإليكترونية

لقد وضح (فايد، 1990) في كتابه أن برامج الحاسوب أنواع متعددة.

1- برامج النظام Software Programs

هي برامج يتم تصميمها للتشغيل أجزاء وعناصر تشغيل برامج الحاسوب المختلفة. وتعرف أيضًا بأنها المنصة أو البيئة الرئيسية لتشغيل برامج الكمبيوتر مثل أنظمة التشغيل Windows و Linux وغيرها من الأنظمة البرمجية، وتمثل الحلقة الوسيطة بين المستخدم والبرامج التطبيقية.

وهناك شكل آخر لبرامج النظام تتمثل الأجهزة الخارجية التي تتصل الكمبيوتر مثل الفأرة ولوحة المفاتيح وغيرها.

2- البرامج التطبيقية Application Programs

هي برامج مصممة لتنفيذ تعليمات وأوامر محددة وفق غرض مصمم ومطور البرنامج، تتميز البرامج التطبيقية أنها ذو واجهة رسومية يمكن للمستخدم التعامل معها لإدخال محددات واستقبال مخرجات.

3- برامج التصميم Programming Programs

هي برامج وظيفتها بناء وتصميم البرامج بواسطة شفرات وبرمجة خاصة يقوم بها المبرمجون لإنشاء برنامج له وظائف معينة.

لغات البرمجة

تتكون لغة الآلة من الرموز الرقمية للعمليات التي يمكن لجهاز كمبيوتر معين تنفيذها مباشرة. الرموز عبارة عن سلاسل من 0 و 1 ، التي تعرف بـ الأرقام ثنائية ("بت") ، والتي يتم تحويلها في من وإلى سداسي عشري (الأساس 16) لعرضها وتعديلها بواسطة المستخدم وهو المطور، تستخدم تعليمات لغة الآلة عادةً بعض البتات لتمثيل العمليات، مثل الإضافة ، وبعضها لتمثيل المعاملات، أو ربما موقع التعليمات.

تم تصميم اللغات الخوارزمية للتعبير عن الحسابات الرياضية أو الرمزية. يمكنهم التعبير عن العمليات الجبرية في تدوين مشابه للرياضيات والسماح باستخدام البرامج الفرعية التي تحزم العمليات شائعة الاستخدام لإعادة الاستخدام (McGuire, 2009)

عناصر تكوين البرنامج الإليكتروني

يحتوي البرنامج على بعض العناصر الضرورية لأداء الغرض المطلوب من عمله، لذلك فإن للبرنامج الإليكتروني عدة عناصر أساسية لا غنى عنها:

1- النصوص Texts

هي عبارة عن الكلام والنصوص المكتوبة التي توضح بيانات البرنامج وتعليمات الاستخدام، وكل ما يخص البرنامج من مفاهيم وتوضيحات، لذلك فهو الرئيسي لبيانات البرنامج، يختلف نوع الخط وطريقة رسمها ولونها وحجمها حسب تصميم البرنامج الملائم، كي يتيح أفضل رؤية وتناسق

مع باقي مكونات البرنامج **(Pavithra, 2018)**، بالإضافة إلى أن استخدام النصوص في البرامج التعليمية مهم جدًا لذوي الاحتياجات الخاصة **(Rayini, 2017)**.

2- الصور والرسومات Pictures

الصور تعطي أنماطًا بصرية عن الشيء أو المادة المراد تقديمها للمتعلم، وهي تحاول نقل أفكاره إلى واقع الشيء بالنسبة للصور الفوتوغرافية، أو تُدخله في بيئة خيالية إذا كانت رسوم وتصميمات رقمية.

3- الفيديو أو الصور المتحركة Videos

يساهم الفيديو في عرض الأحداث المتوالية للمادة التعليمية، حيث يُعرف بأنه عرض للأحداث سواء كان فيديو تمثيلي أو رقمي.

4- الصوتيات Sounds & Voices

على الرغم أن الصوت يُستخدم بدرجة أقل باستثناء الصوت المرتبط بالفيديو، فإن الصوتيات تلعب دورًا فعالًا في تحسين القدرة والانتباه إذا تم تصميم الأصوات بكفاءة، لذلك يمكن أن يوفر متعة الاستماع للموسيقى من أجل تحسين وضبط الحالة المزاجية، أو تضيف الاهتمام إلى موقع نصي من خلال إضفاء الطابع الإنساني على المؤلف، أو تعليم نطق الحروف والمقاطع الصوتية للأطفال

(المتولي وآخرون، 2014)، كما أنها يُعتمد عليها بشكل كبير في مدارس ضعاف البصر مثل: الكتب الناطقة: وهي نسخ صوتية من الكتب التي يمكن تسجيلها على شرائط كاسيت وأقراص مدمجة وأقراص DVD وعلى الإنترنت ككتب إلكترونية، يفضل غالبية ضعاف البصر هذه الوسيلة لأنها الأسهل من ناحية الحصول على المعلومات والتعامل معها، والصحف الناطقة: وهي تستخدم في تناقل الأخبار اليومية والأنباء لضعاف البصر، النصوص الإليكترونية: هي عبارة عن بيانات مخزنة عن الحاسوب يتم التعامل معها بواسطته لاستخراج المعلومات سواء لقراءتها بالنطق أو لطباعتها بأسلوب نظام برايل المنقط، وذلك تحت يد ضعيف البصر **(Rayini, 2017)**.

معايير تصميم البرنامج الإليكتروني

هناك العديد من الخصائص بعضها يخضع للغرض والآخر يكون مطورًا ليسمح بالحصول على خدمات وتنفيذ عمليات أعقد، وعلى أساس هذه المزايا يعمل البرنامج بكفاءة عالية.

- أن يكون مستقرًا، ويمنح المستخدمين مستوى عالٍ من الإمكانيات المتوفرة والمخصصة لتسهيل العمليات، لذلك يجب أن يكون استخدام البرامج التعليمية بسيطًا وبديهيًا.
- يجب أن تكون الواجهة مفهومة ويجب أن تكون أدوات تشغيل البرامج المختارة واضحة ومفهومة ومناسبة للعمر. يجب أن يكون المحتوى الرقمي مفتوحًا ، ويقدم أنشطة تعليمية تفاعلية متنوعة.
- دعم التعلم والاعتراف والاستكشاف، وتقديم الملاحظات، واستخدام التصور والوسائط المتعددة على أوسع نطاق ممكن –حسب الغرض والوظيفة **(Karolcilk et al., 2015)**.

المحور الثاني: التهديدات الأمنية وفيروسات الكمبيوتر

مفهوم فيروسات الكمبيوتر

وقد ذكر باحثون تعاريف متنوعة عن فيروسات الكمبيوتر، حيث وضح (Fatima et al., 2018) في دراسته أن فيروس الكمبيوتر هو برنامج خبيث لأنظمة الكمبيوتر ويعطل الوظائف الطبيعية للنظام ويتلف ملفات البيانات، يعمل فيروس الكمبيوتر مثل الفيروسات البيولوجية التي تربط نفسها بجهاز كمبيوتر مضيف، وتتلف ملف البرنامج وملف البيانات ونظام التشغيل لهذا الكمبيوتر. لديها القدرة على إعادة إنتاج نفسها من خلال الارتباط ببرامج أخرى. سيستمر الفيروس في نشر العدوى إلى الملفات والبرامج الأخرى ويؤثر على أداء أي نظام،

يمكن للفيروسات أن تنتقل من كمبيوتر إلى كمبيوتر بعدة طرق مختلفة، على سبيل المثال عن طريق إرسال نفسها بالبريد إلى عشرات الأشخاص في البريد الوارد لعنوان بريد المضيف. يمكنه أيضًا الإرسال عن طريق تنزيل أي ملف من الإنترنت واتصالات الشبكة والقرص المرن والحافلات التسلسلية العالمية أو عن طريق الأقراص المضغوطة.

وفي دراسة (فطوش، 2019) ذكر الباحث عدة تعريفات لفيروس الكمبيوتر، هي عبارة عن مجموعة من التعليمات التي تتكاثر بمعدل سريع جدا وتصيب النظام المعلوماتي بالشك، وذكر أيضًا "الفيروس هو عبارة عن خلية مغناطيسية نائمة ومبرمجة تنشأ في وقت محدد لتخريب البرنامج الأصلي ومنتشرة في الأجهزة الأخرى التي تضمنتها الشبكة بحيث تفسر ما تحتويه من معلومات."كما عرفه بعض المختصين في المجال المعلوماتي بأنه: برنامج يصممه بعض المختصين

بهدف تخريبي مع إعطائه القدرة على ربط نفسه ببرامج أخرى كي يسمح له بالانتشار داخل النظام حتى يتسبب في تدميره تماما"، ويعرفه آخرون بأنه: "مرض يصيب الحاسب الآلي، فهو ليس فيروسا بالمعنى البيولوجي المعروف، ولكنه برنامج معين يتم تسجيله أو زرعه على الأقراص أو الأسطوانات الخاصة بالحاسب ويظل هذا الفيروس لفترة محددة ثم ينشط فجأة في توقيت معين ليدمر البرامج والبيانات المسجلة والمخزنة في داخل الحاسب ويشمل أثره التخريبي لإتلاف والحذف والتعديل" ، فهو ببساطة شديدة برنامج حاسب مثل أي برنامج تطبيقي آخر ولكن يتم تصميمه بواسطة أحد المخربين بهدف محدد وهو إحداث أكبر ضرر ممكن بنظام الحاسب ولتنفيذ

وفي دراسة (Pande, 2017) فيروس الكمبيوتر هو رمز ضار مكتوب لإتلاف / إلحاق الضرر بالكمبيوتر المضيف عن طريق حذف ملف أو إلحاقه ، أو شغل مساحة ذاكرة الكمبيوتر عن طريق نسخ نسخة الرمز ، أو إبطاء أداء الكمبيوتر ، أو تهيئة الجهاز المضيف ، وما إلى ذلك. يمكن أن ينتشر عبر مرفقات البريد الإلكتروني ومحركات القلم والصور الرقمية والتحية الإلكترونية ، ومقاطع الصوت أو الفيديو وما إلى ذلك، قد يكون الفيروس موجودًا في جهاز الكمبيوتر ولكن لا يمكنه تنشيط نفسه دون تدخل بشري.

تاريخ فيروسات الكمبيوتر

يعود ظهور البرامج ذات الأهداف الخبيثة وهي الفيروسات إلى ثمانينيات القرن العشرين، وذلك بعد الثورة الكبيرة في عالم البرمجة، فظهر العديد من البرامج المتنوعة في وظائفها ومن بعدها الألعاب، إلا أن كم هذا التطور لم يسلم من وجود عيوب برمجية في تلك البرامج، التي أصبحت نقطة

ضعف قوية في بناء برامج تستهدف تلك نقاط الضعف وتغير من وظائف البرنامج سواء بإتلافه أو أعطال معينة ومؤقتة (Spafford, 1991).

خصائص فيروسات الكمبيوتر

الفيروسات هي برامج خبيثة مصممة للوصول إلى الكمبيوتر أو تثبيته دون موافقة المستخدم. يؤدون مهام غير مرغوب فيها في الكمبيوتر المضيف لصالح طرف ثالث. هناك مجموعة كاملة من البرامج الضارة التي يمكن أن تؤدي إلى تدهور خطير في أداء الجهاز المضيف. هناك مجموعة كاملة من البرامج الضارة التي تمت كتابتها ببساطة لإلهاء / إزعاج المستخدم ، إلى البرامج المعقدة التي تلتقط البيانات الحساسة من الجهاز المضيف وإرسالها إلى الخوادم البعيدة (Pande, 2017)

لقد وضح (Khan et al., 2017) أن للفيروسات خصائص مشتركة بين كل الأنواع وهي

- القدرة على إصابة الملفات وإتلافها
- القدرة على تكرار نفسها لإصابة الحاسوب
- القدرة على التخفي والتنكر بشكل يصعب الوصول إليه بسهولة وذلك عن طريق التشفير
- يمكن للفيروس أن يصيب العديد من سجلات الكمبيوتر المصاب (والشبكة التي ينتمي إليها لأن بعض الفيروسات موجودة في الذاكرة بمجرد تحميل قرص مرن أو برنامج في نفس الشيء ، يكون الفيروس "شديد" أو "يلتصق" بالذاكرة نفسها ثم تصيب أي ملف على الكمبيوتر كان له حق الوصول.

- يمكن أن يكون متعدد الأشكال: تمتلك بعض الفيروسات القدرة على تعديل التعليمات البرمجية الخاصة بك ، مما يعني أن الفيروس قد يكون له العديد من الأشكال المتشابهة ، مما يجعل اكتشافها صعبًا.
- قد تكون مقيمة في الذاكرة أم لا: كما ذكرنا سابقًا ، يمكن للفيروس أن يكون مقيمًا ، ويتم تحميله أولاً في الذاكرة ثم يصيب الكمبيوتر. يمكن أيضًا أن يكون "غير مقيم عند تنفيذ رمز الفيروس فقط في كل مرة يتم فيها فتح ملف.
- يمكن أن تكون خفية: تقوم الفيروسات الخفية (الشبح) أولاً بإرفاق نفسها بالملفات الموجودة على الكمبيوتر ثم مهاجمة الكمبيوتر ، مما يؤدي إلى انتشار الفيروس بسرعة أكبر.
- يمكن للفيروس أن يجلب فيروسات أخرى: يمكن للفيروس أن يؤدي إلى فيروس آخر مما يجعله أكثر فتكًا ويساعد بعضنا البعض على إخفاء أو حتى مساعدتك على إصابة قسم معين من الكمبيوتر.
- يمكنك جعل النظام لا يظهر أبدًا علامات الإصابة: يمكن لبعض الفيروسات إخفاء التغييرات التي تجريها ، مما يجعل اكتشاف الفيروس أكثر صعوبة.
- يمكنهم البقاء على الكمبيوتر حتى في حالة تهيئة القرص الصلب: على الرغم من قلة الحالات ، إلا أن بعض الفيروسات لديها القدرة على إصابة أجزاء مختلفة من الكمبيوتر.

آلية عمل فيروسات الكمبيوتر

وظائف برامج الكمبيوتر معقدة ، وهذا يتيح فرصة وجود نقاط ضعف، المعروفة باسم الثغرات Exploits: وهي عبارة عن أخطاء برمجية ناجمة أو شفرات قابلة للتعديل تم توظيفها بشكل

خاطئ فأصبح أمكن التعديل عليها برمجيًا فيؤثر على طبيعة عمل النظام، لذلك تظهر العديد من الطرق الممكنة لدخول الفيروس إلى نظام الكمبيوتر، إذ يضيف الفيروس عادةً شفراته القابلة للتنفيذ إلى بداية البرنامج أو يستبدل تعليماته الأولى ، مما يتسبب في استدعاء البرنامج بالتعليمات الأولى للفيروس بدلاً من الإرشادات الأولى للبرنامج، في معظم الحالات ينشر المستخدم المخالف الفيروس دون علمه. على سبيل المثال ، قد يقوم الشخص بتنزيل برنامج مصاب وتشغيله. في هذه الحالة ، يقوم الفيروس بتحميل نفسه في الذاكرة ويصيب البرامج الأخرى الموجودة على القرص، وعلى الرغم من استمرار الفيروس في إصابة ملف واحد تلو الآخر، إلا أنه ليس لدى المستخدم أي طريقة لمعرفة ما إذا كان الفيروس قد تم تشغيله من قبل (Mishra, 2010).

دورة حياة فيروس الكمبيوتر

وفق تصور الباحث (Ikekonwu et al., 2005) عن دورة حياة فيروس الكمبيوتر، ذكرها في خمس مراحل:

1- المرحلة الأولى: الثبات Dormancy

عند إصابة جهاز جديد أو برنامج جديد ، قد يظل فيروس الكمبيوتر كامنًا لفترة من الوقت لتجنب الشك. قد تختلف مدة فترة السكون اعتمادًا على نوع الآلية المستخدمة. قد تنتظر بعض الفيروسات عددًا معينًا من عمليات تنفيذ البرنامج المفقود أو انقضاء فترة زمنية معينة قبل التقدم إلى المرحلة التالية في الدورة.

2- المرحلة الثانية: الانتشار Propagation

في مرحلة الانتشار يحاول الفيروس إرسال نسخ إلى برامج أخرى على الجهاز المضيف أو الأجهزة على الشبكة. قد يكون الهدف هنا هو ملف COM أو ملف EXE أو BOOT أو القسم أو البيانات، قد ينتشر الفيروس عن طريق البحث في النظام (الأقراص أو الخادم) عن البرامج غير المصابة وربط نفسه بها.

يتم تصنيف آليات انتشار الفيروس على أنها واحد لواحد ، وواحد لأطراف ، وعديد لواحد ، ومتعدد بأطراف. اعتمادًا على الآلية المحددة المستخدمة، يعدل الكود الفيروسي ملفًا قابلاً للتنفيذ بحيث يتلقى التحكم عند تنشيط البرنامج. عند تنفيذ برنامج مصاب ، ينتشر رمز الفيروس إلى الهدف ويضع مرحلته في السكون، ثم عادة ما يتم إرجاع التحكم إلى البرنامج المضيف للعمليات العادية. بهذه الطريقة ، يمكن للفيروس إخفاء وجوده طوال الطريق خلال مرحلة بدء التشغيل.

3- المرحلة الثالثة: التلف Damage

يمكن أن يتراوح الضرر نفسه من مزعج إلى حد ما إلى ضار ، على سبيل المثال فقدان البيانات وفشل البرنامج مثل القدرة على التحميل وفشل التمهيد وضياع ساعات العمل والقلق. تتطلب جميع الفيروسات تقريبًا بعض مراحل التطوير ، ومراقبة أنشطة النظام والمستخدم وإظهار سلوك معين

وقد وضح الباحث (Mishra, 2010) تصورًا آخرا عن دورة حياة فيروس الكمبيوتر كما يلي

1- المرحلة الأولى التكوين

الفيروسات هي عبارة عن برامج لكن يتم إنشائها وبرمجتها لتقوم بأعمال تخريبية وغير قانونية من قبل أشخاص يرغبون في إلحاق الضرر بأجهزة الكمبيوتر وتحقيق أهداف .

2- المرحلة الثانية النسخ

تقوم فيروسات الكمبيوتر بتكرار نفسها ونقل من جهاز كمبيوتر إلى كمبيوتر آخر.

3- المرحلة الثالثة التنشيط

ينشط الضرر المسبّب للفيروسات من تلقاء نفسه عندما يتم استيفاء الشروط بنجاح.

4- المرحلة الرابعة الاكتشاف

تحدث مرة واحدة في السنة على الأقل عندما يصبح الفيروس تهديدًا.

5- المراحل الخامسة الاستيعاب

في هذا الوقت يكتشف مطورو برامج مكافحة الفيروسات العلاج لعلاج الفيروس ، وقد يستغرق ذلك فترة زمنية تتراوح من شهر إلى 6 أشهر أيضًا.

6- المرحلة السادسة القضاء

إذا قام أي مستخدم بتثبيت برنامج مناسب لحذف الفيروسات ، فيمكن حذفه بنجاح ، ولكن الحقيقة هي أنه لا يتم حذف أي فيروس تمامًا ولكن يتم تقليل تأثيره.

التهديدات الأمنية التي تتعرض لها أجهزة الكمبيوتر

يتم برمجة وتصميم البرامج الخبيثة بشكل يمكن استغلال الثغرات الموجودة في نظام الأمان في جهاز الكمبيوتر.

الإعلانات الخبيثة Adware

عادةً عندما ينقر المستخدم فوق ارتباط خطير أو مرفق بريد إلكتروني يقوم بعد ذلك بتثبيت برامج محفوفة بالمخاطر. بمجرد دخول البرنامج الضار إلى النظام ، يمكن أن يقوم بما يلي، يحظر الوصول إلى المكونات الرئيسية للشبكة (مثل فيروسات الفدية) ، أو يثبت البرامج الضارة أو البرامج الضارة الإضافية ، ويحصل سرًا على المعلومات عن طريق نقل البيانات من القرص الصلب (برامج التجسس) ، ويعطل مكونات معينة ويجعل النظام غير صالح للعمل

برامج التجسس Spyware

إنه نوع خاص يتم تثبيته في الكمبيوتر الهدف بإذن المستخدم أو بدونه ، وهو مصمم لسرقة المعلومات الحساسة من الجهاز الهدف. في الغالب يجمع عادات التصفح للمستخدم وإرسالها إلى الخادم البعيد دون علم صاحب الكمبيوتر. يتم تنزيلها في معظم الأوقات على الكمبيوتر المضيف أثناء تنزيل البرامج المجانية ، أي برامج التطبيقات المجانية من الإنترنت، قد تكون برامج التجسس من أنواع مختلفة ؛ يمكنه تتبع ملفات تعريف الارتباط للكمبيوتر المضيف.

التصيد الاحتيالي Phishing

التصيد الاحتيالي هو ممارسة إرسال اتصالات احتيالية يبدو أنها واردة من مصدر حسن السمعة ، عبر البريد الإلكتروني عادةً. الهدف هو سرقة البيانات الحساسة مثل بطاقة الائتمان ومعلومات تسجيل الدخول أو تثبيت برامج ضارة على جهاز الضحية. (Jupin et al., 2017) .

أشكال فيروسات الكمبيوتر

لقد صنف الباحث (Mishra, 2010) في دراسته الفيروسات إلى عدة أنواع وهي:

1- فيروسات الماكرو Macro Viruses

فيروسات الماكرو تصيب هذه الفيروسات جميع الملفات التي تحتوي على وحدات ماكرو مثل doc و pps و xls و mdb ، وتؤثر على وحدات الماكرو والقوالب والمستندات الموجودة في الملفات (Wahahat et al., 2007).

2- فيروسات Direct Action Viruses

تتكرر هذه الأنواع من الفيروسات وتتخذ إجراءات عند تنفيذها ، فهي تصيب الملفات الموجودة في الدليل أو المجلد الموجود فيه. AUTOEXEC.BAT (Horton and Seberry, 1997)

3- فيروسات الكتابة الفوقية Overwrite Viruses

تختص هذه الفيروسات بالقدرة على إتلاف بيانات البرامج وبالتالي يصبح البرنامج عديم الوظيفة، وذلك عن طريق الكتابة فوق يقوم الفيروس بكتابة التعليمات البرمجية الخاصة به مباشرة فوق البرنامج المضيف ، مما يؤدي إلى تدمير جزء أو كل التعليمات البرمجية الخاصة به. لن يتم تنفيذ البرنامج المضيف بعد الآن بشكل صحيح بعد الإضرار به. (Zaqaibeh and Al Daoud, 2008).

4- فيروسات الكمبيوتر الدودية Worms Viruses

فيروسات الديدان من معروفة بقدرتها على التناسخ بدون تحكم من قبل المستخدم، يعمل هذا الفيروس على استغلال نقاط الضعف في أمان الحاسوب لسرقة بيانات المستخدم على الجهاز.

تقوم فيروسات الكمبيوتر الدودية باستهلاك نسبة كبيرة من ذاكرة الجهاز، مما يؤدي إلى حدوث بطء وتعطيلات متكررة في نظام التشغيل (Chen and Robert, 2004).

5- فيروسات الملفات File Viruses

هي فيروسات الملفات فيقوم بنسخ نفسه إلى كل ملف برنامج قابل للتنفيذ يصيبه عند تنفيذ البرنامج القابل للتنفيذ، يتحكم الفيروس في الكمبيوتر ويحاول إصابة الملفات الأخرى (Jaiswal, 2017).

6- فيروسات نظام التشغيل Boot sector virus

تهاجم هذه الفيروسات الأقراص المرنة وتعمل على تلف الملفات المسؤولة عن عملية إقلاع الحاسوب وبالتالي تحدث مشكلة متعددة في عملية التشغيل والإقلاع.

يدخل فيروس Boot sector virus من خلال الأقراص المرنة المصابة عندما ينقل مستخدم قرصًا مرنًا مصابًا إلى جهاز كمبيوتر آخر ، يصيب الفيروس الكمبيوتر الثاني ثم يقوم الفيروس بتغيير سجل التمهيد الرئيسي للقرص الثابت ويظل موجودًا بشكل دائم في نظام الكمبيوتر (Mishra, 2012)

7- فيروسات الشبكة Network Virus

هو نوع من الفيروسات يتميز بقدرته على الانتشار والانتقال عبر شبكات الإنترنت إلى أجهزة الحاسوب، وخاصة الأجهزة الضعيفة التي لا توفر أمن كاف لملفات الجهاز (Han et al., 2008)

نماذج لأشهر فيروسات الكمبيوتر

تُستخدم البرامج الضارة بشكل أساسي لسرقة المعلومات الشخصية أو المالية أو التجارية الحساسة لصالح الآخرين. غالبًا ما تُستخدم البرامج الضارة لاستهداف مواقع الويب الحكومية أو الشركات لجمع معلومات محمية أو لتعطيل عملياتها. في حالات أخرى ، يتم استخدام البرامج

الضارة أيضًا ضد الأفراد للحصول على معلومات شخصية مثل أرقام الضمان الاجتماعي أو أرقام بطاقات الائتمان. منذ ظهور الوصول إلى الإنترنت واسع النطاق على نطاق واسع وهو أرخص وأسرع ، تم تصميم البرامج الضارة بشكل متزايد ليس فقط لسرقة المعلومات ولكن بشكل صارم لأغراض الربح. على سبيل المثال ، تم تصميم غالبية البرامج الضارة المنتشرة للتحكم في أجهزة الكمبيوتر الخاصة بالمستخدم لاستغلال السوق السوداء مثل إرسال بريد إلكتروني عشوائي أو مراقبة سلوكيات تصفح الويب للمستخدم وعرض إعلانات غير مرغوب فيها (Jang and Nepal, 2014).

على مر التاريخ ظهرت العديد من الفيروسات تتمايز فيما بينها في قدراتها التخريبية (Horton and Seberry, 1997)

1- فيروس حصان طروادة Trojan horse

تعد فيروسات المعروفة باسم حصان طروادة من أحد أخطر التهديدات لأمن الكمبيوتر، حيث تخترق هذه الفيروسات الأنظمة مع الملفات العادية التي يحملها المستخدم على الجهاز، وما أن تدخل إلا وتبدأ عملها التخريبي في سرقة بيانات المستخدم والمعلومات المحملة على الجهاز، كما تستهدف البرامج وتعطلها (Al-Saadoon and Al-Bayatti, 2011)

في عام 2009 ، تم الإبلاغ عن أن أحصنة طروادة شكلت 60 بالمائة من جميع البرامج الضارة. في عام 2011 ، قفز الرقم إلى 73 بالمائة. تشير النسبة المئوية الحالية إلى أن ما يقرب من ثلاثة من كل أربعة سلالات جديدة من البرامج الضارة التي تم إنشاؤها في عام 2011 كانت من

الفيروسات وتوضح أنها السلاح المفضل لمجرمي الإنترنت لتطفل الشبكة وسرقة البيانات (Jang and Nepal, 2014).

2- فيروس الفدية Ransomware Viruses

فيروسات الفدية Ransomware Viruses عبارة عن برامج خبيثة تقوم بتشفير الملفات وتجعلها صعبة الوصول إليها من قبل المستخدم لحين قيامه بدفع مقابل مادي لمبرمج هذا الفيروس لفك تشفيره (Shah and Farik, 2017).

المحور الثالث: برامج نظم الأمن لمكافحة الفيروسات في جهاز الكمبيوتر

دائما تتعرض المعلومات على جهاز الكمبيوتر لمخاطر الاختراق والسرق أو هجوم ضار محتمل يسعى إلى الوصول غير القانوني إلى البيانات أو تعطيل العمليات الرقمية أو إتلاف المعلومات، هذه المخاطر يتم صناعتها من قبل جهات فاعلة مختلفة مثل جواسيس الشركات ونشطاء القرصنة والجماعات الإرهابية والمنظمات الإجرامية والمتسللين (Seemma et al., 2018)

برامج مكافحة الفيروسات

برنامج مكافحة الفيروسات هو فئة من البرامج المصممة لمنع وكشف وإزالة الإصابات بالبرامج الضارة على أجهزة الحوسبة الفردية والشبكات وأنظمة تكنولوجيا المعلومات. يمكن لبرامج مكافحة الفيروسات، المصممة في الأصل لاكتشاف الفيروسات وإزالتها من أجهزة الكمبيوتر، الحماية أيضًا من مجموعة متنوعة من التهديدات ، بما في ذلك أنواع أخرى من البرامج الضارة.

أنواع برامج مكافحة الفيروسات

تتنوع تقسيمات برامج مكافحات الفيروسات إلى عدة تصنيفات

1- حسب النظام التشغيل

يتم تقسيم برامج مكافحة الفيروسات في عدد من الأشكال، بما في ذلك برامج مكافحة الفيروسات المستقلة ومجموعات أمان الإنترنت التي توفر الحماية من الفيروسات بجانب جدران

الحماية وضوابط الخصوصية وغيرها من وسائل الحماية الأمنية، ومن أمثلة أنظمة التشغيل المنتشرة عالميًا

- نظام التشغيل .ويندوز Windows antivirus software
- نظام تشغيل Mac OS antivirus software.
- نظام تشغيل Android antivirus software.

يقدم بعض مطوري برامج مكافحة الفيروسات إصدارات أساسية من منتجاتهم مجانًا. تقدم هذه الإصدارات المجانية بشكل عام الحماية الأساسية لمكافحة الفيروسات وبرامج التجسس ، ولكن عادةً ما تكون الميزات والحماية الأكثر تقدمًا متاحة فقط للعملاء الذين يدفعون الثمن. بينما يتم استهداف بعض أنظمة التشغيل بشكل متكرر بواسطة مطوري الفيروسات ، يتوفر برنامج مكافحة الفيروسات لمعظم أنظمة التشغيل.

آلية عمل برامج مكافحة الفيروسات

تستخدم برامج مكافحة الفيروسات مجموعة متنوعة من تقنيات الكشف عن الفيروسات. في الأصل، كانت برامج مكافحة الفيروسات تعتمد على الاكتشاف القائم على التوقيع للإبلاغ عن البرامج الضارة.

تعتمد برامج مكافحة الفيروسات على علامات وشفرات الفيروسات المخزنة - وهي سلاسل مميزة وفريدة من البيانات التي تميز البرامج الضارة المعروفة، يستخدم برنامج مكافحة الفيروسات

هذه التوقيعات لتحديد وقت مواجهته للفيروسات التي تم تحديدها بالفعل وتحليلها من قبل خبراء الأمن.

استعادة وإزالة الفيروسات

بمجرد اكتشاف الفيروس ، كيف يمكن لبرامج مكافحة الفيروسات التراجع عن الضرر الذي أحدثه الفيروس؟ برامج مكافحة الفيروسات سيئة إلى حد ما في استعادة البيانات - الفيروسات التي تحاول إتلاف الملفات بدلاً من مجرد إصابتها ستنجح ما لم يتم نسخ هذه الملفات احتياطيًا. تعمل برامج فحص الفيروسات على إصلاح الملفات عن طريق حذف رمز الفيروس من الملف ، مما يؤدي في معظم الحالات إلى إعادة الملف إلى حالته التي كانت مصابة مسبقًا. ومع ذلك ، بالنسبة للفيروسات التي تلحق الضرر بملفات النظام (مثل الفيروسات التي تمنع الوصول إلى بائعي برامج مكافحة الفيروسات وتغير مكتبة الشبكة بشكل لا يمكن إصلاحه) ، فإن برنامج مكافحة الفيروسات غير قادر على إصلاح جميع الأضرار. الطريقة الوحيدة المضمونة لاستعادة الضرر الذي يسببه الفيروس هي تنظيف جميع الملفات المصابة واستعادة كل شيء آخر من النسخ الاحتياطية (Durkota and Dormann, 2008)

المشاكل التي برامج مكافحة الفيروسات

يعاني برنامج مكافحة الفيروسات من مشاكل أكثر من عدم قدرته على اكتشاف أحدث الفيروسات. العديد من نسخ برامج مكافحة الفيروسات غير قادرة على اكتشاف حتى الفيروسات القديمة ، لأن المستخدمين النهائيين كثيرًا ما ينسون أو ببساطة لا يقوموا بتحديث قواعد بيانات

الفيروسات الخاصة بالماسح الضوئي للفيروسات حتى فوات الأوان. نادرًا ما يتم إجراء عمليات الفحص عند الطلب لأنها بطيئة وتستهلك الموارد أثناء الجري ، لذلك تميل الفيروسات الخاملة إلى أن يكون لها عمر طويل إلى حد ما. لا تخلو الماسحات الضوئية عند الوصول من المشاكل ، فبعضها يستهلك الكثير من الموارد ، لذلك يميل العديد من المستخدمين إلى تعطيلها إذا كانوا يستخدمون جهازًا أبطأ.

بينما قد تصبح برامج مكافحة الفيروسات جيدة للغاية في استشعار نشاط الفيروسات ، هناك دائمًا ثغرات أمنية جديدة لاستغلالها في نظام التشغيل وبرامج الشبكات التي من شأنها أن تمنح الفيروسات نقطة دخول أخرى تتجاوز برنامج مكافحة الفيروسات. يعتبر العثور على ثغرة أمنية والإبلاغ عن أحد هذه المواقع بمثابة شرف لمجتمع كتابة الفيروسات.

تعد برامج مكافحة الفيروسات المستخدمة اليوم فعالة إلى حد ما - ولكن فقط إذا تم تحديثها واتخذ المستخدم الاحتياطات (مثل عدم فتح مستندات أو برامج غير مألوفة.) على الرغم من كل هذا ، لا يمكن لبرامج مكافحة الفيروسات الحماية من الفيروسات الجديدة ، وقليل يتخذ المستخدمون الاحتياطات اللازمة. تم إجراء مسح لمستخدمي أجهزة الكمبيوتر في الشركات ، ووجد أن العديد من المستخدمين ما زالوا يصابون بالعدوى حتى لو طُلب منهم اتخاذ جميع الاحتياطات اللازمة.. مع تزايد حجم الإنترنت يوميًا ، من غير المحتمل أن تكون برامج مكافحة الفيروسات قادرة على حماية جميع المستخدمين المتصلين ؛ ومع ذلك ، مع الرعاية والاهتمام المناسبين ، يجب أن يكون الأشخاص قادرين على التعامل مع جميع الفيروسات باستثناء أكثرها غرابة.

اكتشاف الفيروسات

تستخدم برامج مكافحة الفيروسات مجموعة متنوعة من تقنيات الكشف عن الفيروسات. في الأصل، كانت برامج مكافحة الفيروسات تعتمد على الاكتشاف القائم على التوقيع للإبلاغ عن البرامج الضارة. تعتمد برامج مكافحة الفيروسات على توقيعات الفيروسات المخزنة - سلاسل فريدة من البيانات التي تميز البرامج الضارة المعروفة. يستخدم برنامج مكافحة الفيروسات هذه التوقيعات لتحديد وقت مواجهته للفيروسات التي تم تحديدها بالفعل وتحليلها من قبل خبراء الأمن

1- تقنية المسح Scanning

هي الطريقة الأكثر شيوعًا للكشف عن الفيروسات الموجودة، ويتم تنفيذها في جميع حزم برامج مكافحة الفيروسات الرئيسية . هناك نوعان من المسح الضوئي: عند الوصول وعند الطلب. يقوم الفحص عند الوصول بفحص الملفات عند تحميلها في الذاكرة قبل التنفيذ. يقوم المسح عند الطلب بمسح كل الذاكرة الرئيسية وقطاع التمهيد وذاكرة القرص أيضًا ، ويبدأ من قبل المستخدم عندما يريد. أصبح الفحص عند الوصول أكثر قوة مؤخرًا، مع إجراء عمليات فحص الفيروسات حتى إذا تم تحديد الملفات ، ولكن لم يتم تحميلها.

المزايا:

يمكن للماسحات الضوئية العثور على فيروسات لم يتم تنفيذها بعد - وهذا أمر بالغ الأهمية لديدان البريد الإلكتروني ، والتي يمكن أن تنتشر بسرعة إذا لم يتم إيقافها. أيضًا ، أصبحت الإنذارات الكاذبة نادرة للغاية مع البرنامج المتاح اليوم. أخيرًا ، تعد الماسحات الضوئية جيدة جدًا في اكتشاف الفيروسات التي لديها توقيعات لها.

السلبيات:

هناك نوعان من العيوب الرئيسية لتقنيات المسح، أولهما إذا كان البرنامج يستخدم سلسلة توقيع لاكتشاف الفيروس، فكل ما يتعين على كاتب الفيروسات فعله هو تعديل سلسلة التوقيع لتطوير فيروس جديد. يظهر هذا في الفيروسات متعددة الأشكال. العيب الثاني والأكبر بكثير هو القيد الذي لا يمكن للماسح الضوئي فيه إلا البحث عن شيء يحمل توقيعه. كان فيروس الأميبا المالطي فيروسًا مدمرًا للغاية، تم تنشيطه في 11 نوفمبر 1991 ، وكان قادرًا على الانتشار بسرعة قبل تنشيطه دون أن يتم اكتشافه. وفقًا لنشرة الفيروسات لعام 1991: "قبل 2 تشرين الثاني (نوفمبر) 1991 ، لم يكتشف أي ماسح ضوئي تجاري أو برنامج كومبيوتري (يحتوي VB نسخ منه) فيروس Amoeba المالطي. وأظهرت الاختبارات أنه لم يكتشف أحد أدوات الفحص التجارية الرئيسية المستخدمة ... الفيروس" على الرغم من أن تحديثات الفيروسات تحدث بشكل متكرر اليوم بسبب الإنترنت ، فلا يزال يتعذر اكتشاف الفيروسات حتى يتم تنفيذ أحدها.

2- الكشف عن الفيروسات الكشف

هذه طريقة عامة للكشف عن الفيروسات، يطور صانعو برامج مكافحة الفيروسات مجموعة من القواعد لتمييز الفيروسات عن غير الفيروسات. إذا اتبع برنامج أو مقطع رمز هذه القواعد، فسيتم تمييزه بأنه فيروس ويتم التعامل معه وفقًا لذلك هذا يسمح باكتشاف أي فيروس، ونظريًا يجب أن يكون كافياً للتعامل مع أي هجمات فيروسات جديدة.

المزايا:

الحماية العامة من الفيروسات ستجعل جميع برامج فحص الفيروسات الأخرى عفا عليها الزمن وستكون كافية لإيقاف أي فيروس، لا يحتاج المستخدم إلى تنزيل تحديثات الفيروسات الأسبوعية بعد الآن، لأن البرنامج يمكنه اكتشاف جميع الفيروسات.

السلبيات:

على الرغم من أن هذه فوائد كبيرة للتحقق من الكشف عن الفيروسات إلا أن التقنية الحالية ليست كافية. يمكن لكتاب الفيروسات كتابة فيروسات لا تمتثل للقواعد بسهولة ، مما يجعل المجموعة الحالية من قواعد الكشف عن الفيروسات عفا عليها الزمن. يجب تنزيل التغييرات التي تم إجراؤها على هذه القواعد، وبالتالي يجب تحديث أدوات فحص الفيروسات هذه ولن توقف العديد من الفيروسات الجديدة، مما يمنحها خصائص مماثلة للماسحات الضوئية، بالإضافة إلى ذلك فإن احتمال وجود إنذارات كاذبة وعدم اكتشاف فيروس معروف يكون أكبر باستخدام أدوات التحقق من الكشف عن مجريات الأمور مقارنة بأجهزة الفحص (Choudhary et al., 2013)

أنظمة الأمن وحماية المعلومات في جهاز الكمبيوتر

يستلزم لأي جهاز حاسوب أن يحمل كل سبل وسائل الأمن ضد الفيروسات، وخصوصًا إذا كان متصلا بالإنترنت لأنه أصبح مصدرًا لأنواع متعددة من الفيروسات والبرامج الضارة.

نظام كشف التسلل Intrusion Detection System (IDS)

نظام كشف التسلل هو نظام يراقب حركة مرور الشبكة بحثًا عن أي نشاط مشبوه ويصدر تنبيهات عند اكتشاف مثل هذا النشاط. إنه تطبيق برمجي يقوم بمسح شبكة أو نظام بحثًا عن نشاط ضار أو انتهاك للسياسة. عادةً ما يتم الإبلاغ عن أي مشروع ضار أو انتهاك إما إلى المسؤول أو يتم جمعه مركزيًا باستخدام نظام إدارة المعلومات والأحداث (SIEM). يدمج نظام SIEM المخرجات من مصادر متعددة ويستخدم تقنيات تصفية الإنذارات للتمييز بين النشاط الضار والإنذارات الكاذبة (دخيل وطلحة، 2016).

جدار الحماية Firewalls

جدران حماية الشبكة هي أجهزة أمان تُستخدم لإيقاف أو تخفيف الوصول غير المصرح به إلى الشبكات الخاصة المتصلة بالإنترنت ، وخاصة شبكات الإنترانت. يتم تحديد حركة المرور الوحيدة المسموح بها على الشبكة عبر سياسات جدار الحماية - يتم حظر أي حركة مرور أخرى تحاول الوصول إلى الشبكة. تقع جدران حماية الشبكة في الخط الأمامي للشبكة ، وتعمل كحلقة وصل اتصالات بين الأجهزة الداخلية والخارجية، يمكن تكوين جدار حماية الشبكة بحيث تمر أي بيانات تدخل إلى الشبكة أو تخرج منها - وهو يحقق ذلك عن طريق فحص كل رسالة واردة ورفض تلك التي لا تستوفي معايير الأمان المحددة، عند تكوينه بشكل صحيح، يسمح جدار الحماية للمستخدمين بالوصول إلى أي من الموارد التي يحتاجون إليها مع إبعاد المستخدمين غير المرغوب فيهم أو المتسللين المتنقلة أو البرامج الضارة الأخرى التي تحاول الوصول إلى الشبكة المحمية Wool, (2004).

مصادقة المعلومات The authentication

إنها عملية تحديد هوية الفرد والتأكد من أن الفرد هو نفسه الذي يدعي أنه / هي. الطريقة النموذجية للمصادقة عبر الإنترنت هي عبر اسم المستخدم وكلمة المرور. مع زيادة حالات الجرائم الإلكترونية المبلغ عنها عن طريق سرقة الهوية عبر الإنترنت ، اتخذت المنظمات بعض الترتيبات الإضافية للمصادقة مثل كلمة المرور لمرة واحدة (OTP) ، حيث يشير الاسم إلى أنها كلمة مرور يمكن استخدامها مرة واحدة فقط وهي يتم إرسالها إلى المستخدم كرسالة نصية قصيرة أو بريد إلكتروني على رقم الهاتف المحمول / عنوان البريد الإلكتروني الذي حدده أثناء عملية التسجيل. تُعرف باسم طريقة المصادقة الثنائية وتتطلب نوعين من الأدلة لمصادقة الفرد لتوفير طبقة إضافية من الأمان للمصادقة. بعض الأساليب الشائعة الأخرى للمصادقة ثنائية الاتجاه هي: بيانات المقاييس الحيوية والرمز المادي وما إلى ذلك والتي تُستخدم جنبًا إلى جنب مع اسم المستخدم وكلمة المرور (Pande, 2017).

التورية steganography

إنها تقنية لإخفاء الرسائل السرية في ملف مستند أو ملف صورة أو برنامج أو بروتوكول وما إلى ذلك بحيث تكون الرسالة المضمنة غير مرئية ويمكن استرجاعها باستخدام برنامج خاص. فقط المرسل والمتلقي يعرفان بوجود الرسالة السرية في الصورة. ميزة هذه التقنية هي أنه لا يسهل الشك في هذه الملفات (Mathe et al., 2012)

إرشادات لحماية جهاز الكمبيوتر من الفيروسات

أصبحت أجهزة الكمبيوتر معرضة في أي وقت لمخاطر الاختراق ودخول الفيروسات لنظام التشغيل بالرغم من التطور الهائل في أنظمة الحماية من الفيروسات، لذلك وضع المختصون عدة إرشادات ونصائح أساسية لحماية جهاز الكمبيوتر من الاختراقات (Easttom, 2019).

تثبيت برنامج مضاد للفيروسات Antivirus

هناك العديد من برامج مكافحة الفيروسات المتاحة لكن في بعض الأحيان قد يكون من الآمن لنا تنزيل أكثر من برنامج واحد إذا كان كل منها يغطي جوانب أمنية مختلفة، يمكن القول أنه ليست هناك حاجة لمكافحة الفيروسات طالما أننا لا نصل إلى الإنترنت من جهاز الكمبيوتر الخاص بنا. ومع ذلك، هذا ليس صحيحًا بالضرورة حيث يمكن أن تنتقل الفيروسات بين الأجهزة.

تشغيل الجدار الناري firewall

تقوم الجدران النارية بتصفية الحزم باتخاذ قرارات بناءً على عناوين IP وأرقام المنفذ ، حيث تتعامل عوامل تصفية الحزمة مع المواقف التي يُسمح فيها للعقدة الداخلية التي تفتح اتصالاً بشبكة جهاز التوجيه باستلام البيانات عبر هذا الاتصال. ويمكن إعادة توجيه رسالة معقمة إلى المتلقي (Gollmann, 2010).

تحديث نظام التشغيل

تتلقى برامج التشغيل عدة تحديثات غالبًا تكون تحديثات أمنية تحديثات متكررة تعزز الميزات الفردية. تتضمن هذه التحديثات أيضًا إجراءات أمنية تحافظ على أجهزة الكمبيوتر الخاصة بنا في مأمن من أحدث مجموعة من الفيروسات والبرامج الضارة التي يتم صنعها بواسطة مبرمجين يسعون لأهداف ضارة.

النسخ الاحتياطي

أحيانًا يتعذر علينا حذف فيروس أو برنامج ضار من أجهزة الكمبيوتر الخاصة، سنحتاج إلى إزالة بعض بياناتنا، قد يعني تلف الملفات من التعليمات البرمجية الضارة أنه يتعين علينا إعادة تهيئة محركات الأقراص الثابتة لدينا، بدون نسخة احتياطية ، لا توجد طريقة لاستعادة أي بيانات مفقودة. يعد هذا أكثر أهمية لأن محركات الأقراص الثابتة قد تتلف نفسها عن طريق الخطأ وتكلفنا ملفاتنا. ومع ذلك ، فإن النسخة الاحتياطية التي تحتوي على الفيروس والشفرة الضارة ستكرر فقط المشكلات التي واجهنا حتى لا نقوم بعمل نسخة احتياطية من البرامج الضارة (Ezekiel, 2012) .

مشاركة الملفات عبر الانترنت

يستمتع العديد من المستخدمين بمشاركة الملفات الرقمية مثل الموسيقى والأفلام والصور والبرامج. غالبًا ما تكون برامج مشاركة الملفات التي تصل جهاز الكمبيوتر الخاص بك بشبكة من أجهزة الكمبيوتر متاحة مجانًا. يمكن أن تشكل مشاركة الملفات عدة مخاطر. عند الاتصال بشبكة مشاركة الملفات، يمكن السماح للآخرين بنسخ الملفات التي لم تكن تنوي مشاركتها. قد تقوم بتنزيل فيروس أو جزء من برامج التجسس التي تجعل جهاز الكمبيوتر الخاص بك عرضة للمتسللين، كما يمكنك انتهاك القانون عن طريق تنزيل مواد محمية بحقوق الطبع والنشر (Shih and Chiang, 2004)

الخاتمة

من خلال هذا البحث يمكننا أن نستنتج أنه: من الضروريات التثقيف عن مجال أمن المعلومات، فقد يحتاج المستخدمون إلى تثقيفهم بشكل منتظم حول التهديدات الأمنية المشتركة ووسائل الأمان، إذ يتطلب المستخدمون الدراية الكاملة حول وسائل الأمن الإليكتروني وكيفية التعامل مع المرفقات عبر الإنترنت.

المراجع

دخيل, أحمد نوري, طلحة & ,سعد عبدالسلام. (2016). اختراقات أمن المعلومات وطرق تفاديها.

فايد، هشام محمد. (1990). التطبيقات المتخصصة لاستخدام الحاسب الآلي. *الهيئة العامة لمكتبة الاسكندرية*. (1).

قطوش إسلام & ,شرف الدين. (2019 .(*واقع القرصنة الإلكترونية من خلال التحقيق الصحفي* (Doctoral dissertation, جامعة محمد بوضياف بالمسيلة كلية العلوم الانسانية والاجتماعية.

المتولي محمد محمد عامر, م., محمد, عبدالسميع, مصطفى, عبدالفتاح سويدان, & محمد أمين. (2014). أثر استخدام برامج الوسائط المتعددة علي التحصيل الدراسي لدي طلاب كليات التربية. *مجلة بحوث التربية النوعية*، 2014(35)، 606-646.

Al Daoud, E., Jebril, I. H., & Zaqaibeh, B. (2008). Computer virus strategies and detection methods. *Int. J. Open Problems Compt. Math*, *1*(2), 12-20.

Al-Saadoon, G., & Al-Bayatti, H. M. (2011). A comparison of trojan virus behavior in Linux and Windows operating systems. *arXiv preprint arXiv:1105.1234*.

Chen, T. M., & Robert, J. M. (2004). The evolution of viruses and worms. In *Statistical methods in computer security* (pp. 289-310). CRC press.

Choudhary, S., Saroha, R., & Beniwal, M. S. (2013). How Anti-virus Software Works??. *International Journal*, *3*(4).

Durkota, M. D., & Dormann, W. (2008). Recovering from a trojan horse or virus. *White Paper). United States Computer Emergency Readiness Team*.

Easttom, C. (2019). *Computer security fundamentals*. Pearson IT Certification.

Ezekiel, A. W. (2012). Hackers, spies, and stolen secrets: Protecting law firms from data theft. *Harv. JL & Tech.*, *26*, 649.

Fatima, U., Ali, M., Ahmed, N., & Rafiq, M. (2018). Numerical modeling of susceptible latent breaking-out quarantine computer virus epidemic dynamics. *Heliyon*, *4*(5), e00631.

Ghandorh, H., Noorwali, A., Nassif, A. B., Capretz, L. F., & Eagleson, R. (2020, February). A Systematic Literature Review for Software Portability Measurement: Preliminary Results. In *Proceedings of the 2020 9th International Conference on Software and Computer Applications* (pp. 152-157).

Gollmann, D. (2010). Computer security. *Wiley Interdisciplinary Reviews: Computational Statistics*, *2*(5), 544-554.

Han, L., Han, S., Deng, Q., Yu, J., & He, Y. (2008). Source tracing and pursuing of network virus. In *2008 IEEE 8th International Conference on Computer and Information Technology Workshops* (pp. 230-235). IEEE.

Hindle, A., Barr, E. T., Gabel, M., Su, Z., & Devanbu, P. (2016). On the naturalness of software. *Communications of the ACM*, *59*(5), 122-131.

Horton, J., & Seberry, J. (1997). Computer Viruses An Introduction.

Ikekonwu, G. A., & Bakpo, F. S. (2005). Petri Net Modeling of Computer Virus Life Cycle. *Nigerian Journal of technology*, *24*(1), 87-92.

Jabar Al-Atabi, Akram & Al-Noori, Bushra. (2020). E-Learning In Teaching. *Researchgate*. https://www.researchgate.net/publication/341684491_E-Learning_In_Teaching

Jaiswal, M. (2017). Computer Viruses: Principles of Exertion, Occurrence and Awareness. *International Journal of Creative Research Thoughts (IJCRT)*, 648-651.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993.

Jupin, J. A., Sutikno, T., Ismail, M. A., Mohamad, M. S., Kasim, S., & Stiawan, D. (2019). Review of the machine learning methods in the classification of phishing attack. *Bulletin of Electrical Engineering and Informatics*, *8*(4), 1545-1555.

Khan, H. A., Syed, A., Mohammad, A., & Halgamuge, M. N. (2017, March). Computer virus and protection methods using lab analysis. In *2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA)* (pp. 882-886). IEEE.

Mathe, R., Atukuri, V., & Devireddy, S. K. (2012). Securing information: cryptography and steganography. *International Journal of Computer Science and Information Technologies*, *3*(3), 4251-4255.

McGuire, M. (2009). Programming Language Notes. *Researchgate*. https://www.researchgate.net/publication/228882836_Programming_Language_Notes

Mishra, U. (2010). An introduction to computer viruses. *Available at SSRN 1916631*.

Mishra, U. (2012). Detecting Boot Sector Viruses-Applying TRIZ to improve anti-virus programs. *Available at SSRN 1981886*.

Pande, J. (2017). Introduction to cyber security. *Technology*, *7*(1), 11-26.

Pavithra, A., Aathilingam, M., & Prakash, S. M. (2018). Multimedia and its applications. *International journal for research & development in technology*, 10(5), 271-276.

Rayini, J. (2017). Library and information services to the visually impaired persons. *Library Philosophy and Practice* (e-journal), 1510.

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering*, *7*(11), 125-128.

Shah, N., & Farik, M. (2017). Ransomware-Threats Vulnerabilities and Recommendations. *International Journal of Scientific & Technology Research*, *6*(06), 307-309.

Shih, D. H., & Chiang, H. S. (2004). E-mail viruses: how organizations can protect their e-mails. *Online Information Review*.

Spafford, E. H. (1990). Computer Viruses--A Form of Artificial Life?.

Wahahat, H. M., Alsmadi, T., & Ibrahim, Y. K. (2007). The Function Mechanism for a Selected Group of Macro Viruses. *IJCSNS, 7*(2), 339.

Wool, A. (2004). A quantitative study of firewall configuration errors. *Computer*, *37*(6), 62-67.

Xavier, U. H. R., & Pati, B. P. (2012, November). Study of internet security threats among home users. In *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)* (pp. 217-221). IEEE.