وزارة التعليم العالي والبحث العلمي

جامعة الفرات الاوسط

المعهد التقني /السماوة

قسم تكنولوجيا المعلومات والاتصالات

مدرس المادة :م.م بيداء هادي محمد سعودي

المحاضرة الرابعة

أمنية الحاسبات والبيانات

COMPUTER & DATA SECURITY

خصائص السياسة الامنية

Features of security Policy

هناك أربع خصائص رئيسية لاي سياسة أمنية فعالة يمكن تلخيصها كالتالي:

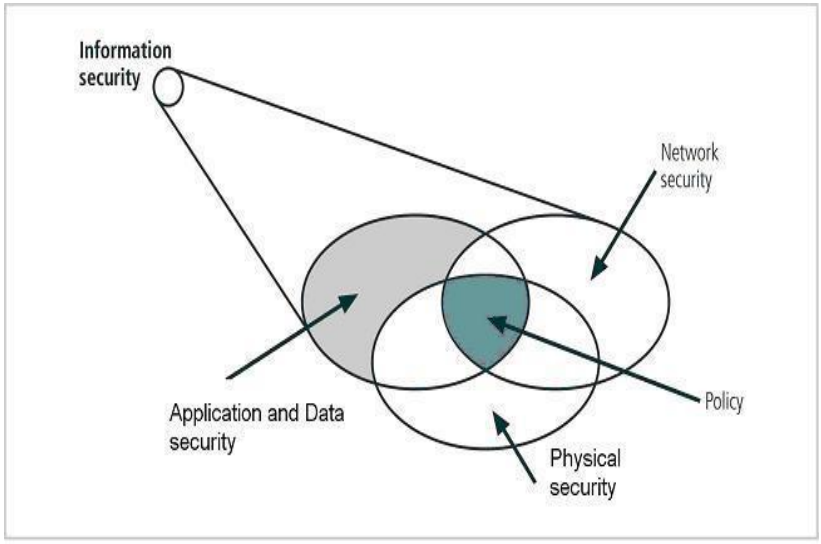
أولا: يجب أن تضع السياسة الامنية إطارا قويا للبرنامج الامني، يتضمن تفاصيل شاملة للمعايير والإجراءات التقنية.

ثانياً: يجب أن تضع هذه السياسة تفاصيل توثيق السياسة وانتشارها، مع ضمان فهم المعنيين داخل المؤسسة وخارجها للسياسة وكيفية تحديدها لمسؤولياتهم

ثالثًا: إضافة إلى ذلك، من مزايا السياسة الامنية الهامة الاخرى مراقبة التهديدات الناشئة والتعامل معها لضمان تطور السياسة والحلول التي تستند إليها أيضا.

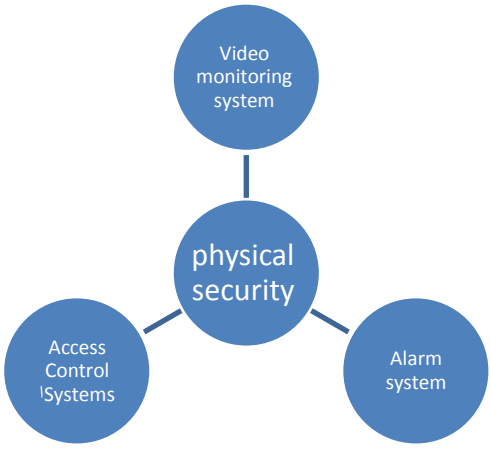
رابعاً وأخيرا: فان السياسة الامنية الفعالة يجب أن توفر الدليل لضمان أن جميع الأنظمة متوافقة وملتزمة بالسياسة الامنية والتعليمات.

مما سبق لضمان أمن المعلومات لابد من تطبيق سياسة أمنية متكاملة تضمن مايلي:
١ـ الامن المادي للمؤسسة و محتوياتها
٢ـ أمن الشبكات والاتصالات
٣ـأمن التطبيقات والمعطيات



الامن المادي

يتضمن الامن المادي عدة أنظمة تتكامل فيما بينها لتحقيق الحماية الفزيائية و هي



:

اولا:انظمة التحكم بالدخول Access Control Systems

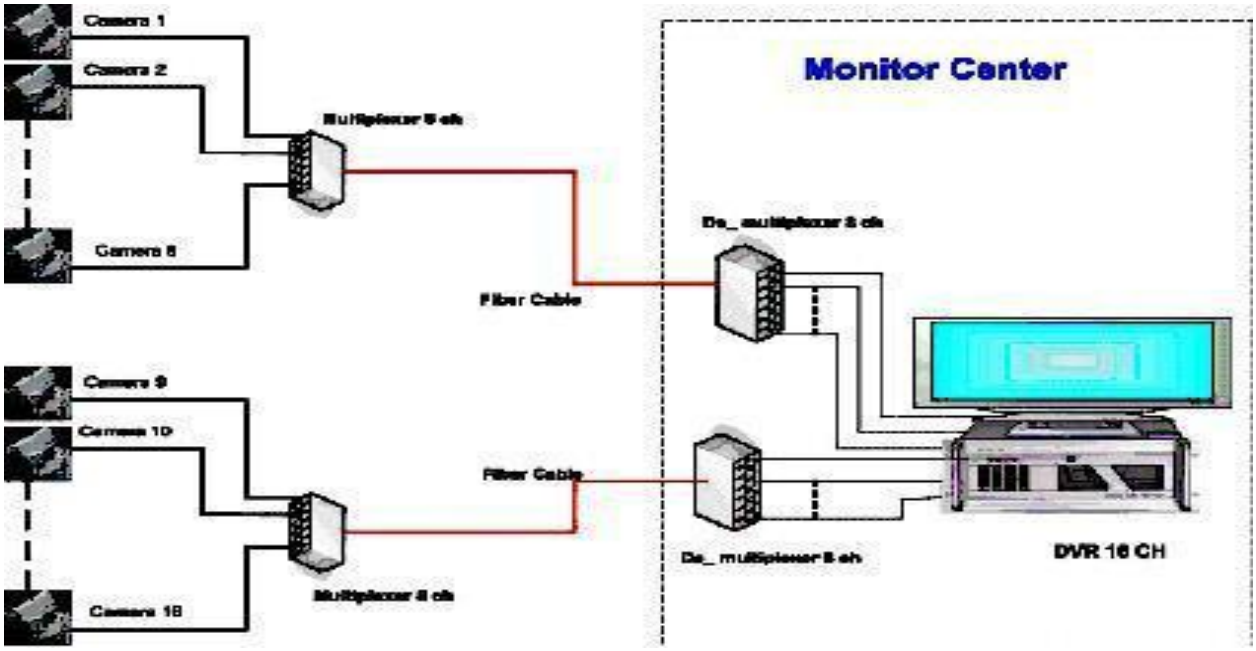
هناك العديد من تقنيات التحكم بالدخول سواء بالدخول إلى المباني أو الدخول إلى الحواسيب ،تعتمد أنظمة التحكم بالدخول إلى المباني والغرف حالياً على الاقفال المبرمجة لفتح أو إقفال البوابات في المباني أو العربات وذلك عن طريق قارئات
تقوم بالتحقق من الشخص المخوَّل للدخول أو الخروج وإعطاء الأوامر للأقفال بفتح هذا الباب أو إغلاقه .
ويمكن أن تكون هذه القارئات تقليدية تعتمد على رقم سري للدخول أو بطاقة (مغناطسية- شريط مرمز- ذكية) أو يمكن أن تكون قارئات متطورة تعتمد على مطابقة الصفات الحيوية لأشخاص)شكل الوجه، بصمة الأصبع، بصمة اليد، قزحية العين، الصوت أو مركبة المورثات (DNA.
ترتبط هذه القارئات بنظام مراقبة مركزي تسمح للمسؤول عن حماية النظام والمنشاة مراجعة قواعد البيانات ومعرفة حركة الدخول والخروج في كافة أماكن وغرف المنشأة.

ثانياً :أنظمة المراقبة المرئية Video monitoring system

تعتمد هذه الأنظمة على كاميرات المراقبة وملحقاتها من أجهزة تسجيل وتحكم، فتوضع الكاميرات بما يتناسب مع الموقع المراد مراقبته من حيث القطاع وشدة الإضاءة. ويمكن أن تكون هذه الكاميرات ثابتة أو متحركة، ويمكن أن تكون مصمَّمة لمراقبة المواقع داخل مبنى أو خارجه .
ويوجد تقنيتان في كاميرات المراقبة :

١ـ الكاميرات التمثيلية CCTV أنظمة الدارات التلفزية المغلقة

توصل الكاميرا بكيبل مخصصة لنقل إشارة الفيديو من الكاميرا إلى جهاز التسجيل الرقمي الذي يمكن أن يكون جهازاً خارجياً مستقلاً أو بطاقةً Digital Video Recoder (DVR) تحصيل تركب في أحد الحواسب . ويبين الشكل التالي مخطط ربط كاميرات عن طريق كبالٍ ضوئية



2-IP cameraكاميرات عبر الشبكة الحاسوبية

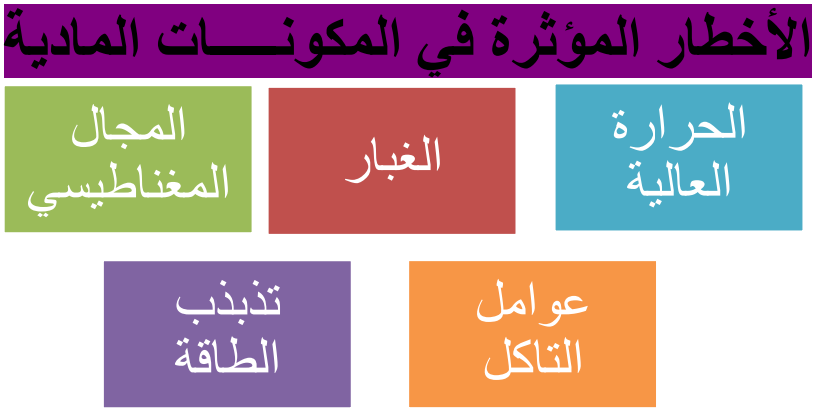
توصَل مباشرة إلى الشبكة الحاسوبية الموجودة، ويكون لهذه الكاميرات عنوان يولج إليها أو للتحكم عن طريق هذا العنوان وضمن IP Addressشبكي خاص سماحيات وطرق ولوج محددة

ثالثاً : أنظمة الانذار Alarm system

تعتمد هذه الأنظمة على توزيع مجسات تقوم بمراقبة خصائص معينة وإعطاء الإنذارات عند مستويات محددة لاعطاء الإنذارات المناسبة عند حدوث خطر معين في المبنى ويمكن استخدام :

مجسات الحريق، مجسات الدخان، مجسات الحرارة، مجسات الرطوبة، مجسات الضغط، مجسات الصوت أومجسات تغير التدفق كما يمكن أيضاً تصميم الأبنية والغرف السرية باستخدام جدران وأسقف وأرضيات من مواد معينة تكون مقاومةً للحريق والانفجار.

إن التكامل بين الأنظمة المستخدمة في الأمن المادي هو من الأمور الأساسية الواجب أخذها بعين الاعتبار في دراسة السياسة الأمنية للمؤسسة، كذلك تكامل هذه الأنظمة مع بقية التقانات الأمنية المستخدمة في أمن المعلومات Information Security للوصول إلى نظام أمني متكامل .



هناك الكثير من العوامل التي تعرض سلامة الحاسوب الشخصي للخطر والتي يمكن تصنيفها إلى :

١-الحرارة العالية

الحاسوب الشخصي شأنه شأن الأجهزة الكهربائية الأخرى، فيه الكثير من القطع التي تولد حرارة أثناء عملية التشغيل مما يؤدي إلى ارتفاع درجة الحرارة داخل الحاسوب بمعدلات أعلى من البيئة المحيطة له، لذا يتم تجهيز الحاسوب بمراوح داخلية تعمل مع بداية التشغيل، لغرض تقليل درجة الحرارة للمعدل المقبول، من خلال دفع الهواء الساخن الناتج عن ارتفاع درجة حرارة القطع والبطاقات الموجودة داخل علبة الحاسوب. وسحب تيار هواء بارد من المحيط الخارجي من خلال فتحات التهوية الموجودة في الأغطية الخارجية للعلبة. الا ان ارتفاع درجة الحرارة الخارجية إلى أكثر من المعدلات الموصى بها (١٦-٣٣ درجة مئوية). قد يؤدي إلى تضرر الحاسوب، وعليه يجب اتخاذ الإجراءات الآتية للمحافظة على الحاسوب:

أ.التأكد من وضع الحاسوب في المواضع التي تسمح للهواء بالمرور إلى داخل علبة الحاسوب من خلال فتحات التهوية.

ب. تجنب تشغيل الحاسوب عندما ترتفع درجة حرارة الغرفة إلى أكثر من (٣٣) درجة، في حال تعطل أجهزة التكيف.

ت. الفحص المستمر للمراوح الداخلية والتأكد من عملها بشكل صحيح. خاصة المروحة المخصصة للمعالج ومجهز القدرة.

ث. تجنب وضع أجهزة تولد طاقة حرارية بالقرب من الحاسوب المستخدم. فضلا عن تجنب وضعه في مكان تصل إليه أشعة الشمس بشكل مباشر.

ج. و لزيادة الأمان نقوم باضافة بطاقات أو دارات متحسسة للحرارة تركب داخل الحاسوب وتطلق إشارة إنذار عند ارتفاع درجة الحرارة لحد معين خارج الحد المسموح به.

٢-الغبار

يتألف الغبار من ذرات رمل صغيرة ومواد أخرى عضوية، ويسبب عدة مشاكل للمكونات الداخلية للحاسوب الشخصي، مع ملاحظة ان تشغيل الحاسوب، سيؤدي إلى وجود شحنة كهربائية تولد مجال مغناطيسي يؤدي إلى جذب الغبار والاتربة إلى داخل علبة الحاسوب، فضلا عن ان عمل المراوح الداخلية يؤدي إلى تكوين تيار هواء يسحب معه الغبار إلى داخل علبة الحاسوب.

ان هذا الغبار يمكن ان يؤدي إلى:

أ. تراكم ذرات الغبار على الدارات داخل الحاسوب يودي إلى تشكيل طبقة عازلة حرارياً وهذا يقلل من تبديد الحاسوب للحرارة الناتجة

ب. يسد الغبار منطقة امتصاص الهواء في وحدة امداد بالطاقة و القرص الصلب.
ت. ولتجنب هذه المشاكل يراعى وضع الحاسوب في الغرف والقاعات التي يتم تكيفها باستخدام أجهزة التكيف ، ولايتم فتح النوافذ لمنع دخول الغبار .
كما يفضل وضع الحواسيب ،وضع الحواسيب في مؤسسات في القاعات التي لايستخدم السجاد في تغطية ارضيتها .ومن المفيد دائما تنظيف الحواسيب باستخدام اجهزة نفخ الهواء كل سنة مرة على الاقل

٣- المجال المغناطيسي
معظم الاجهزة الكهربائية تولد مجال مغناطيسي عند تشغيلها، ولكن بحدود قليلة نسبيا، لكن في حال تعرض الحاسوب الشخصية إلى مجال مغناطيسي عالي، فان المكونات الممغنطة فيه مثل القرص الصلب او الاقراص المرنة قد تتأثر، ويتم فقد المعلومات المخزنة عليها

وهو ضرر قد يحدث في حال تمرير الاقراص المرنة او أجهزة الحاسوب الشخصية في (المحمول). أجهزة فحص الامتعة في المطارات والمناطق الحساسة الاخرى.لذا يفضل دائما استخدام الاقراص الليزرية في تخزين نسخ من البيانات والمعلومات في حال وجود تنفيذ عملية فحص الاجهزة في اماكن المشار اليها.

٤- تذبذب الطاقة
يعتبرمقبس الطاقة الجداري مصدراً لكثير من المشاكل التي في المكونات المادية للحواسيب، إذ تصنف تأثيرات مصدر الطاقة إلى:
أ-المشاكل الناتجة عنن ازياد الجهد وانخفاض الجهد(تذبذب التيار) إن انخفاض الجهد يؤدي إلى زيادة التيار المستهلك وهذا بدوره يؤدي إلى زيادة القواطع الكهربائية والتوصيلات مما يؤدي إلى ارتفاع حرارةوحدة الامداد بالطاقة وكذلك الرقائق ويمكن حل .هذه المشكلة بالاستعانة بأجهزة تنظيم الكهرباء
ب- المشاكل الناتجة عن غياب الجهد نهائيا
.والتي تؤدي إلى توقف التشغيل في بعض المكونات، واستمراره في مكونات أخرى.
ت-المشاكل الناتجة عن العبور
العبور هو عبارة عن تغير طفيف في الطاقة لايمكن أنه يكرر نفسه مرة أخرى ويأتي على شكل انخفاض في الجهد أو ارتفاع في الجهد
فاذا امتلك العبور ترددا كافياً عطل مكثفات الحماية وعناصر أخرى لوحدة الامداد بالطاقة كما أن الجهد يؤدي إلى نفس الاضرار وتعطيل رقائق الحاسوب تشغيل الطاقة أو اندفاع الطاقة
ث- المشاكل الناتجة عن عملية تفريغ الكهرباء الساكنة، جسم الانسان قابل أن يشحن بشحنة ساكنة وقد تصل إلى حوالي٥٠ ألف فولت ويكفي ٢٠٠ فولت لافساد الرقائق الكترونية لذلك قبل البدء بأي عملية صيانة يجب تفريغ الشحنة التي تحملها بواسطة لمس أشياء معدنية ويمكن تجنب مشكلة الكهرباء من خلال رطوبة الجوبواسطة اجهزة زيادة الرطوبة او زيادة رطوبة الجو عن طريق اقتناء نباتات الزينة واحواض الاسماك

٥-عوامل التأكل
يعد الماء والاملاح من المواد الخطرة على الحاسوب ويجب تجنيب الحاسوب الأشياء التالية:

أ.انسكاب الماء او إي سوائل أخرى غير المقصود
ب.الترشيح الناتج عن تسرب المياه الرطبة إلى داخل الحاسوب
ت.فيضان المياه ودخول الماء إلى الحاسوب
ث. يعد التآكل عمل اخر من عوامل الأضرار بالأجهزة نتيجة تراكم الاملاح بسب تعرق جسم الانسان، و تراكم الاحماض الكبريتية الناتجة عن النقل بواسطة الطائرات

ج. إن المشكلة الكبرى التي نتعرض لها هي أكسدة نقاط الدارات وبالتالي تفقد وظيفتها في وصل الدارات ببعضها، وبالتالي تعطل الحاسوب

لهذا السبب، يجب توخي الحذر عند التعامل مع بطاقات الدارات وعدم لمس أقطابها خوفًا من تأثير الاملاح الناتجة عن التعرق

البيئة المناسبة لعمل الحاسوب

يجب ملاحظة بعض الامور لجعل البيئة المحيطة بالحاسوب مناسبة للتشغيل وتحقق مستوى امان مناسب للحفاظ على الجهاز ومن هذه الامور ,وتحقق مستوى امان مناسب

أ. تأكد من تأمين شروط حماية الطاقة الكهربائية .وذلك بعندم ربط الحاسوب مباشرة إلى مصدر طاقة، وذلك بعدم ربط الحاسوب مباشرة الى مصدر طاقة وإنما يفضل استخدام جهاز حماية UPS.

ب. يفضل عدم مشاركة الحاسوب لاي جهاز كهربائي اخر على نفس مصدر الطاقة.

ت. لا يفضل تشغل محركات ضخمة على نفس خط الطاقة الذي يغذي الحاسوب .

ث. إبعاد الحاسوب عن مصادر الضجيج .

ج. حافظ على مستوى معتدل لدرجة حرارة الغرفة.

ح..يساعد إبقاء الحاسوب في حالة عمل دائم على ضبط حرارة الحاسوب الداخلية بشكل جيد .

خ.تأكد من عدم وجود أي مصدر للاهتزاز على نفس الطاولة .التي يوجد عليها الحاسوب.

د.الحرص عنى تعميم إجراءات السلامة تلك على جميع العاملين في مؤسسات المعلومات الذين يستخدمون الحاسوب.

أهم الاخطار التي تهدد بيئة المعلومات الرقمية وكيفية تجنبها،و وسائل الحماية المناسبة لتأمينها.

اولا :الفيروساتvirus

فيروس الحاسوب، هو برنامج خارجي، تنم تطويره من قبل مبرمجين محترفين، لغرض إلحاق الضرر في الحواسيب من خلال تغيير خصائص الملفات التي يصيبها، لتقوم بتنفيذ بعن الأوامر إما بالازالة أو التعديل أو التخريب و ما شابهها من عمليات. أي ان فيروسات الحواسيب هي برامج تتم كتابتها بغرض إلحاق الضرر بحاسوب آخر، أو السيطرة عليه.

سمي الفيروس(Virus) بهذا الاسم لتشابه آلية عمله مع تلك التي تصيب الكائنات الحية، بعدد منن الخصائص، كخاصية انتقال بالعدوى، أو كونه كائنا غريبا يقوم بتغيير حالة الكائن المصاب، إضافة إلى الضرر الذي يعقبه إن لم يتم العلاج. سُميت بالفيروسات، لانها تشبه تلك الكائنات المتطفلة في صفتين رئيسيتين:

الصفة الأولى تحتاج فيروسات الحاسوب دائماً إلى ملف عائل تعيش متستّرةً فيه. فالفيروسات دائماً تستر خلف ملف آخر، ولكنها تأخذ زمام السيطرة على البرنامج المصاب. بحيث أنه حنين ينتم تشغيل البرنامج المصاب، يتم تشغيل الفيروس ايضا تشبه بطريقه هذه الفيروسات ألبيولوجيه حيث لايستطيع أي فيروس العيش بدون إصابته لخليه في جسم الكائن الحي(بدون الخلية يتلف الفيروس ويتلاشى) .

الصفة الثانية انتقالها يشبه طريقة انتقال الفيروسات البيولوجية حيث تتواجد الفيروسات في مكان أساسي في الحاسب كالذاكرة رام مثال، وتصيب أي ملف يشغل في أثناء وجودها بالذاكرة مما يزيد عدد الملفات المصابة،كلما تأخر وقت اكتشاف الفيروس(كما الفيروس البيولوجي بعد استنزافه للخلية الحية يندمرها ويتكاثر في خلايا اخرى .ويمكن الاحساس بوجود الفيروس فني جهاز الحاسوب من خلال سلسلة منن الاعراض التي تظهر عند الاستخدام ومنها على سبيل المثال:

- **تكرار رسائل الخطأ في أكثر من برنامج.**
- **ظهور رسالة تعذر الحفظ لعدم كفاية المساحة.**
- **تكرار اختفاء بعض الملفات التنفيذية.**
- **حدوث بطء شديد في إقالع نظام التشغيل أو تنفيذ بع التطبيقات.**
- **رفض بعض التطبيقات للتنفيذ.**

انواع الفيروسات

ان أهداف الفيروسات في الغالب تكون مختلفة، وحجم الضرر الذي يمكن ان تلحقه يتباين بين التدمير الشامل الى مجرد الازعاج، وبشكل عام يمكن تصنيف الفيروسات الى ثلاث أصناف على اساس سلوكها في إحداث الضرر في المعلومات وكلاتي:

١-الفيروس

يمكن القول بأنه برنامج تنفيذي يعمل بشكل منفصل ويهدف إلى إحداث خلل في نظام الحاسوب وتتراوح خطورته حسب مهمته فمنه الخبيث الذي قد يؤدي الى إبطال عمل الحاسوب تماما، ومنه المنزعج الذي لا يحدث ضرر كبير ولايؤثر في المعلومات، لكنه يشكل مصدر إزعاج مستمر لمستخدم الحاسوب، مثل تغير اللغة او لون الشاشة او ان يكرر نفسه في مواضع خزنية مختلفة.

٢- الدودة (worm)

هي فيروس ينتشر عبر الشبكات والأنترنت ، عن طريق دفتر عناوين البريد الإلكتروني غالبا، فعند إصابة الجهاز يبحث البرنامج الخبيث عن عناوين الاشخاص المسجلين في دفتر العناوين على سبيل المثال ويرسل نفسه إلى كل شخص وهكذا ... مما يؤدي إلى انتشاره بسرعة عبر الشبكة وقد اختلف الخبراء فمنهم اعتبره فيروس ومنهم من اعتبره برنامج خبيث وذلك كون الدودة ال تنفذ أي عمل مؤذي إنما تنتشر فقط. مما يؤدي إلى إشغال موارد الشبكة بشكل كبير. ومع التطور الحاصل في ميدان الحوسبة أصبح بامكان المبرمجين الخبيثين إضافة سطر برمجي لملف الدودة بحيث تؤدي عمل معين بعد انتشارها ، مثلا بعد الانتشار إلى عدد ٥٠٠٠٠ جهاز يتم تخريب الأنظمة في هذه الأجهزة) او إي شي اخر (مثلا في يوم معين او ساعة او تاريخ...الخ)وأصبح الديدان من أشهر الفيروسات على الشبكة العالمية وأشهر عملياتها التخريبية وأخطرها تلك التي يكون هدفها حجب الخدمة تسمـــى (هجمات حجب الخدمة) حيث تنتشر الدودة على عدد كبير من الأجهزة ثم توجه طلبات وهميه لجاهز خادم معين) يكون المبرمج قد حدد الخادم المستهدف من خلال برمجته للدودة (فيغرق الخادم بكثرة الطلبات الوهمية ولا يستطيع معالجتها جميعا مما يسبب توقفه عن العمل. وهذه الديدان استهدف مواقع لكثير من الشركات العالمية أشهرها مايكروسوفت .

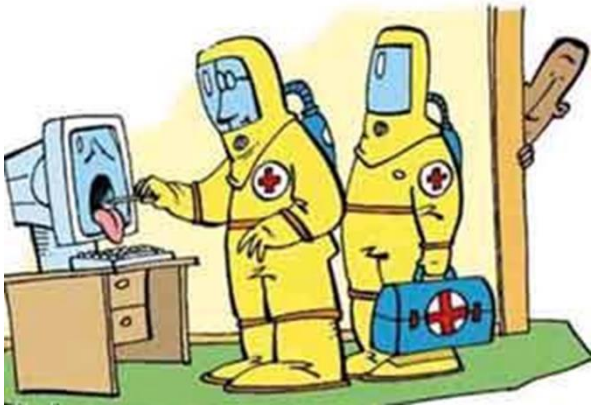
٣-حصان طروادة Trojan Horse

سمي هذا الفيروس بحصان طروادة ألنه يذكر بالقصة الشهيرة لحصان طروادة، حيث اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها، وهكذا تكون آلية عمل هذا الفيروس، حيث يكون مرفقا مع أحد البرامج أي يكون جزء من برنامج ما دون ان يعلم المستخدم. فعندما يبدأ البرنامج تنفيذ عمله ويصل إلى مرحلة ما يبدأ الفيروس العمل والتخريب. وقد لايكون هدف الفيروس التخريب هنا قد يكون هدفه ربحي مثل القرصنة على الحسابات المصرفية والكشف عن كلمات المرور.

عموما توجد عدة تصنيفات اخرى للفيروسات ، فمثالً من حيث سرعة الانتشار هناك فيروسات سريعة الانتشار،وفيروسات بطيئة الانتشار ومن حيث توقي النشاط ،فيروسات تنشط في أوقات محددة وفيروسات دائمة النشاط، ومن حيث مكان الإصابة فيروسات مقطع التشغيل boot sector على الأقراص وهي الأكثر شيوعاً، وفيروسات الماكرو macro التي تختص باصابة الوثائق والبيانات الناتجة عن حزمة مايكروسوفت أوفيس، أمنا من حيث حجم الضرر فهناك الفيروسات المدمرة للأجهزة التي تعطل الذاكرة روم في الحاسب كما في فيروس تشرنوبل، او ان يمحي معلومات ال MBR على القرص الصلب فتعود الأقراص الصلبة كما خالية، وفي الحالتين السابقتين لايتم إقلاع الجهاز مما يوحي للبعض ان الفيروس قد أعطب الجهاز. ومن المخاطر المحتملة للفيروسات على حواسيب مؤسسات المعلومات، إنها تتسبب في إتلاف البيانات المخزنة والتي قد تكون)البيانات(انتاج عشرات

السنين مما يؤدي إلى خسائر جسيمة او إلى توقف الحاسبات عنن العمل وبالتالي توقف الخدمات المقدمة للمستفيدين.

وسائل الحماية من الفيروسات



حماية الحاسوب الشخصي من الاصابة بالفيروسات تبدو مهمة شبه مستحيلة، خاصة عندما يكون الحاسوب مرتبط بشبكة الأنترنت ، وعلى العاملين في مؤسسات المعلومات إدراك هذه الحقيقة، والتعاطي معها كي لا يتم هدر الجهد الكبير الذي بذل في بناء محتوى قواعد المعلومات الخاصة بالمؤسسة. وعليه هناك العديد من وسائل الحماية، التي يمكن اتخاذها للحد من خطر الإصابة بالفيروسات وتقليل أثارها الى ادنى حد ممكن.

وقبل ان نناقش هذه الوسائل يجب التعرف على طرائق انتقال الفيروس الى الحاسوب الشخصي. والتي يمكن ان تكون عن طريق استخدام الأقراص المرنة في نقل الملفات، او الأقراص المدمجة المنسوخة، او الذاكرة الضوئية، او مرفقات رسائل البريد الإلكتروني، او المواقع الاباحية. فضلا عنن ذلك فان ذاكرة أجهزة الهاتف المحمول في حال تعريفها الى جهاز الحاسوب تعد طريقة اخرى لنقل الفيروسات منع وجود تقنية البلوتوث. وقد تلجأ بعض شركات البرمجيات الى استخدام الفيروس وسيلة لحماية منتجاتها البرمجية من النسخ والتقليد. وأمام هذه الطرائق المتعدد لانتقال الفيروسات، نؤكد القول السابق ان المهمة تكاد تكون شبه مستحيلة للحفاظ على الحاسوب من خطر الإصابة، لكن يمكن الحد منها وتقليل أثارها باستخدام وسائل الحماية الآتية:

١-تنصيب برامج مكافحة الفيروسات (Antivirus) والتركيز على الإصدارات العالمية المعروفة بكفاءتها. وتجنب استخدام الإصدارات المستنسخة. او تحميلها من خارج مواقعها الرسمية على الإنترنت .

٢-التحديث المستمر لقاعدة بيانات برامج مكافحة الفيروسات، من خلال شبكة الإنترنت .

٣-تجنب تنصيب بعض برامج مكافحة الفيروسات المعروضة مجانا على الإنترنت ، او تجربتها.

٤-منع استخدام الحاسوب الشخصي خارج الأغراض المخصص لها في مؤسسة المعلومات. وفي حال عدم الحاجة لاستخدام قارئ الأقراص المرنة، يفضل دائما فصله من داخل علبة الحاسوب.

٥-توعية العاملين في مؤسسة المعلومات بمخاطر الفيروسات وتأثيرها على المعلومات والبيانات.

وفي كل الأحوال ومع وجود إي وسائل للحماية، فان الضمان الحقيقي لمؤسسة المعلومات، هو في تنفيذ عملية النسخ الاحتياطي للبيانات والمعلومات، وحفظها على أقراص تخزين مدمجة خارج الحاسوب، لضمان اعادتها في حال الإصابة الشديد التي قد تتطلب عملية اعادة التهيئة.

ثانيا: الاختراق Penetration

معنى الاختراق بشكل عام، هو القدرة على الوصول لهدف معين بطريقة غير مشروعة، عنن طريق ثغرات في نظام الحماية الخاص بالهدف وبطبيعة الحال هي سمة سنية، يتسم بها المخترق لقدرته على دخول أجهزة االاخرين عنوه ودون رغبة منهم، وحتى دون علم منهم بغض النظر عن الاضرار الجسيمة التي قد يحدثها

سواء بأجهزتهم الشخصية او بنفسيتهم عند سحبة ملفات وصور تخصهم وحدهم . ولم تنتشر هذه الظاهرة لمجرد العبث وإن كان العبث وقضاء وقت الفراغ من أبرز العوامل التي ساهم في تطورها وبروزها الي عالم الوجود . وترتبط عمليات الاختراق بجملة من الدوافع نوجزها بالاتي:

١-الدافع السياسي والعسكري: مما الشك فيه أن التطور العلمي والتقني أديا الي الاعتماد بشكل شبة كامل على أنظمة الكمبيوتر في أغلب الاحتياجات التقنية والمعلوماتية. فمنذ الحرب الباردة والصراع ألمعلوماتي والتجسسي بين الدولتين العظمتين على أشده. ومنع بروز مناطق جديدة للصراع في العالم وتغير الطبيعة المعلوماتية لأنظمة والدول ، اصبح الاعتماد كليا على الحاسب الآلي، وعن طريقة اصبح الاختراق من اجل الحصول على معلومات سياسية وعسكرية واقتصادية مسالة أكثر أهمية.

٢ - الدافع التجاري: من المعروف أن الشركات التجارية الكبرى تعيش هي ايضا فيمنا بينها حربا مستعرة وقد بين الدراسات الحديثة أن عددا من كبريات الشركات التجارية يجرى عليها أكثر من خمسين محاولة إختراق لشبكاتها كل يوم. من قبل مبرمجين الشركات المنافسة او من قبل مبرمجين هواة بهدف الحصول على المعلومات وبيعها للشركات المنافسة.

٣-الدافع الشخصي: تتطلب عملية الاختراق ذكاء وقدرة برمجية عالية وهي سمة دفع العديد من الهواة فني تجريب قدرتهم واثبات مهاراتهم البرمجية من خلال القيام بعمليات الاختراق، وقد تطورت هذه الحالة إلى سلوك إجرامي في أحيان كثيرة.

٤-دوافع انتقامية. قد يلجأ بعد المبرمجين ممن يتم فصلهم من وظائفهم إلى الشعور بالظلم ومحاولة انتقام من المؤسسة التي سرحتهم باختراق أجهزتها واللحاق الضرر في معلوماتها.

انواع الاختراق

يمكن تقسيم الاختراق من حيث الطريقة المستخدمة الي ثالثة أقسام:

١- إختراق المزودات او الأجهزة الرئيسية.
للشركات والمؤسسات او الجهات الحكومية وذلك باختراق الجدران النارية التي عادة توضع لحمايتها وغالبا ما ينتم ذلك باستخدام المحاكاة Spoofing، وهو مصطلح يطلق على عملية انتحال شخصية للدخول الي النظام، حيث أن حزم الـ IP تحتوي على عناوين للمرسِل والمرسَل إليه، وهذه العناوين ينظر اليها على أنها عناوين مقبولة وسارية المفعول، من قبل البرامج وأجهزة الشبكة . ومن خلال طريقة تعرف بمسارات المصدر Source Routing فضن حزم الـ IP قد تم إعطائها شكال تبدو معه وكأنها قادمة من كمبيوتر معين بينما هي في حقيقة الامر ليس قادمة منه وعلى ذلك فان النظام إذا وثق بهوية عنوان مصدر الحزمة فانه يكون بذلك قد حوكي(خدع)وهذه الطريقة هي ذاتها التي نجح بها مخترقي الهوت ميل في الولوج الي معلومات النظام.

٢- إختراق الأجهزة الشخصية
والعبث بما تحويه من معلومات وهي طريقة للاسف شائعة لسذاجة أصحاب الاجهزة الشخصية من جانب ولسهولة تعلم برامج الاختراقات وتعددها من جانب اخر.

٣- التعرض للبيانات أثناء انتقالها
والتعرف على شفرتها إن كان مشفرة وهذه الطريقة تستخدم في كشف أرقام بطاقات الائتمان وكشف الارقام السرية للبطاقات المصرفية .ATM

ثالث: التجسس Espial

قد لا يختلف التجسس عن الاختراق الا في الهدف، وتبقى الاساليب المتبعة في تنفيذ عمليات الاختراق ذاتها تقريبا. لذا يمكن تعريف التجسس في مجال الحاسوب على انه، اختراق هادف يراد من خلاله تمكين المتجسس من التعرف على محتويات الحاسوب المستهدف، أول بأول دون الاضرار بها. وغالبا منا تتم عمليات التجسس باستخدام نوع من الفيروسات التي تنقل الى الحواسيب وتعمل على إرسال نسخ من البيانات والمعلومات الى حاسوب اخر، او تمكينه من الدخول الى الحاسوب والتعرف على محتوياته. وغالبا ما تتم عمليات التجسس الرقمي اذا صح التعبير، من خلال مؤسسات سواء كان مؤسسات حكومية، او غير حكومية، وفي كل الاحوال، يعد التجسس شأنه شأن الاخطار سابقة الذكر عمل غير مشروع. وسائل الاختراق لاغراض التجسس ومن النادر بالنسبة لاشخاص قليل الخبرة والمؤسسات الصغيرة ان تدرك اصابة بملفات التجسس،
كونها لا تؤدي الى حدوث أعراض محسوسة عند استخدام. وهناك عدة طرائق لتنفيذ عمليات الاختراق لاغراض التجسس يمكن إيجازها بالاتي:

١-ملفات أحصنة طروادة Trojan

لتحقيق نظرية الاختراق البد من توفر برنامج تجسسي يتم إرساله وزرعه من قبل المستفيد في جهاز الضحية ويعرف بالملف اللاصق ويسمى (الصامت) أحيانا وهو ملف باتش patch صغير الحجم مهمته الأساسية المبيت بجهاز الضحية (الخادم)وهو حلقة الوصل بينه وبين المخترق (المستفيد) . هذا الملف قد يحمل إي اسم، إلا ان اسم الجامع له على اساس الدور الذي يقوم به وطريقة تسلله إلى حاسوب (الضحية)هو(حصان طروادة)لانه يقوم بمقام الحصان الخشبي الشهير في الاسطورة المعروفة، و ربما يكون اكثر خبثا من الحصان الخشبي بالرواية، لانه حالما يدخل لجهاز الضحية يغير من هيئته فهو خلال فترة قصيرة يغير اسمه وبشكل مستمر . لهذا السبب تكمن خطورة أحصنه طروادة، فهي من جانب تدخل للأجهزة في صمت وهدوء، ومن جانب اخر ويصعب اكتشافها . فضلا عن ذلك فهي لاتترك إي علامات دالة على وجودها. و تتم عملية إرسال ملفات التجسس بعدة طرق من أشهرها:

- البريد الإلكتروني حيث يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر فيجد به برنامج الباتش المرسل فيظنه برنامجا مفيدا فيفتحه او أنه يفتحه بدافع الفضول فيكتشف انه لايعمل، منع هذه العملية يكون المخترق قد وضع قدمه الاولى بداخل الجهاز.

- تتم عمليه نقله عبر المحادثة من خلال برنامج الـ ICQ.
- -عن طريق إنزال بعض البرامج من المواقع الغير موثوق بها .
- كذلك يمكن اعادة تكوين حصان طروادة من خلال الماكرو الموجودة ببرامج معالجات النصوص.

٢-بوابات الاتصال Contacting Gates

يتم الاتصال بين أجهزة الحواسيب عبر بوابات ports او منافذ اتصال وهذه المنافذ في واقع الامر هي جزء من الذاكرة له عنوان معين يتعرف علية الجهاز بأنه منطقة اتصال يتم من خلاله إرسال واستقبال البيانات ويمكن استخدام عدد كبير من المنافذ للاتصال، إذ يزيد عن ٦٥٠٠٠ويميز كل منفذ عن الاخر رقمه، فمثال المنفذ رقم ١٠٠١ يمكن إجراء اتصال عن طريقة وفي نفس اللحظة يتم استخدام المنفذ رقم ٢٠٠١ لاجراء اتصال اخر. من خلال هذه البوابات يتم زرع ملف الباتش في الحاسوب الضحية ليؤدي الدور المطلوب منه في تنفيذ عملية التجسس. ملف الباتش به ورغم خطورة وجود بجهاز الضحية فأنه يبقى في حالة خمول طالما لم يطلب منه المخترق التحرك . ولكن بدونه لا يتمكن المخترق من السيطرة على جهاز الضحية عنن بعد، وحتى يتم له ذلك، فان على المخترق بناء حلقة وصل متينة بينه وبين الخادم عن طريق برامج خاصة تعرف ببرامج الاختراق .

٣-عن طريق الـ IP Address

ذكرنا سابقا بأن ملفات الباتش الحاملة لاحصنة طروادة هي حلقة الوصل بين المخترق والضحية ، ولكن في واقع الامر فان ملفات الباتش ليس إلا طريقة واحدة لتحقيق التواصل . عند اتصالك بالأنترنت تكون معرض لكشف الكثير من المعلومات عنك، كعنوان جهازك وموقعه ومزود الخدمة الخاص بك وتسجيل كثير من تحركاتك على الشبكة. و كثيرا من المواقع التي تزورها تفتح سجلا خاصا بك يتضمن عنوان الموقع الذي جئت منه IP Address ونوع الحاسوب والمتصفح الذي استخدمته بل وحتى نوع معالج جهازك وسرعته ومواصفات شاشاتك وتفاصيل كثيرة. مبدئيا عنوانك الخاص بالأنترنت Internet Protocol او IP يكشف الكثير عنك فكل جهاز متصل بالشبكة يكون له رقم معين خاص به يعرف باسم الـ IP Address . وباختصار يكون الـ IP كرقم هوية خاص بكل من يعمل على الإنترنت . ومن خلاله يتمكن المخترق المحترف من الولوج الى الجهاز والسيطرة عليه خلال الفترة التي يكون فيها الضحية متصلا بالشبكة فقط ، ولكن هذا الخيار لايخدم المخترق كثيرا لا السيرفر الخاص بمزود الخدمة يقوم بتغيير رقم الـ IP الخاص بالمشترك تلقائيا عند كل عملية دخول للشبكة .

٤-عن طريق الكوكي Cookie

يمكن ايضا تحقيق التواصل للاختراق عن طريق الكوكي Cookie وهي عبارة عن ملف صغير، تضعه بعض المواقع التي يزورها المستخدم على قرصه الصلب. هذا الملف به آليات تمكن الموقع الذي يتبع له جمع وتخزين بعض البيانات عن الجهاز، وعدد المرات التي زار المستخدم فيها الموقع، كما وأنها تسرع عمليات نقل البيانات
بين جهاز المستخدم والموقع فالهدف الاساسي منها هو تجاري أصلا. ولكنه يساء استخدامه من قبل بعض المبرمجين المتمرسين بلغة الجافا Java فهذه اللغة لديها قدرات عالية للتعمق اكثر لداخل الاجهزة والحصول على معلومات اكثر عن المستخدم.
وبعد فان آلية الاختراق تتم مبدئيا بوضع برنامج الخادم بجهاز الضحية ويتم الاتصال به عبر المنفذ port الذي فتحة للمستفيد)المخترق(في الطرف الاخر ولكن حلقة الوصل هذه تنقصها المعابر وهي البرامج المخصصة للاختراق .
بعد التعرف على طرائق المتجسس في زرع ملف التجسس، يبقى ان نقول انه من حسن الحظ ان برامج مكافحة الفيروسات تتعامل مع ملفات أحصنة طروادة على إنها فيروسات قادرة على إزالتها، اذا تم تحديثها بشكل مستمر. ولكن دائما نؤكد على ان الوقاية خير من العلاج، ولان البريد الإلكتروني هو من اكثر الطرق التي يختارها المتجسسين للوصول الى الحواسيب لذا ينصح التعامل مع الرسائل التي نستلمها بحذر شديد ونتجنب فنتح إي رسالة ال نعرف مصدرها مهما حمل من إغراءات، خاصة الملفات المرفقة، فملفات أحصنة طروادة لاتعمل ما لم يتم فتح الرسالة المرفقة. لذا فان حذف الرسالة هو الطريقة المثلى للتخلص من هكذا ملفات.

رابعا: البرامج الضارة - Harmful Software

الاختراق ليس الا احد انواع التدمير الممكنة عبر البرامج المؤذية ، لذلك فالمخاطر التي يتعرض لهنا مستخدم الحاسوب العادي تتنوع بتنوع واختلاف البرامج المؤذية وإمكاناتها. وإن كان الاختراق هو أخطرها وأبرزها. إذ تتراوح المخاطر التي يتعرض لها المستخدم من مجرد إزعاج بسيط الي مستوى الكارثة وقد صنف هذه المخاطر الي أربعة أصناف:

١- القنابل وبرامج الطوفان Flooders/Bombers حيث يفاجأ المستخدم بوجود مئات الرسائل في عنوانه الإلكتروني او عبر برنامج الـ ICQ من أشخاص وعناوين لم يسمع بهم من قبل وهذا الصنف من المخاطر هو الاقل خطورة حيث انه يسبب إزعاجا على حساب وق المستخدم .

٢- الخداع .Spoofing وهو عملية تمويه وطمس للهويه حيث تتم سرقة حساب الدخول للا نترنيت باسم المستخدم فيجد ساعاته تنقص دون ان يستخدمها او يتم من خلاله سرقة كلمة السر في ساحات الحوار فتكتب مقالات باسمه لم يكتبها.

٣-التدمير من خلال برامج الـ .Hunkers تقوم هذه البرامج بتعطيل نظام التشغيل ويتراوح خطرها بين تغيير الوقت بساعة النظام وبين توقف النظام كليا عن العمل وتوجد انواع منها، بعضها موجه إلى التركز على برنامج معين لتدميره دون إلحاق الضرر بنظام التشغيل ذاته.

٤-الباب الخلفي Backdoor هذا الصنف هو الاخطر، وهو الشائع بين كل المخترقين، لانه يجعل المخترق قادرا على الدخول لجهاز الضحية والسيطرة عليه كليا او جزئيا، بحسب البرنامج المستخدم . ويقصد بالباب الخلفي الثغرات الموجودة بقصد او دون قصد في أنظمة التشغيل وبعض البرامج او المواقع، والتي يراد منها
أحيانا التعرف على عيوب النظام، لكن هذه الثغرات تستغل من قبل المخترقين للدخول إلى أجهزة الغير لتحقيق أهدافهم.

الحماية من الاختراق

للحماية من الاختراقات والتجسس هناك عدة طرق تستخدمها برامج الحماية لاداء مهامها ويمكن

تصنيف هذه الطرائق الي أربعة على النحو التالي:

١-إنشاء قاعدة بيانات بأسماء أحصنه طروادة، والتي يمكن من خلالها عمل مسح لكافة الملفات الموجودة بجهاز المستخدم ومطابقتها مع الموجود بقاعدة البيانات تلك للتعرف على الملفات المطابقة . على ان يتم تحديث قاعدة البيانات دوريا اما من خلال الاقراص المرنة. وهي طريقة تعتمدها شركة مكافي ببرنامجها الشهير أنتي فيروس او يتم ذلك مباشرة من خلال الانترنيت كما في برنامج . Norton
٢-البحث عن وجود تسلسل محدد من الرموز التي تميز كل ملف تجسسي والتي تميز أحصنه طروادة وغيرها وهذا الملف يعرف تقنيا باسم Signature وهذه الطريقة تحدث دوريا بالطريقة التي سبق ذكرها .

٣- الكشف عن التغيرات التي تطرأ على ملف التسجيل Registry وتوضيح ذلك للمستخدم لمعرفة ان كان التغيير حصل من برنامج معروف او من حصان طروادة. هذه الطريقة يتبعها برنامج Look Down الشهير.
٤- مراقبة منافذ الاتصالات بالجهاز (اكثر من ٦٥٠٠٠ منفذ) اكتشاف أي محاولة غير مسموح بها لاتصال بالجهاز المستهدف وقطع لاتصال تلقائيا وإعطاء تنبيه بذلك في حالة وجود محاولة لاختراق . هذه هي طريقة برنامج Gamer المعروف.