

طبعة ملونة

هيئة التعليم التقني

INFORMATION SECURITY

الدكتور دلال صادق الدكتور حميد ناصر الفتال

أمن المعلومات

أمن المعلومات



اليازوري

الدكتور دلال صادق الدكتور حميد ناصر الفتال



أمن المعلومات

الدكتورة دلال صادق الجواد
أستاذ مساعد أستاذ مساعد

الدكتور حميد ناصر الفتال
الكلية التقنية الإدارية الجامعة المستنصرية

المحتويات

I.....	الدكتورة دلالة صادق الجواد أستاذ مساعد أستاذ مساعد
I.....	الدكتور حميد ناصر الفتحال الكلية التقنية الإدارية الجامعة المستنصرية
1	المقدمة
3	الفصل الأول مدخل إلى أمن المعلومات
3	1-1 المقدمة:-
3	2-1 مفهوم أمن المعلومات:-
4	3-1 طبيعة وتحديات مشكلة الحماية الأمنية:-
7	4-1 أساليب مواجهة تهديدات أمن المعلومات:-
7	أولاً: تحليل المخاطر الناجمة عن الانتهاك
7	ثانياً: تحديد المستوى الحالي لظهور مخاطر الانتهاك
7	ثالثاً: العقوبات التي تقف في طريق توفير المستوى المناسب لتدابير الحماية الأمنية
7	1-4-1 تحليل المخاطر الناجمة عن الانتهاك:-
7	الدافع:-
7	ويرجع إلى عدة أسباب:-
8	2- منفذ الضعف:-
9	3- المعرفة بالمصادر:-
10	4- متطلبات الوصول:-
10	5- تكرار وأسلوب الحدث:-
11	6- المصادر الإضافية المطلوبة:-

- 11 2-4-1 تحديد المستوى الحالي لظهور مخاطر الانتهاك:-
- 12 3-4-1 العقوبات التي تقف في طريق توفير المستوى المناسب لتدابير الحماية الأمنية:-
- 12 5-1 مكونات أمن المعلومات:-
- 14..... أسئلة الفصل الأول**
- 15..... الفصل الثاني أمن الأفراد والإدارة.**
- 15 1-2 المقدمة:-
- 15 2-2 دور الإدارة وإجراءاتها في تحقيق وتعزيز أمن الحاسبات:-
- 15 1-2-2 التحكم بدخول الأفراد:-
- 16..... شكل رقم (1) دخول الافراد للنفاذ الى شبكة المعلومات**
- 17 2-2-2 عناصر التحكم في دخول الأفراد:-
- 19 3-2 متطلبات نظام الحماية الأمنية لمراكز الحاسبات:-
- 21 4-2 تحديد المسؤول عن أمن بناية مركز الحاسبة:-
- 23..... أسئلة الفصل الثاني.**
- 24..... الفصل الثالث الأمن في بناية مراكز الحاسبات.**
- 24 1-3 المقدمة:
- 25 2-3 الموقع:-
- 26 3-3 التصميم الهندسي لبنانية مركز الحاسبة:
- 27 4-3 اختبار قاعة الحاسبة في المبنى:-
- 28 5-3 متطلبات الحماية الأمنية لقاعة الحاسبة الإلكترونية:-
- 30 6-3 متطلبات الحماية الإلكترونية للمبنى:-
- 31 7-3 المواد التي يسمح بدخولها إلى قاعة الحاسبة:-
- 32 8-3 أمن الأجهزة البيئية لمركز الحاسبة الإلكترونية:-

- 33 9-3 منظومة الطاقة الكهربائية:-
- 33 1-9-3 تغذية مركز الحاسبة بالطاقة الكهربائية:-
- 34 2-9-3 منظومة توليد الطاقة الكهربائية في الحالات الطارئة:-
- 34 أ- منظومة توليد الطاقة الكهربائية الأساسية BASIC UPS:
- 34 ب- مولدة الطاقة الكهربائية البديلة:
- 35 10-3 مكافحة الحرائق:-
- 35 1-10-3 سبل تقليل الخسائر عند حدوث الحريق في مركز الحاسبة:-
- 36 2-10-3 منظومة الإطفاء الطوعي:-
- 37 3-10-3 الإجراءات المتخذة عند حدوث حريق:-
- 38 4-10-3 تجهيزات ضرورية لمواجهة الحالات الطارئة:-
- 37 شكل رقم (2) منظومة إطفاء طوعية بغاز الهالون.....
- 38 11-3 جرد المعدات:-
- 39 أسئلة الفصل الثالث
- 40 الفصل الرابع أمن الوثائق والمعلومات.
- 40 1-4 المقدمة:-
- 40 2-4 تصنيف المعلومات:-
- 40 1- سري للغاية TOP SECRET
- 41 2- سري SECRET
- 41 3- رسمي CONFIDENTIAL
- 41 4- محدود RESTRICTED
- 41 5- غير مصنفة UNCLASSIFIED
- 42 3-4 إجراءات حماية البيانات الخاصة بمركز الحاسبة:-

- 42 أ- البطاقات المثقبة والأشرطة الورقية المثقبة:-
- 43 ب - الأشرطة والأقراص المغنطة:-
- 43 4-4 إجراءات حفظ وأتلاف الأشرطة والأقراص المغنطة:-
- 44 أ- حفظ الأشرطة والأقراص المغنطة:-
- 44 ب - إتلاف المواد المصنفة:-
- 47 أسئلة الفصل الرابع
- 48 الفصل الخامس أمن الاتصالات
- 48 1-5 المقدمة:-
- 48 2-5 الاتصالات وثورة المعلومات:-
- 50 3-5 عناصر أمن الاتصالات:-
- 51 أمن خطوط الاتصالات السلكية:-
- 51 أولاً- الإجراءات الفنية لحماية خطوط التناقل:-
- 53 ثانياً- دلائل وجود مسترق على خط تناقل البيانات:-
- 54 أمن خطوط الاتصال اللاسلكية:-
- 55 4-5 إجراءات أمن الاتصالات:-
- 55 1 - نطاق الترددات BANDWIDTH:-
- 56 2 - النقاط النهائية:
- 56 1- القنوات:
- 56 2- طريقة البث:
- 57 3- اتجاه البث:-
- 58 أسئلة الفصل الخامس
- 60 الفصل السادس الفيروس

60	1-6 المقدمة:-
60	2-6 تعريف الفيروس:-
61	3-6 بداية نشوء الفيروس:-
62	4-6 الاسم (فيروس):-
64	5-6 صفات (خصائص) الفيروس:-
65	6-6 أعراض الإصابة بالفيروس:-
67	7-6 تصنيف البرمجيات الماكرة MALWARE:
70	8-6 أخطار الفيروس:-
71	أ- إبطاء تشغيل الحاسبة:-
71	ب- تدمير قطاع التحميل Boot sector:-
72	ج- تدمير جدول توزيع الملفات File Allocation Table:-
72	د- تحطيم الفهرس الرئيسي Root Directory:-
73	هـ- التجسس على النظم:-
73	2- أخطار الفيروس على المكونات Hardware:-
74	9-6 أكثر الفيروسات انتشاراً:-
75	1- الفيروس Worm Explorer Zip:-
75	2- الفيروس ATAKA (A.K.A. IE0199.exe):-
75	3- الفيروس W32/Ska (A.K.A Happy99.exe):-
76	4- الفيروس Laroux:-
76	5- الفيروس W32.CIH:-
77	10-6 وصايا لتجنب الاصابة بالفيروس:-
78	أسئلة الفصل السادس.

80	الفصل السابع الأمن التقني.....
80	1-7 المقدمة:-.....
80	2-7 من أجهزة الحاسبة الإلكترونية:-.....
80	1- الحاسبات الرئيسية Main Frame:-.....
81	2- المحطة الطرفية Remote Terminal:.....
82	3- المودم Modem.....
83	شكل رقم (4).....
83	المحطات الطرفية.....
84	3-7 أمن أجهزة الحاسبات الإلكترونية:-.....
84	1-3-7 أمن المحطات الطرفية:-.....
85	2-3-7 أمن بقية أجهزة الحاسبة الإلكترونية:-.....
86	4-7 التجسس على مراكز الحاسبات بالطرق الميكانيكية والإلكترونية:-.....
87	5-7 مشكلة الانبعاث المغناطيسي:.....
88	6-7 وسائل الحماية:-.....
90	أسئلة الفصل السابع.....
92	الفصل الثامن أمن أنظمة التشغيل والبرمجيات.....
92	1-8 المقدمة:-.....
92	2-8 أمن أنظمة التشغيل:-.....
93	3-8 الحماية التي توفرها أنظمة التشغيل:-.....
93	1-3-8 كلمات السر أو المرور:.....
95	2-3-8 جدول الصلاحيات:-.....
96	4-8 أمن التطبيقات:-.....

97	5-8 التوثيق الأمني:-
99	أسئلة الفصل الثامن
100	الفصل التاسع الترميز والتشفير
100	1-9 المقدمة:-
101	2-9 نبذة تاريخية عن الترميز والتشفير:-
102	3-9 مصطلحات الترميز والتشفير:-
103	فك الشفرة التشفير
103	4-9 أنظمة الترميز:-
103	النص الصريح الرسالة الأصلية اشفرة
103	فك الرموز او الشفرة
103	الرسالة الأصلية
103	النص الصريح
103	الكتابة المشفرة
103	الرسالة السرية
103	الترميز او التشفير
103	الرسالة السرية الكتابة المشفرة
103	شكل رقم (5)
104	أ) نظام ترميز الجزء الواحد (ONE PART SYSTEM):-
105	ب) نظام ترميز الجزأين (TWO PART SYSTEM):-
107	5-9 أنظمة التشفير:-
107	1-5-9 الشفرات الابدالية:-
107	1- عكس الرسالة:
108	2- الأنماط الهندسية:-

109	3- إبدال المسلك:-
112	4- الإبدال العمودي:-
113	9-5-2 الشفرات التعويضية:-
113	1- الشفرة الرقمية:-
115	2- أنظمة تشفير الآسكي:-
115	3- الشفرات العكسية:-
116	4- الشفرات القيصرية:-
118	أسئلة الفصل التاسع
120	الفصل العاشر أمن الحاسبات الصغيرة
120	10-1 المقدمة:-
122	10-2 معضلات أمن الحاسبات الصغيرة:-
123	10-3 إجراءات الحماية المطلوبة لسلامة الحاسبات الصغيرة:-
125	10-4 العناية بالأقراص المرنة:-
128	10-5 اعتبارات أمنية أساسية:-
129	أسئلة الفصل العاشر
130	الفصل الحادي عشر القانون وجرائم الحاسبات
130	11-1 المقدمة:-
130	11-2 جرائم الحاسبات الإلكترونية:-
131	11-2-1 الاحتيال وانتهاك سرية الأفراد باستخدام الحاسبة الإلكترونية:-
133	11-2-2 سرقة الكيانات المنطقية أو برمجيات الحاسبة الإلكترونية:-
134	11-3 القانون وجرائم الحاسبات الإلكترونية:-
135	11-4 شخصية القائم بجرائم الحاسبات الإلكترونية:-

138 أسئلة الفصل الحادي عشر
140 المصادر
140 الكتب العربية
141 الكتب الأجنبية

EBSCOhost®

المقدمة

في بادئ الأمر نحمد الله ونشكره على توفيقه لنا لإنجاز هذا الكتاب وبعد، ان التطور الكبير الذي حصل في الحاسبات الإلكترونية واستخدامها لحفظ الكثير من المعلومات والبيانات، أدى إلى ظهور مشكلة جديدة وهي كيفية الحفاظ على المعلومات السرية والمهمة من المتطفلين. وقد أصبح الإلمام بموضوع أمن المعلومات ضرورة من ضرورات العصر الحديث. اذ يعتبر موضوع أمن المعلومات من المواضيع المتشعبة والواسعة، وتعتبر مشاكله من اعقد المشاكل بسبب تعدد مكونات امن المعلومات من جهة وتداخله مع فروع الأمن الأخرى من جهة ثانية.

ان الهدف من وراء إعداد هذا الكتاب هو إعطاء فكرة عامة وشاملة عن موضوع امن المعلومات. وقد جاءت محاولتنا في كتابة فصول هذا الكتاب منسجمة وطبيعة المفردات المنهجية، وهو موجه بصورة أساسية إلى طلبة الجامعات والمعاهد.

شمل هذا الكتاب أحد عشر- فصلاً تغطي معظم الأمور المهمة في أمن المعلومات. فقد تضمنت الفصول الخمسة الأولى مواضيع عن مفهوم أمن المعلومات، أمن الأفراد والإدارة، الأمن في بناية مركز الحاسبة، أمن الوثائق والمعلومات، أمن الاتصالات. أما الفصل السادس فقد تطرق إلى موضوع الفيروس. وفي الحقيقة، من الصعب جداً الإلمام بكافة جوانب هذا الموضوع في فصل واحد إلا انه أعطيت فكرة عامة عن الموضوع لأهميته في

الوقت الحاضر. أما الفصل السابع والثامن فقد تضمن الأمن التقني أمن التشغيل والبرمجيات.

ونظراً لأهمية موضوع الترميز والتشفير فقد خصص الفصل التاسع لهذا الموضوع وقد روعي ان تحتوي مادة هذا الفصل الأمور الأساسية التي تخص الموضوع دون الخوض في الكثير من التعقيدات التي لا تبدو ضرورية. أما الفصل العاشر والحادي عشر فقد تضمن أمن الحاسبات الصغيرة والقانون وجرائم الحاسبات.

في الختام نأمل أن نكون قد قدمنا خدمة متواضعة لمكتبة العربية بشكل عام ولطلبة الجامعات والمعاهد بشكل خاص. وان تكون محاولتنا هذه خدمة بسيطة نؤديها الى بلدنا الغالي وامتنا المجيدة، والله ولي التوفيق.

المؤلفان

الفصل الأول مدخل إلى أمن المعلومات

1- 1 المقدمة:-

يزداد يوماً بعد يوم أهمية الدور الذي تلعبه الحاسبات في المؤسسات الاقتصادية والتجارية والعسكرية لخصن ومعالجة البيانات ذات الطابع المهم والحساس إلى جانب المعلومات الشخصية التي تمس حرية وخصوصية المؤسسات والأفراد في المجتمع. هذه المعلومات يتم التوصل إليها بشكل متزايد وعلى نطاق واسع من خلال شبكات عامة للاتصال غالباً ما تكون وسائل الحماية الخاصة بها ضعيفة مما يهدد أمن وسرية المصادر البيانية ويؤثر على نوع الخدمة التي تقدمها الكثير من أنظمة المعلومات الممكنة.

أن التطور التكنولوجي السريع في مجال تقنيات الحاسب أدى إلى ظهور أجهزة وأساليب جديدة مثل البريد الإلكتروني، والتراسل الآلي وغيرها والتي ساعدت على تسهيل وتبادل المعلومات واتساع رقعته، ألا أنها أدت إلى زيادة احتمالية انتهاك وتسرب هذه المعلومات وتعرضها لخطر التغيير والتزوير من قبل أطراف غير معنية سواء بشكل متعمد أو عن غير قصد.

1- 2 مفهوم أمن المعلومات:-

يتسع مفهوم أمن المعلومات ليشمل الإجراءات والتدابير المستخدمة في المجالين الإداري والفني لحماية المصادر البيانية (من أجهزة وبرمجيات وبيانات

وأفراد) من التجاوزات والتدخلات غير المشروعة التي تقع عن طريق الصدفة او عمداً عن طريق التسلل أو كنتيجة لإجراءات خاطئة أو غير الوافية المستخدمة من إدارة هذه المصادر وعليه فان موضوع أمن المعلومات يشمل عدداً من المحاور أهمها:-

الأخطاء العفوية غير المتعمدة أثناء تجهيز البيانات لإدخالها على الحاسبة.

حوادث فقدان أو تغيير المعلومات بسبب تعطيل الأجهزة أو حصول خلل في البرامج.

سرقة المعلومات أو التقاطها وتغييرها بشكل غير مأذون وما ينتج عن هذا من سوء استخدام هذه المصادر.

فقدان قدرات إدارة المعلومات نتيجة وقوع بعض الكوارث الطبيعية مثل الفيضانات والكوارث غير الطبيعية مثل الحرائق وحوادث التفجير.

1- 3 طبيعة وتحديات مشكلة الحماية الأمنية:-

تتطلب دراسة مشكلة أمن وسرية المعلومات تسليط الضوء على مجموعة من الحقائق التي تحكم بيئة إدارة المعلومات أهمها:-

1- الاتجاه المتزايد نحو تكديس المعلومات الحساسة داخل أوعية مركزية عرفت بقواعد البيانات مما أدى إلى زيادة المخاطر التي تتعرض لها المصادر البيانية ولا يساعد توزيع هذه المصادر على مواقع جغرافية منفصلة على تقليل هذه المخاطر طالما كانت هذه الأنظمة مرتبطة من خلال شبكات

الاتصال، بل أن هذا التوزيع غالباً ما يكون سبباً في وقوع المزيد من حوادث الانتهاك.

2- أصبحت مصادر البيانات قابلة للالتقاط بسهولة أكبر عن طريق استخدام منافذ اتصال زهيدة التكلفة مع ارتفاع طاقة وقدرة هذه الأجهزة على البث. وبهذا تحولت النظم الإلكترونية لإدارة المعلومات من مجرد أداة مساعدة إلى أسلوباً للإدارة لا يمكن الاستغناء عنه.

3- بسبب حداثة ظاهرة الانتهاك نوعاً ما، إلى جانب اتجاه الكثير من المؤسسات إلى التكتّم على الأخبار التي تتصل بعمليات الاختراق أما نتيجة الخوف من توجيه النقد لعدم وجود تدابير وقائية مناسبة أو الخوف من فقدان ثقة العملاء أو الخوف من تكرار المحاولات من جانب أشخاص قد يسعون إلى استغلال نقطة الضعف التي تم كشف النقاب عنها. لذا فقد يؤدي نقص الوعي والكتمان إلى عدم توفر قاعدة كافية من المعلومات يمكن على أساسها وضع سياسة مناسبة للحماية وتحديد حجم الاستثمارات المطلوبة لمواجهة مثل هذه المخاطر.

4- كثير من المخاطر والانتهاكات يتم التغاضي عنها أو التصغير من شأنها إذا كان تأثيرها على العمليات اليومية العادية ضئيل ومحدود. كذلك فإن الكثير من المؤسسات ما زالت لا تدرك القيمة الحقيقية لمصادر البيانات ومدى تأثيرها على سياسات وأهداف المنشأة وكيفية إدارة الموارد الأخرى.

5- الكثير من إجراءات الحماية المتبعة حالياً سواء ما يتعلق منها بإجراءات التدقيق وتعريف الهوية أو إجراءات الحماية من الوصول غير المخول أو إجراءات التشفير تحتاج إلى تطوير.

6- من الصعب في كثير من الأحيان اكتشاف أو تتبع التغيرات التي تطرأ على المصادر البيانية بسبب تشعب وتعقد النظم وبالتالي فإن إقامة الأدلة على القائمين بهذه الأعمال يعتبر غاية في الصعوبة.

7- نقص التشريعات القانونية في هذا المجال إلى جانب عجز معظم هذه القوانين عن التمييز بين القيمة الحقيقية للمعلومات والقيمة المادية للأوساط التي استخلصت منها المعلومات.

8- هناك أيضاً ظاهرة مثيرة للاهتمام فيما يتعلق بحوادث الاحتيال باستخدام الحاسبة وهي ان الأشخاص الذين ينفذون عملية احتيال كبرى بهذا الأسلوب دون ان يتم الكشف عنهم بسرعة يصبحون حتى في نظر القضاة أحياناً أبطال من نوع خاص استطاعوا بذكائهم ان يهزموا النظام الأمني المتبع او خدعوا الآلة وهو في رأي البعض نوع من الإبداع.

في مواجهة هذه المواقف الصعبة وهذه الحقائق فإن أي سياسة واقعية للتغلب على المشكلة يجب أن تتفادى الوقوع في ثلاثة أخطاء هي:-

- عدم الاهتمام بما يعلن عن حوادث الانتهاك بعذر أن الحادث يمس الآخرين.
- المبالغة في وصف المخاطر وتجسيم الحوادث بما يؤدي إلى إثارت البلبلة بين الأفراد إلى الحد الذي قد يؤثر على مرونة الخدمات التي تقدمها المصادر البيانية بسبب عدم اتباع الإجراءات المناسبة والفعالة وقد يمتد الخوف إلى تجنب النظم الإلكترونية في إدارة المعلومات.

- اتباع إجراءات وقائية غير واقعية تتجاهل المفاهيم الأساسية لأمن وسرية المعلومات حيث يجب على إدارة المنشأة أن تنظر إلى مسألة الأمانة باعتبارها

جزء مكمل لسياستها العامة وان تهتم بهذه المشكلة أثناء التخطيط لهذه السياسات.

1- 4 أساليب مواجهة تهديدات أمن المعلومات:-

يعتمد النجاح في مواجهة التهديدات لأمن المعلومات على ما يأتي:-

أولاً: تحليل المخاطر الناجمة عن الانتهاك.

ثانياً: تحديد المستوى الحالي لظهور مخاطر الانتهاك.

ثالثاً: العقوبات التي تقف في طريق توفير المستوى المناسب لتدابير الحماية الأمنية.

1- 4- 1 تحليل المخاطر الناجمة عن الانتهاك:-

ينتج الانتهاك غير المتعمد لأمن وسلامة البيانات غالباً عن إجراءات خاطئة وغير سليمة تتراوح بين إجراءات تجهيز وإدخال البيانات وحتى أخطاء التشغيل التي تحدث أثناء المعالجة، مروراً بالأخطاء ونقاط الضعف غير المنظورة في البرامج التطبيقية نفسها.

أما الانتهاك المتعمد فيمكن تحليلية على وفق المعايير الآتية:-

الدافع:-

ويرجع إلى عدة أسباب:-

أ- **الأسباب المالية:** بهدف اختلاس الصكوك والأسهم والسندات أو الأوراق المالية القابلة للتحويل، أو المواد الأولية والسلع المصنعة أو تغيير

البيانات لإيجاد تسويات مالية محظورة، إلى جانب سرقة المعلومات وإعادة بيعها لأطراف منافسة واستخدام بعض المصادر المتاحة لتطوير برامج لصالح مكاتب خدمات خارجية أو مؤسسات أخرى لقاء مبالغ مالية.

ب- **الأسباب العاطفية:** والتي تقع عند شعور أحد العاملين بالغبن بسبب تخطي الآخرين له في الترقية أو انه يعامل بصورة لا يراها منطقية من قبل المسؤولين بالإضافة إلى الإحساس بالفشل عقب صدام مع الإدارة أو الزملاء أو كرد فعل للتعرض للنقد الشديد غير الموضوعي.

وكما نرى أن الدوافع العاطفية مرتبطة كلها بالعمل وبالتالي يسهل ملاحظتها ويمكن العمل على تفاديها. أما الدوافع العاطفية الشخصية فأنها لقللة ارتباطها بالعمل يصعب اكتشافها وتحديدتها والتعامل معها.

ج- **الأسباب الفكرية:** وتعد هذه الأسباب أكثر الدوافع تحدياً حيث لا دخل للاعتبارات المالية أو العاطفية في الجريمة فقد يرتكب الفاعل جريمته لمجرد إرضاء فضوله الفكري أو من منطلق التحدي لاثبات خطأ الإدارة عندما أعلنت ان لديها نظاماً آمناً لا يمكن اختراقه.

2- منفذ الضعف:-

ويقصد به الفارق الزمني الذي تتوفر خلاله احتمالات الانتهاك وقد يكون هذا المنفذ ضئيل نسبياً يظل مفتوح لفترة لا تتجاوز ثوان او دقائق محدودة، كما قد تطول الفترة إلى ساعة أو أكثر ولعدة مرات يومياً، او يظل مفتوحاً باستمرار.

ومن الأمثلة لبعض المنافذ الرئيسية او الهامة نذكر:

- فترة تشغيل النظام.
- فترة تعديل او تحديث النظام.
- إصلاح الخلل او العطل في النظام.
- تفريغ قاعدة البيانات على أجهزة الحزن الخارجي.
- تغيير نوبات العمل وجولات المسؤولين.
- إلغاء أو تغيير كلمة السر.

علمًا بأن عدد مرات ومدة فتح المنفذ يشكلان اهم عوامل حدوث الانتهاك التي يمكن ان يستعملها الجاني المتربص، ففي الحوادث البسيطة قد لا يستخدم سوى منفذ واحد ولمرة واحدة أما في الحوادث المعقدة فغالباً ما تستخدم منافذ متعددة وبصورة متكررة على مدى فترة زمنية طويلة.

3- المعرفة بالمصادر:-

يساعد على وقوع حوادث الانتهاك المتعمد نوعان من المعرفة بمصادر إدارة المعلومات هي:

- أ- **معارف مادية:-** مثل موقع المصادر، طرق الوصول إليها، مواعيد استخدامها، نوع الرقابة أو الحراسة المتبعة، الإجراءات الأمنية للمبنى او الموقع، تنسيق الوقت بين نوبات العمل والحراسة.
- ب- **معارف منطقية:-** مثل معرفة محتوى المصادر، إجراءات تبويبها والتقاطها، كلمات السر، خوارزميات الترميز المتبعة، المعرفة بالإجراءات الأمنية نفسها وكيفية الاستفادة من حدوث كارثة.

ويوفر الحصول على المعارف المادية والمنطقية بالمصادر اكبر العون للجاني المتعمد أثناء بحثه عن منفذ ضعف لتنفيذ جريمته ويلاحظ ان اكثر هذه المعلومات توجد في الوثائق والملفات اليدوية الخاصة بإدارة المعلومات والتي لا تنال عادة نفس القدر من الحماية الذي يمنح للمعلومات المخزونة داخل الحاسب.

4- متطلبات الوصول:-

بعض أشكال الانتهاك يمكن تحقيقها من مواقع بعيدة دون الحاجة الى الوصول المادي إلى بناية المؤسسة. وفي أشكال الانتهاك المتوسطة قد يتطلب الامر الوصول إلى موقع واحد أو جهاز اتصال واحد (محطة طرفية) داخل هذا الموقع.

أما الحوادث المعقدة فأنها غالباً ما تتطلب مستويات اكبر من الوصول المادي وتشمل مصادر متعددة وانتهاز اكبر عدد من الفرص على مدى زمني طويل.

5- تكرار وأسلوب الحدث:-

يبن تحليل الحوادث المسجلة لحالات الاختراق بان الحوادث المنفردة كثيراً ما تكون ذات أساليب شديدة البساطة ولا تتطلب مصادر واسعة أو التواطؤ مع أفراد آخرين وغالباً ما تنفذ من قبل جهة واحدة دون بذل أي محاولة للتمويه من جانب المرتكب الذي غالباً ما يكون بعيداً عند اكتشاف الحدث وقد يكون موظفاً في نفس المؤسسة أو شخصاً خارجياً استطاع الحصول على أحد المستويات المطلوبة لمعرفة المصادر والوصول إليها، وتشكل الصيغة الفردية

لتلك الحوادث خبرة لدى مرتكبها ونتيجة لذلك فان كشفها يكون في العادة أمر شديد الصعوبة.

6- المصادر الإضافية المطلوبة:-

تشمل المصادر الإضافية التي تتطلبها مختلف جرائم الانتهاك المتعمد على، الأجهزة الإلكترونية للاختبار والتشخيص وهي عالية الكفاءة ويسهل استخدامها لرصد ونسخ وتغيير (من خلال المحاكاة) البيانات داخل جهازي معالجة المعلومات والشبكة، ومعدات لنقل الأفراد والمعدات إلى داخل الموقع او فيما بين عدة مواقع. وبالإضافة إلى تمويل شراء او استئجار الأجهزة الإلكترونية يستلزم توفير الأموال أيضاً لأغراض أخرى مثل تشجيع وإغواء موظفي المؤسسة لكي يشاركوا في جريمة الانتهاك. ويلاحظ عادة أن الجرائم المدروسة تتطلب وقتاً أطول نسبياً سواء في مرحلة التخطيط أو التنفيذ.

1- 4- 2 تحديد المستوى الحالي لظهور مخاطر الانتهاك:-

تساهم عوامل عديدة في تعقيد إمكانية تحديد المستوى الحالي لظهور مخاطر الانتهاك، من هذه العوامل هي:-

- 1- صعوبة تحديد القيمة (الخسارة) الناجمة عن مختلف حوادث الانتهاك.
- 2- عدم إلمام مسؤولي أمن المعلومات بطبيعة العمليات التي تتم بداخل النظم المعقدة او في مواضع نقاط الضعف لهذه النظم وبالتالي صعوبة تحديد عدم كفاية الإجراءات الحالية.

- 3- صعوبة تقدير احتمالات وقوع او نجاح بعض محاولات الانتهاك بسبب عدم وجود توثيق شامل وجيد لحوادث الانتهاك داخل وخارج المؤسسة.
- 4- صعوبة التنبؤ بالعوامل الإنسانية وبالتالي عدم إمكانية إخضاعها للقياس.

1- 4- 3 العقبات التي تقف في طريق توفير المستوى المناسب لتدابير الحماية الأمنية:

- أ- نقص الأفراد المدربين والذين يبدون اهتماما بمشكلة أمن وسلامة البيانات.
- ب- نقص التمويل والوقت، والاهم من ذلك الوعي والمساندة من جانب الادارة والجهات المستفيدة من المعلومات.
- ج- سوء التقدير لمدى تعقد النظم والتطبيقات والاستعجال لبلوغ حالة التشغيل الأمر الذي يؤدي إلى قلة الاهتمام أو إغفال تدابير السلامة الضرورية.

1- 5 مكونات أمن المعلومات:-

- باستثناء بعض المؤسسات الحكومية والعسكرية، سيكون من غير الواقعي ان نفرض بأن 100% من التطبيقات والنظم المعاونة هي بالفعل حرجة للغاية وبالتالي تتطلب تدابير شاملة للحماية الأمنية. ولاشك ان التكلفة ستكون عقبة أمام غالبية المستفيدين في المجالات التجارية والمالية والصناعية.
- وإذا افترضنا ان الحماية بنسبة 100% أمر غير عملي، تبرز أمامنا مشكلة جديدة هي: كيف يمكننا أذن تحديد المخاطر النسبية المرتبطة بكل المصادر المختلفة، وتكلفة مستويات الحماية المقبولة.

وقبل ان نتطرق إلى تدابير الحماية والسلامة التي يمكن تعريفها وتطويرها واختبارها عبر كل مصدر من مصادر أمن المعلومات بالشكل الذي يساعد على تخفيض مستوى ظهور حالات الانتهاك إلى الدرجة المقبولة التي تم إقرارها في ضوء تحليل المخاطر المحتملة، يتعين علينا أولاً التعرف على مكونات أمن المعلومات التي يمكن تقسيمها إلى ما يلي:

- 1- أمن الأفراد والإدارة.
- 2- أمن المعلومات والوثائق في مراكز الحاسبات.
- 3- أمن بناية مركز الحاسبة الإلكترونية.
- 4- أمن الأجهزة البيئية الخاصة بمركز الحاسبة.
- 5- أمن الاتصالات الخاصة بالحاسبات الإلكترونية.
- 6- أمن أنظمة التشغيل والبرمجيات.
- 7- أمن أجهزة الحاسبات الإلكترونية.

في الفصول التالية سيتم التعرف من خلالها على مكونات أمن المعلومات واحتمالات انتهاك أمنها وسلامتها وأسلوباً للتوصيف والمحافظة على المستويات المقبولة للحماية.

أسئلة الفصل الأول

- 1- عدد أهم المحاور التي يشتمل عليها موضوع أمن المعلومات.
- 2- تتطلب دراسة مشكلة أمن وسرية المعلومات تسليط الضوء على مجموعة من الحقائق التي تحكم بيئة إدارة المعلومات. تكلم عن أربعة من هذه الحقائق.
- 3- يساعد على وقوع حوادث الانتهاك المتعمد نوعان من المعرفة، عددهما مع الشرح.
- 4- ما هي العوامل التي تساهم في تعقيد إمكانية تحديد المستوى الحالي لظهور مخاطر الانتهاك.
- 5- ما هي العقوبات التي تقف في طريق توفير المستوى المناسب لتدابير الحماية.
- 6- ما هي مكونات أمن المعلومات.

EBScohost®

الفصل الثاني أمن الأفراد والإدارة

2- 1 المقدمة:-

لغرض إدارة مركز حاسبة بصورة صحيحة وخصوصاً من الناحية الأمنية، تقوم الإدارة باتخاذ مجموعة من الإجراءات من شأنها الحفاظ على أمنية مركز الحاسبة من أخطار الأشخاص غير المخولين. تختلف خطورة هؤلاء حسب طبيعة عملهم. وسيتم التوضيح في هذا الفصل الإجراءات التي تتخذها الإدارة لضمان أمنية مراكز الحاسبات.

2- 2 دور الإدارة وإجراءاتها في تحقيق وتعزيز أمن الحاسبات:-

من الإجراءات المهمة التي تتخذها الإدارة لتحقيق وتعزيز أمن مراكز الحاسبات هو في التحكم في دخول الأفراد.

2- 2- 1 التحكم بدخول الأفراد:-

يمكن تحديد ثلاثة مستويات للتحكم في دخول الأفراد إلى موقع مصادر إدارة المعلومات، هذه المستويات هي:-

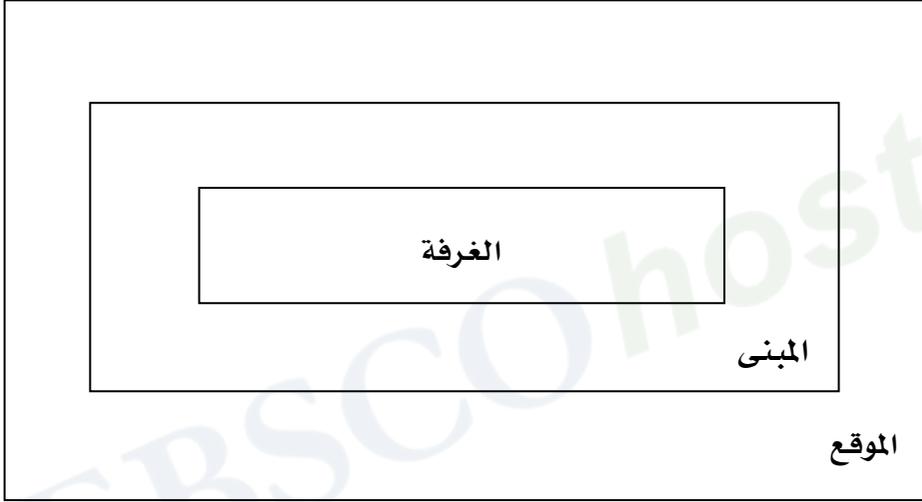
1- الموقع.

2- المبنى.

3- الغرفة.

ويقصد بالموقع هو محيط أو حدود المؤسسة (بصورة عامة) التي تحوي بداخلها مصادر إدارة المعلومات، أما المبنى هو نفس المبنى المشيد بداخل حدود الموقع والذي يحوي على مصادر إدارة المعلومات. والغرفة او الغرف هي تحوي المصادر.

شكل رقم (1)



دخول الافراد للنفاذ الى شبكة المعلومات

وقد تكون هذه المستويات الثلاثة مطلوبة أو مبررة في بعض المؤسسات بينما قد لا يستخدم سوى مستويين أو مستوى واحد في مؤسسة أخرى.

تحدد حرية الدخول إلى المؤسسات حسب طبيعة هذه المؤسسات. ففي المؤسسات العسكرية أو الحكومية أو المالية يكون التحكم في دخول الأفراد للموقع فوق المتوسط في حين في مؤسسات أخرى كالمؤسسات التجارية

والجامعية تكون حرية الدخول مباحة نسبياً، إذ لا توجد وسيلة آلية شاملة لمراقبة دخول الأشخاص.

2-2 عناصر التحكم في دخول الأفراد:-

من أهم عناصر التحكم في دخول الأفراد إلى مناطق مصادر إدارة المعلومات هو إيجابية تعريف هوية الأفراد الذين يطلبون الدخول.

يوجد ثلاثة معايير للتعريف بالهوية الشخصية للأفراد هي:-

1- الشيء المحمول

2- الشيء المعلوم

1- بعض الخصائص المادية (البصمات، الصوت، خطوط الكف، بصمات الشفاه، التوقيع).

1- **الشيء المحمول**:- يقصد بالشيء المحمول هو هوية (بطاقة) الموظفين وعليها صورة شخصية وشارات ومفاتيح مرمزة مغناطيسياً. تمتاز هذه الهويات بقلّة تكلفتها عند إنتاج أعداد كبيرة منها والسرعة النسبية في استعمالها وسهولة حملها من قبل الموظفين، وتكون ذات تأثير إيجابي عند استعمالها مع أحد الأشكال الأخرى للمراقبة.

أما عيوبها هي في حالة فقدان أو السرقة، كذلك أن استعارة أو تبادل البطاقات والمفاتيح لا يمكن اكتشافه بدون وجود شكل آخر للمراقبة، إضافة إلى وجود تقنيات لإنتاج نسخ مزيفة من الهويات يصعب اكتشافها.

2- **الشيء المعلوم:** - ويقصد به رقم البطاقة أو الهوية، تاريخ الميلاد، تاريخ التعيين، كلمات السر، الأرقام السرية للأقفال، وغيرها من خوارزميات الدخول. وعندما يكون التحكم في هذا الأسلوب عن طريق الحاسب الآلي فإنه يتميز بانخفاض الكلفة وسهولة اكتشاف الخطأ واستحالة التزييف.

ومن عيوبه هو عدم القدرة على التحكم في حالة استعارة أو تبادل كلمات السر أو الأرقام السرية. كذلك سهولة كشف واستعمال البيانات الشخصية للأفراد الآخرين.

3- **بعض الخصائص المادية:** - تتركز هذه الطريقة على استعمال مجموعة من الخصائص الشخصية المادية مثل بصمات الأصابع ومضاهاة الصوت وخطوط الكف وبصمات الشفاه والتوقيع وغيرها من الصفات الذاتية في الأنسان. وتهدف جميعها الى أيجاد أسلوب يقلل من إمكانية دخول الأفراد غير المأذونين.

تعد بصمات الأصابع من السمات الفريدة، وتقنية فحص البصمة لا تزال عالية الكلفة وتتطلب عدد من الأجهزة وهو أبطأ من أساليب الدخول بالبطاقات المرمزة. أما أسلوب مضاهاة الصوت فهو أسلوب إيجابي مقبول ويقلل من احتمال دخول أفراد غير مأذونين إلا أن هذه التقنية مرتفعة التكلفة.

أما أسلوب خطوط الكف فهي اسهل وأسرع في استعمالها نسبياً لكنها لاتزال عالية التكلفة مع ما تتطلبه من ضرورة ربطها بحاسب ألي لاختزان تسجيلات المطابقة ومعالجة طلبات الدخول. وهي كذلك لا تستطيع مراقبة حركة نقل المواد وعملية دخول (خروج) عدة أشخاص في وقت واحد.

أما بصمات الشفاه فهي أيضاً من السمات الشخصية الفريدة، لكن هذه الطريقة تتطلب المزيد من الدراسة المتأنية لدراسة الآثار الاجتماعية والجوانب النفسية قبل التغلب على كل الاعتراضات المثارة ضد هذه التقنية.

وأما التوقيع فهو أسلوب آخر للتعرف على الأشخاص والمتغيرات التي يتم تحليلها، وهي سرعة القلم مع الوقت، الضغط على القلم مع الوقت، الزمن الكلي للتوقيع، نسبة وضع أو رفع اليد عن الورق، وغيرها من العوامل. ان مضاهاة التوقيع توفر بالفعل مستوى عال من التحكم. والجهاز سهل الاستعمال وينتج سجلاً ورقياً لعملياته. هذه التقنية لاتزال في مراحلها الأولى وهي عالية التكاليف وتتطلب طاقة خزن كبيرة ومعالجة على الحاسب.

2- 3 متطلبات نظام الحماية الأمنية لمراكز الحاسبات:-

لضمان الحماية الأمنية، فان هنالك مجموعة من الأساليب الممكن اتخاذها ولكل أسلوب له مميزاته وعيوبه. من هذه الأساليب هي :-

1- المراقبة البصرية عن طريق مسؤولي الأمن:- ان المراقبة البصرية من قبل مسؤولي الأمن لها عدة مميزات منها التحكم الإيجابي في حركة الأشخاص

الداخلين والخارجين والمواد التي يحملونها. ومن عيوبها ارتفاع تكلفتها في المؤسسات الكبرى التي تتعدد فيها نقاط الدخول والخروج.

إضافة إلى ذلك، ان مسؤولي الأمن يعتادون على رؤية بعض الأشخاص يدخلون أمامهم كل يوم، وغالباً ما يتركونهم يمرون بصورة آلية سواء ابرز الشخص الداخل هويته أم لا. وفي هذه الحالة، قد يمر موظف سابق دون أن يعترض طريقه أحد إذا ما حاول دخول المنشأة.

2- الأساليب الإلكترونية (الدائرة التلفزيونية المغلقة):- يمتاز هذا الأسلوب بقلّة التكلفة، خاصة إذا ما دعت الحاجة لاستعمال عدد كبير من الأجهزة. أما أهم عيوبها، هي سهولة إخفاء أية مادة محمولة، كذلك صعوبة التحكم في مراقبة العديد من الأشخاص الداخلين في وقت واحد.

3- أجهزة مرمزة مغناطيسياً لقراءة الهوية:- ان هذا الأسلوب يمتاز بقلّة التكلفة وسرعة وسهولة الاستعمال.

4- أقفال مرمزة (بأرقام سرية):- يعمل هذا الأسلوب عن طريق الضغط على الأزرار لإدخال متوالية عددية من الأرقام وهو أسلوب سهل الاستعمال وسريع وقليل التكلفة نسبياً.

2- 4 تحديد المسؤول عن أمن بناية مركز الحاسبة:-

مركز الحاسبة كأى دائرة مهمة وذات خصوصية لابد وان يتواجد فيها من يكون مسؤولاً عن إدارة الأمن والأشراف على تطبيق الوصايا في هذا الموضوع.

لذا تقع على عاتق هذا الفرد جملة من الأعمال والوصايا التي تعتبر أساسية لخلق مناخ عمل أمين للآخرين، وتشمل هذه الوصايا ما يلي:-

1- مواجهة التهديدات ووضع قائمة تعدل سنوياً بالتهديدات المحتملة، او عند ظهور تهديد جديد. ولابد من الإشارة بشكل واضح في هذه القائمة الى تحديد الجزء المشمول بالتهديد والإجراءات المضادة المناسبة لكل منها.

2- وضع الإجراءات والوصايا الأمنية العامة بمركز الحاسبة.

3- تثقيف وتدريب العاملين بالقواعد الأمنية الصحيحة المتعلقة بأعمالهم.

4- تحديد الأشخاص الذين لهم صلاحية تداول المعلومات، للأشراف على سير أعمالهم قدر تعلق الأمر بالناحية الأمنية.

5- تبادل المشورة مع الاختصاصيين من العاملين في مركز الحاسبة لاستكمال

الصورة الأمنية لمركز الحاسبة، ووضع سياقات أمنية لبقية أقسام المركز

6- يرفع مسؤول الأمن تقرير عن الحالة الأمنية في المركز مع المقترحات إلى

مدير المركز شهرياً في الأقل وحسب مقتضيات المصلحة العامة.

7- استلام الشحنات الخاصة بالمركز وفحصها، والتأكد من المواد المخرجة من المركز كونها مرفقة باستمارة خاصة تصف المادة وسبب خروجها وعدم حملها أي إشارة أو تسمية يمكن ان يستدل من خلالها بأهميتها.

وعلى مدير المركز عدم إسناد مسؤولية أمن مركز الحاسبة لشخص واحد لمدة طويلة، او عندما يبدأ مسؤول الأمن بعدم الاكتراث والمتابعة أو عند وجود محذور أمنى في استمراره في عمله.

EBSCOhost®

أسئلة الفصل الثاني

- 1- عدد مستويات التحكم بدخول الأفراد مع الشرح المختصر.
- 2- عدد معايير التعريف بالهوية الشخصية للأفراد.
- 3- ما هي الأساليب الممكنة اتخاذها لضمان الحماية الأمنية لمراكز الحاسبات.
- 4- ما هي الخصائص المادية، وكيف يمكن الاستفادة منها في تعريف هوية الأشخاص.
- 5- تقع على عاتق مسؤول الأمن في مركز الحاسبة جملة من الأعمال والوصايا، عددها باختصار.

EBSCOhost®

الفصل الثالث الأمن في بناية مراكز الحاسبات

3- 1 المقدمة:

في بعض الظروف تتعرض أجهزة الحاسبة الإلكترونية إلى تلف كبير أو تلف شامل نتيجة لظروف خارجية مثل الزلازل أو الفيضانات أو الحريق أو عمليات الهجوم سواء كان برياً أم جويماً أو عن طريق التخريب. كما قد تتعرض هذه الأجهزة للعطل بسبب سوء الاستخدام أو عدم ملائمة البيئة داخل الموقع ونقص أجهزة الخدمات أو تعطلها أو بسبب القدم. وهذا سيلحق الضرر بالبيانات أيضاً.

وقد ازداد الاهتمام مؤخراً بالحوادث التي تتعرض لها أجهزة ومعدات الحاسبة والأجهزة الحديثة الملحقة بسبب التكلفة العالية والجهد المطلوب لعمليات الاستعادة، خاصة بعد أن تعرضت مراكز الحاسبات في البلدان المختلفة إلى عدد من الكوارث نذكر منها، حريق نشب في أحد مراكز الحاسبات في الولايات المتحدة الأمريكية عام 1973 أدى إلى خسارة بلغت قيمتها أكثر من 6,7 مليون دولار واحترق أكثر من سبعة آلاف شريط مغناطيسي إضافة إلى تدمير البناية والأجهزة والوسائل الخدمية الأخرى.

ولغرض تحقيق الحماية المطلوبة لابد من تهيئة نظام أممي متكامل وسوف نتطرق بإيجاز إلى أهم عناصره.

3- 2 الموقع:-

العديد من مراكز الحاسبات كانت تقع في أبنية مزججة جذابة وبعدد كبير من المستخدمين وهذه الأبنية تقع على شوارع مزدحمة بالناس والمركبات. غير ان المخاطر التي تهدد مراكز الحاسبات غيرت من هذا الوضع بشكل كبير، حتى اصبح اختيار موقع المركز يتم بتحفظ اكبر.

ان الموقع المختار للبنية يجب ان يكون اقل عرضة للدمار، ولكي يكون هذا الاختيار موقفاً يفضل ان يتصف بنايلي:-

1- ان تبتعد بناية مركز الحاسبة مسافة كافية عن مجرى النهر لتقليل مخاطر الفيضان والمياه الجوفية وكذلك بعيداً عن المناطق المهتدة بالزلازل.

2- أن تكون بناية مركز الحاسبة بعيدة عن المناطق العسكرية والحساسة في المدينة.

3- أبعاد بناية مركز الحاسبة بمسافة كافية عن الشارع العام ويفضل ارتباط البناية بشارع فرعي خاص وتوفر له وسائل السيطرة المناسبة.

4- يفضل أن تكون بناية مركز الحاسبة قريبة من مركز الإطفاء والشرطة، وذلك للحصول على افضل الخدمات في أوقات الطوارئ.

أما في حالة عدم إمكانية اختيار الموقع لمركز الحاسبة وخاصة المراكز التابعة للمؤسسات الموجودة فعلاً فان بعض المخاطر لا يمكن تجاوزها. أن المخاطرة الموجودة والمحيطه بمراكز الحاسبة يجب ان تخمن بغض النظر عما إذا كانت في

الموقع الخاص المختار أو ضمن موقع المؤسسة الحالي، كما وان هذه المخاطر بحاجة إلى إعادة النظر فيها بين فترة وأخرى.

3- 3 التصميم الهندسي لبناية مركز الحاسبة:

ان الحماية الأمنية لمركز الحاسبة هو العامل الأكثر أهمية الذي يجب ان يؤخذ بالحسبان عند التصميم لأنها تضم أجهزة منظومة الحاسبة وكذلك غرف العاملين عليها بالإضافة للمعدات والخدمات المساعدة لتشغيلها. لذلك فان أي إخفاق او نقاط ضعف في التصميم سوف يؤثر على مركز الحاسبة في مختلف النواحي. لذلك ينصح بأخذ الملاحظات التالية عند المباشرة بوضع التصميم الهندسي للبناية.

1- لا يفضل وضع قاعة الحاسبة تحت مستوى الأرض لاحتمال تهديد الحاسبة وأجزاءها بالمياه الجوفية او الفيضان أو بأي تسرب للمياه يحدث في البناية فضلاً عن مشكلة التهوية، بيد ان البناء تحت مستوى الأرض يوفر حماية كافية ضد الهجمات الجوية.

2- عدد الأبواب والشبابيك وفتحات التهوية يجب ان تكون محدودة عند التصميم ويفضل عمل فتحة صغيرة لمعرفة هوية الأشخاص قبل فتح الباب لهم لتجنب دخول الأشخاص غير المخولين وخاصة أثناء الليل.

3- جعل بناية المركز بمدخل واحد للأشخاص و آخر لدخول المواد والشحنات ويفضل ان يزود البناء بمصعد خاص لنقل المواد.

4- يفضل استخدام الاسيجة بنوعيتها السلكي والحجري بدلاً من مواجهة البناية المباشرة للشارع، وكذلك للسيطرة على المساحات المحيطة ببناية المركز.

5- يمكن دعم إجراءات السيطرة والحماية باستخدام إضاءة خارجية فعالة وقوية. كما ويفضل طلاء جدران البناية باللون الأبيض أو الألوان الفاتحة لتسهيل عملية مراقبتها ليلاً.

3- 4 اختيار قاعة الحاسبة في المبنى:-

عند اختيار قاعة الحاسبة في المبنى، يجب مراعاة الأمور الآتية:-

1- لا يفضل اختيار موقع قاعة الحاسبة في طوابق عالية من البناية لغرض حمايتها عند حصول كوارث معينة كحدوث حريق في الطوابق الوسطى الذي قد يؤدي إلى انهيار الطابق العلوي الذي تقع فيه اجهزة الحاسبة مما يؤدي إلى تناثر أجزائها وكافة الوسائل والمعدات التابعة لها كافة، فضلاً عن جنوح نيران الحرائق نحو الأعلى دائماً.

2- يفضل اختيار الطابق الأول من البناء لقاعة الحاسبة وملحقاتها لان الطابق الأرضي مهدد بالعديد من المخاطر الأمنية لكونه نقطة التماس الأولى مع الوسط الخارجي. لذلك يفضل استغلال الطابق الأرضي للأعمال الإدارية والخدمية، فضلاً عن ان صالة الاستقبال يمكن ان تستغل لمنع دخول الأشخاص غير المخولين إلى غرف المركز وقاعة الحاسبة.

3- يفضل جعل القاعة التي تحتوي على الأجهزة الحساسة للحاسبة في منتصف الطابق وان يحيط بها قاعة إدخال البيانات وغرف المبرمجين ومكاتب العاملين في الخدمات المساعدة على ان تكون القواطع بين الغرف وقاعة الحاسبة من المواد غير القابلة للاشتعال مثل الحديد او الألمنيوم أو الطابوق، ولا يجوز أحداث ثقب أو فتحات خلال هذه القواطع لغرض الإضاءة أو التهوية أو لأي غرض آخر.

4- الغرف فوق وتحت قاعة الحاسبة تكون متساوية من حيث الأهمية ويفضل ان تشغل من قبل المبرمجين والعاملين على تشغيل وصيانة الحاسبة لحمايتها من التخريب أو أن يكون أشغالها لأغراض محددة لا تساعد على زيادة مخاطر الحريق.

3- 5 متطلبات الحماية الأمنية لقاعة الحاسبة الإلكترونية:-

في الفقرة السابقة بينا أن قاعة الحاسبة هي المكان الذي توضع فيه الأجهزة الحساسة للحاسبة وان موقع قاعة الحاسبة لا يكون في الطوابق العليا او الطوابق السفلى لحماية أجهزة الحاسبة عند حصول كوارث معينة مثل الحريق والفيضان. كما ان قاعة الحاسبة يفضل أن تكون بعيدة عن مدخل الطابق لزيادة الجهد الأمني لحماية هذه القاعة من كافة أنواع التهديدات.

لذا تتخذ مراكز الحاسبات جملة من الوصايا لحماية هذه القاعة وعلى النحو

التالي:-

1- اختيار أثاث وتجهيزات قاعة الحاسبة من مواد بطيئة الاشتعال.

2- يفضل استخدام الأرضية الكاذبة لاختفاء أسلاك الكهرباء اللازمة لعمل أجزاء الحاسبة وكذلك وحدات إدخال البيانات. كذلك يمكن الاستفادة من الفسحة تحت الأرضية الكاذبة لمرور أنابيب الماء ومعدات أجهزة التكييف.

3- بلاطات الأرضية الكاذبة يجب ان تكون مصنوعة من المواد غير القابلة للاشتعال وجعل بعض هذه البلاطات متحركة يمكن رفعها وأجراء الصيانة والتنظيف للفسحة تحت الأرضية الكاذبة وبشكل دوري.

4- تسريح ارض الطابق تحت الأرضية الكاذبة إلى أحد زوايا الغرفة التي تتواجد فيها فتحة لتصريف المياه المتجمع نتيجة لعمل أجهزة التكييف او في حالة تسرب المياه لأي سبب آخر، لانه يشكل خطورة على أسلاك الكهرباء الموجودة الأمر الذي يوجب رفع هذه الأسلاك عن ارض الطابق بمسافة كافية.

5- عزل أماكن تواجد الطابعات بقواطع مغلقة تحد من وصول الأشخاص إليها لضمان أمنية المعلومات المطبوعة ذات الدرجة السرية العالية. ويفضل عمل نافذة في أحد جدران قاعة الحاسبة لتسليم المطبوعات والأشرطة دون الحاجة إلى دخول المستخدمين إلى قاعة الحاسبة.

6- من شروط قاعة الحاسبة الأساسية شمولها بمنظومة الإطفاء الطوعية.

7- يجب ان يكون هناك مسافات مناسبة لحزن المواد وخاصة المطبوعات الورقية ووسائل الحزن كالأقراص المرنة والأشرطة المغناطيسية والمواد

الاحتياطية وغيرها وعدم وضع أي مواد من شأنها إعاقة الحركة داخل القاعة أو منع تهويتها.

8- أن تكون هناك مساحات كافية تسمح بتوسيع مركز الحاسبة عند إضافة أجهزة جديدة أو ازدياد عدد العاملين فيه.

3- 6 متطلبات الحماية الإلكترونية للمبنى:-

توفر الرقابة البصرية بواسطة مسؤولي الأمن ونقط الحراسة عدة مميزات منها التحكم الإيجابي في حركة الأشخاص الداخلين والخارجين، وفي حركة المواد. بالإضافة إلى الرقابة بواسطة مسؤولي الأمن قد يستخدم بعض منظومات المراقبة الإلكترونية ضد المتسللين أو المخربين أو أي شخص يحاول إلحاق الأذى بأمن مركز الحاسبة. ولا يشترط تواجد جميع المنظومات، بل ان تواجدها يعتمد بشكل أساسي على نوع التهديدات المحتملة والإمكانات المادية للمركز وحجمه. وتشمل الحماية الإلكترونية المنظومات الآتية:-

1- منظومة المراقبة التلفزيونية:

توضع أعداد من الكاميرات التلفزيونية في الأماكن الحساسة والمهمة في المركز وعلى سبيل المثال في المداخل والممرات المهمة وفي قاعات المركز ومدخل قاعة الحاسبة. وتقوم مجموعة من مسؤولي الأمن بمتابعة هذه الكاميرات وإبلاغ الحرس أو إطلاق صافرة الإنذار عند وجود خطر ما.

2- منظومة الحماية ضد المتسللين باستعمال أشعة ليزر:

تعمل هذه المنظومة بمبدأ انعكاس حزم متوازية من أشعة ليزر عبر قاعة الحاسبة او الممرات المطلوب حمايتها، وعند مرور أي شخص عبر هذه الحزم فانه يعمل على قطعها وبالتالي ستقوم المنظومة بإطلاق صافرة انذار صوتية لتنبيه مسؤول الأمن بوجود متسلل .

3- منظومة الحماية ضد المتسللين باستعمال الأشعة فوق البنفسجية او تحت الحمراء، وتعمل بنفس مبدأ أشعة ليزر.

4- منظومة الحماية ضد المتسللين عن طريق إكمال دائرة كهربائية:

تصبح هذه المنظومة فعالة عندما يطأ المتسلل بلاطة او سجادة تحتوي في تركيبها الداخلي على مفتاح يعمل بمجرد الضغط على هذه البلاطة او السجادة حيث تطلق المنظومة جهاز الإنذار الصوتي، وتوضع هذه السجادة او البلاطة في المداخل المهمة بعد مغادرة الجميع .

3- 7 المواد التي يسمح بدخولها إلى قاعة الحاسبة:-

تقع على عاتق مدير مركز الحاسبة مسؤول او مسؤول الأمن فيه فحص المواد التي تدخل قاعة الحاسبة ومنع قسم منها وحسب ما يشكل ذلك من خطورة على عمل الحاسبة وسلامة العاملين فيها. وفيما يلي قائمة بالمواد التي يمنع دخولها إلى قاعة الحاسبة في جميع الأوقات:-

1- جميع أنواع المغناطيس (الصناعي والطبيعي).

2- المواد الغذائية والمشروبات بأنواعها.

3- المعدات الشخصية الكهربائية والإلكترونية.

4- الأسلحة والمتفجرات والمواد الحارقة.

5- الأجهزة القادرة على إطلاق غازات سامة (عدا مطافئ الحريق).

6- جميع المواد المتطايرة وسريعة الاشتعال (عدا تلك التي تستخدم لأغراض الصيانة).

7- آلة التصوير ألا بموجب تصريح من مدير المركز او مسؤول الأمن.

كما يمنع التقارير غير المصرح بها حول سلسلة من الإجراءات التي تخص البرامج والملفات المطلوبة للدخول إلى النظام، وكذلك استنساخ الملفات والتقارير المعدة من قبل مركز الحاسبة.

3- 8 أمن الأجهزة البيئية لمركز الحاسبة الإلكترونية:-

لظروف التشغيل المثلى للحاسبة الإلكترونية حدود سماح يجب أن لا تعتبر بديلاً لما هو محدد في مواصفات التشغيل لقاعة الحاسبة حيث يفضل ان لا تزيد حدود السماح لدرجة الحرارة عن $2 \pm$ م وللرطوبة 10 % Rh على أن لا يستمر ذلك فترة طويلة، يقوم خلال هذه الفترة المشرفون على هذه المنظومة بالوقوف على أسباب تجاوز هذه الحدود والعمل على إعادتها ضمن الحدود المقررة. ويفضل إيقاف منظومة الحاسبة الموجودة في مركز الحاسبة عند ارتفاع أو انخفاض درجة الحرارة أو ارتفاع أو انخفاض درجة الرطوبة أو عندما يقرر المهندس المختص عدم ملائمة جو القاعة لتشغيل منظومة الحاسبة لأي سبب.

3- 9 منظومة الطاقة الكهربائية:-

يمكن اعتبار أجهزة ومعدات تجهيز الطاقة الكهربائية كوسيلة لعمليات التخريب عن طريق التلاعب بمستويات الطاقة المجهزة للحاسبة الإلكترونية مما يلحق أضرار كبيرة بمنظومة الحاسبة. لذلك يفضل جعل المحولات وخطوط التغذية للمركز بالإضافة إلى أجهزة التغذية الكهربائية المستمرة (ups) uninterruptible power supply والبطاريات الملحقة بها فضلاً عن معدات توليد الطاقة الكهربائية الخاصة بالحالات الطارئة وغيرها من المعدات الأخرى في مناطق مقفلة أو مسيجة يمكن مراقبتها من الخارج بسهولة ومنع الاقتراب منها.

3- 9- 1 تغذية مركز الحاسبة بالطاقة الكهربائية:-

لتغذية مركز الحاسبة بالطاقة الكهربائية يؤخذ بنظر الاعتبار ما يلي:

أ- يجب ان تتم تغذية مركز الحاسبة بالطاقة عبر مصدرين مختلفين على الأقل ويمكن التحويل من أحدها إلى الآخر بسرعة ويسر، وكل مصدر يتصل بمحطة طاقة كهربائية منفصل أو على الأقل يتصل بأجزاء منفصلة من محطة توليد الطاقة الكهربائية.

ب- لا يشترك مركز الحاسبة وبالذات منظومة الحاسبة مع أية منظومة أخرى لما في ذلك من مشاكل كثيرة تتعلق بأستقرارية مصدر الطاقة التي من شأنها عرقلة عمل المركز والحاسبة ويلحق أضراراً بمعداتنا.

3-9-2 منظومة توليد الطاقة الكهربائية في الحالات الطارئة:-

عند انقطاع مصدر التغذية الرئيسي، هناك عدة طرق للحصول على الطاقة الكهربائية منها:-

أ- منظومة توليد الطاقة الكهربائية الأساسية BASIC UPS:

تستطيع هذه المنظومة من توفير الطاقة الكهربائية المستمرة لمدة تصل إلى 45 دقيقة اعتماداً على حجم البطاريات المتوفرة في المنظومة، مما يتيح للعاملين في مركز الحاسبة من حفظ المعلومات وإيقاف المنظومة بشكل متكامل عند عدم توفر مصدر بديل للطاقة.

ب- مولدة الطاقة الكهربائية البديلة:

وهي أحد أجزاء منظومة الطاقة الأساسية، وتعتمد هذه المولدة على محرك ديزل أو تربين غازي، ويتم السيطرة على مولدة الطاقة المساعدة هذه وحدة سيطرة تقوم بتشغيلها عند انقطاع مصدر الطاقة الرئيسي- وربطها الى منظومة الحاسبة بعد وصولها إلى درجة الاستقرار المطلوبة لاداء منتظم. وهذه المولدة تستمر في العمل طالما كان الوقود (الديزل أو LPG) متوفر، لذلك يجب خزن كمية كافية من الوقود المناسب في الموقع او توفر إمكانية التجهيز.

ويشترط بمولدة الطاقة المساعدة هذه توفير قدرة كافية لتشغيل منظومة الحاسبة والإضاءة الضرورية وفي بعض الأحيان مصعد واحد على الأقل،

بالإضافة إلى أجهزة الإنذار والاتصالات. كما ويفضل توفر مفتاح تحويل يدوي للتحميل مع مفتاح التحميل الآلي الموجود في وحدة السيطرة لاستعماله عند عطل الأخير.

3- 10 مكافحة الحرائق:-

يعد خطر الحريق في الغالب التهديد الرئيسي لمراكز الحاسبات، حيث يسبب الحريق اfdح الخسائر بوقت قصير، وتعتبر الوقاية منه إحدى العضلات الرئيسية التي ينبغي لادارة المركز والعاملين فيه إيجاد الحلول له. والحريق يمكن ان يكون نتيجة لحوادث عديدة مثل التماس الكهربائي أو تسرب غاز سريع الاشتعال أو إلقاء متفجرات.

3- 10- 1 سبل تقليل الخسائر عند حدوث الحريق في مركز الحاسبة:-

- 1- توفر معدات الإطفاء المناسبة داخل مركز الحاسبة وان تكون سهلة الاستخدام وموزعة في جميع الأماكن المهمة في المركز.
- 2- يجب ان توضع علامات توضيحية للدلالة على مكان وجود معدات الإطفاء وأبواب الطوارئ.
- 3- يجب فحص المطافئ وأجهزة منظومة الغاز وبشكل دوري.
- 4- توفير مفتاحان رئيسيان للطاقة الكهربائية أحدهما قرب غرفة السيطرة console والآخر في المدخل الرئيسي لقاعة الحاسبة. هذه المفاتيح يجب ان

تكون معلومة للجميع وبشكل واضح، لذلك يجب شرح المهام التي وجدت من اجلها والكيفية التي يتم بها إغلاق الأجهزة.

5- عند دخول العاملين إلى مركز الحاسبة تسجل أسمائهم ويتم تأشير خروجهم أيضاً لمعرفة عدد العاملين وهويتهم عند حدوث الحريق، ولسهولة التأكد من خلو المبنى استناداً إلى القائمة المذكورة.

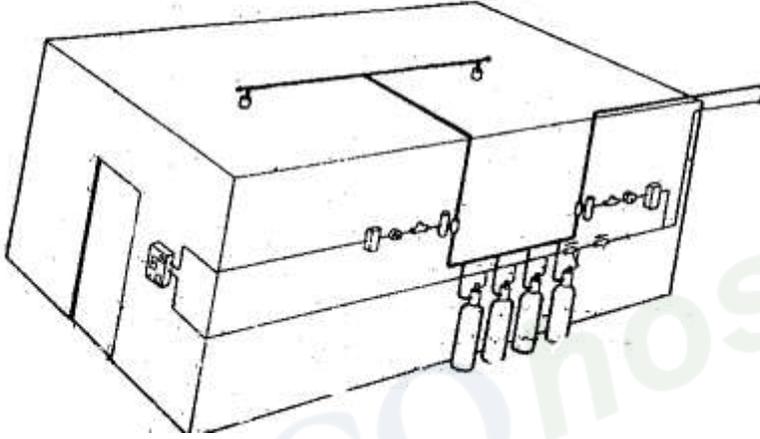
6- على العاملين مغادرة المبنى فور سماعهم صفارة الإنذار على ان يجتمعوا في نقطة محددة سلفاً لمطابقة القائمة المذكورة في الفقرة (5) للتأكد من خروج الجميع.

7- نسخ الملفات والبرمجيات وتوثيق الإجراءات المتبعة في التشغيل والدخول إلى الحاسبة بحيث تكون الوثائق دقيقة وحديثة، ويجب ان تحفظ في خزانات محصنة ضد الحريق والسرقة. ويفضل أن تخزن في بناية أخرى خارج مركز الحاسبة وذلك لاعطاء حماية إضافية.

3- 10- 2 منظومة الإطفاء الطوعي:-

يفضل استخدام منظومة الإطفاء التي تعمل بغاز الهالون Halon 1301 الذي يخدم عملية الاحتراق عند نشره بتركيز معين رغم ارتفاع تكاليفه في قاعات الحاسبات وأماكن خزن الأشرطة والأقراص والمواد. وعلى الرغم من مخاطر هذا الغاز عند استخدامه بتركيز عالية على العاملين ومنعاً من حدوث اية حوادث يفضل إطلاق صفارة الإنذار لتنبية العاملين لمغادرة المكان قبل إطلاق الغاز. وعند استخدام هذا الغاز في إطفاء الحريق فانه من الحكمة بعد ذلك

فتح الشبائيك او استخدام معدات التهوية اليدوية لتغيير هواء الغرفة
بالهواء الخارجي.



شكل رقم (2)

منظومة إطفاء طوعية بغاز الهالون

3- 10- 3 الإجراءات المتخذة عند حدوث حريق:-

يجب تدريب جميع العاملين في مركز الحاسبة على سبيل الوقاية من الحريق
واستخدام المعدات اليدوية المتوفرة وان تعلن الملاحظات الهامة لمكافحة الحريق
بشكل واضح فيما يخص:-

1- إغلاق المفاتيح الرئيسية للطاقة الكهربائية في مركز الحاسبة ووسائل التهوية
والأجهزة المساعدة.

- 2- الاتصال بالدفاع المدني في المنطقة مع ذكر أرقام الهواتف.
- 3- مواجهة الحريق بما يتيسر من معدات إطفاء الحريق (مطافئ الحريق مثلاً).
- 3- 10- 4 تجهيزات ضرورية لمواجهة الحالات الطارئة:-
 - 1- جهاز لاسلكي يدوي يؤمن الاتصال المباشر مع مركز الطوارئ في البناية ومكبر صوت لاستعماله عند الحاجة.
 - 2- مصباح يدوي يعمل على البطارية واحد في الأقل.
 - 3- عدة إسعاف أولية.
 - 4- قناع وقاية واحد في الأقل.
 - 5- خوذ واقية من الصدمات.
- 3- 11 جرد المعدات:-

في حالة حدوث حريق كبير يتم التحفظ على كافة الوثائق والأشرطة والأقراص المتخلفة بعد الحريق، وتتم متابعة هذه العملية أثناء الإطفاء أو بعده وإنقاذ ما يمكن إنقاذه من هذه المواد أثناء إخلاء البناية قدر الإمكان.

أسئلة الفصل الثالث

- 1- عدد أهم السمات الأساسية الواجب توافرها عند اختيار موقع مركز الحاسبة.
- 2- عدد أهم الملاحظات الواجب اتخاذها عند وضع التصميم الهندسي لبنية مركز الحاسبة.
- 3- عدد أهم الأمور الواجب مراعاتها عند اختيار موقع قاعة الحاسبة.
- 4- عدد أهم الوصايا الواجب اتباعها لحماية قاعة الحاسبة الإلكترونية.
- 5- عدد أهم المواد التي يمنع دخولها الى قاعة الحاسبة.
- 6- ما هي أهم سبل تقليل الخسائر عند حدوث حريق في مركز الحاسبة.
- 7- ما هي التجهيزات الضرورية لمواجهة الحالات الطارئة.

EBSOHOST®

الفصل الرابع أمن الوثائق والمعلومات

4- 1 المقدمة:-

ان القليل من المؤسسات الخاصة تمتلك أسلوباً منظماً لحماية معلوماتها، ومن جانب آخر فان المؤسسات الحكومية لها تاريخ طويل في حماية المعلومات والوثائق السرية. أن الوثائق ذات السرية العالية يجب حفظها في مواقع خاصة بحيث أن أي تغيير في مواقعها يعتبر دليل على عملية تلاعب في هذه الوثائق، وقد يتطلب ذلك مراجعة مستمرة لهذه الوثائق وخاصة عند تغيير الموظف المسؤول أو تركه للعمل.

4- 2 تصنيف المعلومات:-

جرت العادة أن تقوم المؤسسات بتصنيف وثائقها ومطوباتها بدرجة سرية ملائمة. وفيما يلي بعض درجات التصنيف وهي بمثابة خطوط يسترشد بها عند دراسة اختيار درجات تصنيف المعلومات، وهذه الدرجات هي:-

1- سري للغاية TOP SECRET

وهي أعلى درجات التصنيف حيث تصنف بهذه الدرجة الوثائق عظيمة الحساسية والتي لها تأثير كبير على سلامة المؤسسة والتي تحاول الجهات المعادية الحصول على مثل هذه المعلومات. يقتصر توزيع معلومات هذه الدرجة على كبار المسؤولين عن مصالح المؤسسة في مجال الاختصاص. وتعطى النسخ

الورقية من هذه المعلومات أرقاماً متسلسلة وتسلم إلى أشخاص محددين بالاسم ولا يسمح لحامل النسخة نفسه بإفشاء معلوماتها.

2- سري SECRET

وهي الدرجة الثانية من حيث السرية، وتصنف بهذه الدرجة الوثائق الأقل أهمية والتي سوف تعرض المؤسسة للخطر عند انتهاكها من قبل غير المخولين. ويقتصر توزيع هذه المعلومات على أفراد مخولين رسمياً يحق الاطلاع عليها.

3- رسمي CONFIDENTIAL

التصنيف بهذه الدرجة يتضمن جميع الوثائق التي يمكن أن تضر- بمصالح المؤسسة أو التفاصيل التي ستكون محرجة للمؤسسة عند إفشائها.

4- محدود RESTRICTED

هذه الدرجة قد لا توجد في تصنيف بعض الدول وتطبق على المعلومات أو المطبوعات التي ربما لا تخلو من فائدة للجهات المعادية (المنافسة) والتي لا تفضل المؤسسة أن تراها منشورة في الصحف اليومية، مثل المعلومات المتاحة لأي موظف، ولفروع المنشأة حسبما تنص عليه الاتفاقات المعقودة بينها.

5- غير مصنفة UNCLASSIFIED

جميع المعلومات الأخرى والمطبوعات يمكن أن تسمى غير مصنفة ولا تنطبق عليها أي مقاييس للحصانة، (مثل معلومات وصف وتسعير المنتجات والبرامج الزمنية للإنتاج وطلبات المناقصة وغيرها).

ان بعض المؤسسات قد يناسبها استخدام الدرجات الخمس معاً، بينما البعض الآخر يكتفي قسم منها.

4- 3 إجراءات حماية البيانات الخاصة بمركز الحاسبة:-

تعد المعلومات الموجودة (المحفوظة) على أي وسط خازن للمعلومات مشمولة بدرجات التصنيف المذكورة سابقاً، فالبطاقات المثقبة والأشرطة الورقية المثقبة والأوراق والأشرطة والأقراص المغنطة تعامل معاملة أي مطبوع آخر من ناحية الحماية الأمنية.

ولذلك فان جميع هذه الوسائل يجب أن تؤشر بدرجة تصنيف المعلومات المخزونة فيها، على ان تكون تلك الإشارات من النوع الثابت وغير القابل للإزالة.

أ - البطاقات المثقبة والأشرطة الورقية المثقبة:-

لتحديد درجة التصنيف للبطاقات المثقبة والأشرطة الورقية المثقبة تستعمل مراكز الحاسبات ألوان مميزة. فالمعلومات ذات الدرجة سري للغاية تكون لون بطاقتها او أشرطتها باللون الأحمر الضارب للصفرة. اما المعلومات ذات الدرجة سري تكون بطاقتها وأشرطتها ذات اللون الوردي. اما المعلومات ذات الدرجة رسمي تكون بطاقتها وأشرطتها ملونة باللون الأخضر الفاتح. ويستخدم اللون الأصفر الفاتح لتمييز المعلومات ذات الدرجة محدود واللون الأبيض للبطاقات والأشرطة ذات المعلومات غير المصنفة.

وفي بعض العمليات الحساسة والخاصة ربما ينصح باستعمال بطاقات وشرطة ورقية مطبوعة مسبقاً بدرجة السرية. ويتم ذلك بطبع درجة السرية في الزاوية العليا اليمنى لكل بطاقة او على طول الشريط الورقي بمسافة 15 أنج بين إشارة واخرى.

ب - الأشرطة والأقراص المغنطة:-

الأشرطة والأقراص المغنطة يمكن الإشارة الى درجتها السرية مباشرة عند إجراء عملية الحفظ وذلك بان تكون درجة السرية بشكل رمز يضاف الى اسم الملف ولجميع الوثائق المصنفة على أن يكون آخر رمز في اسم الملف. فمثلاً يرمز الى درجة سري للغاية بالحرف T وللدرجة سري بالحرف S وللدرجة رسمي بالحرف C والمحدود بالحرف R ويمثل الحرف U درجة غير مصنف، وعليه يكون اسم الملف الذي يحتوي معلومات صنفت بالدرجة سري VWXYZS بدلاً من VWXYZ وهكذا.

أو يشار إلى درجة السرية على الأجزاء المساعدة مثل بكرة الشريط الورقي المثقب أو الغطاء البلاستيكي حيث تستخدم اللاصقات أو أقلام خاصة.

4- 4 إجراءات حفظ وأتلاف الأشرطة والأقراص المغنطة:-

تعتبر المواد التي تستخدم لحزن أو حفظ المواد المصنفة (كالأشرطة والأقراص المغنطة) ذات أهمية تعادل أهمية المعلومات التي تحتويها. لذلك فان

عملية الحفظ والإتلاف لهذه الأوساط الخزنية يجب ان تحظى بالعناية والحماية المناسبة لكل درجة.

أ - حفظ الأشرطة والأقراص الممغنطة:-

عند حفظ الأشرطة والأقراص الممغنطة التي تحمل معلومات مصنفة، يجب ان يشار إلى درجة أعلى تصنيف للمعلومات المخزونة على ذلك الشريط او القرص. وعند مسح أو حذف هذه المعلومات من الشريط او القرص فانه يجب ان يحتفظ به بدرجة التصنيف السابقة نفسها وان لا يستخدم الا لحفظ معلومات جديدة بدرجة السرية نفسها أو أعلى من تلك الدرجة.

الوثائق ذات السرية العالية يجب ان تخزن في موقع خاص بحيث ان ازلتها من موضعها يشكل دليل مباشر على عملية التلاعب غير الموثقة عند عملية المراقبة البصرية. وان تتم عملية مراجعة مخزنية سنوية لهذه الوثائق او عند تغيير الموظف المسؤول أو تركة العمل في المؤسسة.

ب - إتلاف المواد المصنفة:-

تحرص الكثير من المؤسسات على إتلاف المواد المصنفة (مثل البطاقات المثقبة، الأشرطة الورقية المثقبة، الأشرطة والأقراص الممغنطة) عند وجود محذور آمني من ارسال الأقراص والأشرطة الممغنطة لاصلاحها لدى الشركة او عند عدم وجود حاجة لشريط معين نتيجة لانخفاض جودته ويحتوي على معلومات مهمة جداً. وبالرغم من ان عملية الاتلاف تكبد هذه المؤسسات تكاليف باهضة

من أجراء ذلك، ألا ان هذه العملية تصبح معقولة وطبيعية جداً عندما ينظر إليها من وجهة نظر أمنية، لاحتمال استفادة الجهات المنافسة او المعادية من هذه المواد عند عدم إتلافها ورميها.

ان افضل وسيلة لأتلاف المواد المصنفة بعد إقرار إتلافها هو حرقها. ويجب ان تجمع مثل هذه المواد في حاوية مخصصة لحرق النفايات قبل إجراء عملية الحرق وان تكون هذه الحاوية مقفلة بشكل جيد.

ان عملية الإحراق يفضل ان تتم داخل المؤسسة وبموافقة الإدارة وبأشراف شخصين او اكثر من المستخدمين الموثوق بهم. ويتم تسجيل المواد التي يتم أتلافها في سجل خاص وتثبيت التاريخ والوقت الذي جرت فيه عملية الإتلاف والتوقيع على ذلك. كذلك الحرص على عدم تطاير أي جزء منها والتأكد من ان عملية الإتلاف قد تمت بشكل جيد.

ولغرض أتلاف المواد المصنفة تتخذ الإجراءات التالية:-

1- قبل حرق الأقراص المغنطة يجب إزالة الأقراص من محورها وتكسيورها إلى قطع بواسطة فأس أو مطرقة ومن ثم حرقها بشكل جيد حتى تتحول إلى كتلة من الألمنيوم والبلاستيك المصهور.

2- أما الأشرطة المغنطة فانه يجب أن تقسم قطعياً إلى قسمين او اكثر ورفع الأجزاء (القطع) عن البكرة ثم بعد ذلك يقطع كل جزء إلى شرائط بعرض 1/32 أنج أو اقل. ان فكرة التقطيع فكرة جيدة ولكن يجب ان تسبق عملية

الحرق ولا تكون بديلة عنها، أي أن عملية التقطيع تعتبر إجراء تمهيدي لعملية الحرق التي يجب أن تتم في المكان المخصص لذلك.

EBSCOhost®

أسئلة الفصل الرابع

- 1- عدد درجات تصنيف المعلومات مع الشرح المختصر.
- 2- بين باختصار كيف يمكن تحديد درجة سرية الأشرطة والأقراص الممغنطة.
- 3- تكلم باختصار عن أتلاف المواد المصنفة.

EBSCOhost®

الفصل الخامس أمن الاتصالات

5- 1 المقدمة:-

في الوقت الذي أصبحت فيه المعلومات التي يتم تخزينها داخل ذاكرة الحاسبات على جانب كبير من الأهمية والخطورة، فإن مسألة الحفاظ عليها من التسرب او السرقة او التلاعب في ذات الوقت أصبحت أيضاً مشكلة ومصدر للقلق والمتاعب. وهذا مما دفع بالعديد من الشركات والباحثين ان يولوا هذا الجانب الأهمية التي تستحقها وذلك لحماية المعلومات والجهود والأسرار من السارقين او المتطفلين.

ان اكثر طريقة يمكن الحصول بها على المعلومات بصورة غير شرعية في نظام معين هي التطفل على أنظمة الاتصالات. وقد تضاعفت حوادث التطفل في العديد من المجالات منها الاقتصادية والتجارية والعسكرية خلال العقدين السابقين وحتى الآن مقارنة مع الفترات السابقة حيث كانت أنظمة الاتصالات وطرق التطفل عليها اقل تطوراً. أما في الوقت الحاضر فيتم نقل المعلومات بطرق متطورة جداً ولذلك يتم التطفل عليها بطرق متطورة أيضاً.

5- 2 الاتصالات وثورة المعلومات:-

أن ثورة المعلومات التي حصلت في العديد من الجوانب ومنها في جانب علم الاتصالات قد بدأت تأخذ مكانها في المجالات المختلفة كالمجال التجاري

والصناعي والعسكري. اذ كان الاتصال في السابق يتم بواسطة الحمام الزاجل وكذلك بواسطة الجياد. أما أول خدمة بريدية منظمة أنشئت في بغداد عام 1150م كانت بواسطة استخدام الحمام الزاجل. كانت الرسائل توضع في كبسولات خاصة يجري تثبيتها في رجل الحمامة او فوق ظهرها. وفي سنة 1844م استطاع صمويل مورس بعد تجارب شاقة من إجراء اتصالاً تلغرافياً نقل مورس فيه أول رسالة تلغرافية لمسافة (40) ميلاً. وبهذا يكون مورس قد فتح الباب أمام ابتكارات عديدة في حقل الاتصالات حيث اصبح في الإمكان في سنة 1890م استلام الرسائل التلغرافية مطبوعة على الآلة الكاتبة. وقد قاد ذلك إلى تطوير نظام الإرسال المتعدد وتعميمه في سنة 1914م، والى تطوير الطابعة البرقية (Tele-printer) وتعميم استخدامها في عام 1920.

وهكذا طورت خلال القرنين الماضيين قدرة البشر على الاتصال كما تطورت السرعة التي يتم فيها هذا التواصل بحيث ان سرعة نقل صفحة واحدة من المعلومات عبر مسافة طويلة قد تضاعفت بنسبة تبلغ عشرة ملايين. إذ في إمكان الألياف البصرية الآن أن تستخدم الليزر في اتصالاتها والأقمار الصناعية أن تبث بليون بت من المعلومات في الثانية. ومن هذا نستطيع ان نتصور مقدار التطور الذي حصل في علم الاتصالات وما زال التطور مستمراً وبخطوات سريعة جداً.

مما تقدم يمكن ان نعرف الاتصالات بأنها عبارة عن نقل معلومات من نقطة إلى أخرى. أما مكونات نظام الاتصالات فانه يتألف من:-

- أ- مصدر المعلومات وهو الذي يحدد كمية ونوع المعلومات المطلوب نقلها.
- ب- وسيلة الإرسال أو الأداة التي تتلقى المعلومات وتحولها إلى إشارات أو رموز معينة ثم تقوم بنقلها بدقة.
- ج- قناة الاتصال وهي الوسط الذي تنتقل الإشارات أو الرموز عبره بوضوح وبأقل وقت ممكن.
- د- وسيلة الاستلام أو الأداة التي تتلقى الإشارات أو الرموز وتقوم بتحويلها من رموز وإشارات إلى معلومات واضحة.
- هـ- المستفيد وهو الذي يتلقى المعلومات في النهاية.
- من الممكن ان يتم الاتصال بواسطة الكلمة المكتوبة أو المسموعة، الصوت، الصورة، الإيماء، والإشارات المختلفة. وبما أن الغرض من الاتصالات هو نقل المعلومات بين مختلف المحطات، لذلك فان هذه المعلومات تكون معرضة خلال انتقالها بشكل كبير للسرقة والتطفل. وتختلف درجة وصعوبة هذا التطفل على نوعية واسطة الاتصال، فهناك وسائط يكون فيها التطفل قليلاً وصعباً، وهناك وسائط نقل اخرى يكون فيها التطفل بشكل كبير وبطرق بسيطة ويمكن توضيح إمكانية التطفل الغير المشروع على شبكة اتصالات نموذجية كما في الشكل (3).

5- 3 عناصر أمن الاتصالات:-

يمكن تقسيم أمن الاتصالات بشكل عام الى العناصر الاتية:-

أ- أمن خطوط الاتصالات السلكية.

ب- أمن خطوط الاتصال اللاسلكية.

أمن خطوط الاتصالات السلكية:-

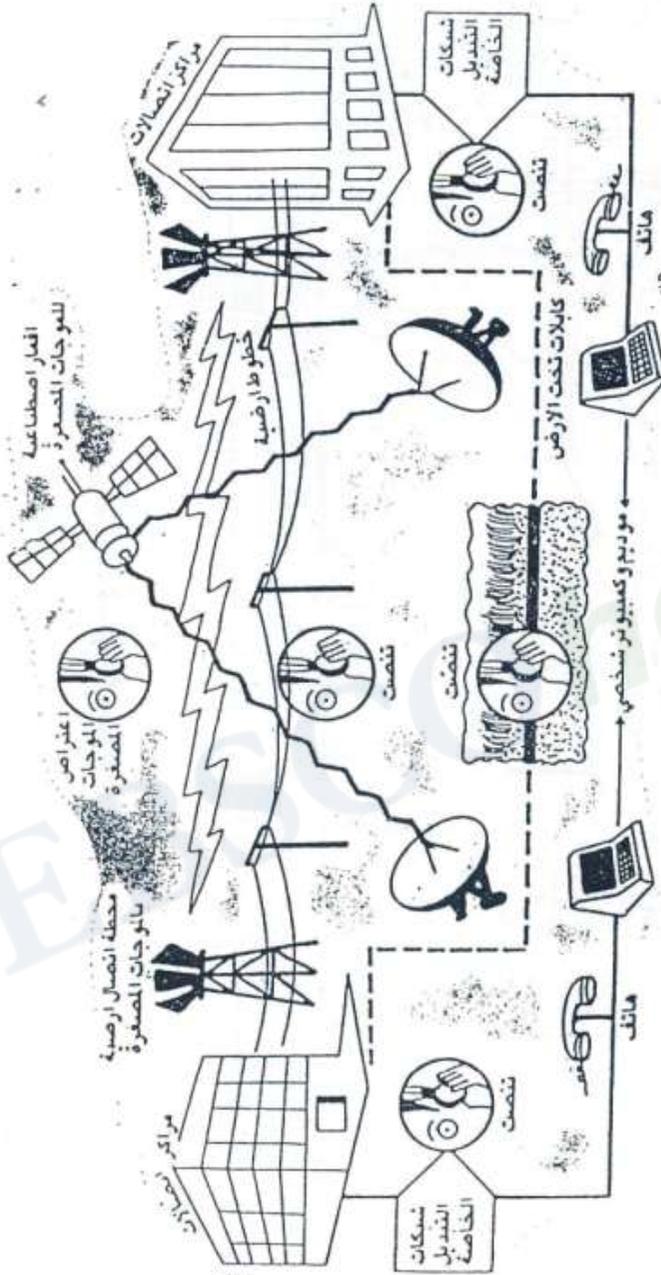
أولاً - الإجراءات الفنية لحماية خطوط التناقل:-

للحصول على إجراءات أمينة يجب البدء بعملية التحري كسياق عام من بناية البدالة والى مركز الحاسبة وعلى النحو التالي:

1- يفضل ان تمر خطوط الاتصال بأقل عدد ممكن من البدالات او نقاط التحويل وكلما اقترب خط الاتصال إلى الخط مباشرة كلما قلت تهديدات الاستراق.

2- عدم ترك كابينات الخطوط الهاتفية التي تمر بها خطوط المعلومات وأحكام عملية الصيانة القائمة عليها وتحديد الأشخاص الذين يسمح لهم بصيانتها وعدم تركها سهلة المنال للمسترقين اللذين يتحلون صفة عمال الصيانة لعمل توصيلات خاصة لاستراق المعلومات من خطوط الاتصال الخاصة بالحاسبة، وربطها الى خط هاتفى محدد تكون معدات الاستراق مثبتة عليه سلفاً.

3- يفضل جعل خطوط تناقل البيانات غير مؤشرة وتمر عبر كابل يحتوي على عدد كبير جداً من خطوط الاتصال مما يجعل عملية العثور عليه صعبة وتستغرق وقتاً وجهداً كبيراً.



(اعتراض شبكات الاتصالات)

4- وضع التقاسيم الهاتفية في أماكن يسهل مراقبتها مع أقفالها بشكل دائم والتأكد من سلامة القفل.

5- التأكد من هوية عمال صيانة الهاتف وجعلهم موضع شك حتى تتوفر القناعة بسلامة هوية هؤلاء العمال.

6- ترقيم كافة الخطوط الهاتفية داخل صندوق التقاسيم بأرقام مجردة وبدون تمييز خطوط الحاسبة عن باقي الخطوط مما يوفر مراقبة سهلة للأشخاص المخولين ويربك المسترقين.

7- عدم ابقاء من جهاز الهاتف مرتبطاً بالخط عند البدء بعملية تبادل البيانات وذلك لكثرة المخاطر الأمنية التي قد يسببها الجهاز لكونه هدفاً ملائماً لزراعته بمعدات التجسس والاستراق المتنوعة.

ثانياً - دلائل وجود مسترق على خط تناقل البيانات:-

أن العوارض التالية تعطي مؤشراً لاحتمال وجود مسترق على خط الاتصال الهاتفي، وقد تتباين هذه العوارض باختلاف المسافة والأجهزة المستخدمة إلا أنها تشترك تقريباً بالعوارض المدرجة التالية:-

1- وجود تشويش ملحوظ على خط الهاتف.

2- انخفاض درجة وضوح البيانات المرسلة (أو ما يقابل بانخفاض شدة الصوت أو نغمة الاشتغال في الاستعمال الاعتيادي)، وكثرة حدوث أخطاء أو فقدان البيانات المرسلة.

3- لا تهمل قول أحد زملائك اللذين يقولون بأنهم حاولوا الاتصال بالمركز (خط تبادل البيانات) ولكن الخط كان مشغولاً، وأنت تعرف بصورة قطعية بعدم استخدام أحد للهاتف في ذلك الوقت.

وهناك أجهزة استراق حديثة لا تترك أي من العوارض المذكورة سابقاً لذا كن حذراً وشكوكاً واطلب فحص الخطوط على فترات غير منتظمة من قبل الجهات المختصة بالتنسيق مع مسؤول الأمن في المركز.

أمن خطوط الاتصال اللاسلكية:-

ويشمل المعلومات التي تنقل لاسلكياً بين مراكز الحاسبات بشكل مباشر او عبر محطات تقوية، وعلى الرغم من ان إمكانية الاستراق ممكنة ألا ان المسترق لا يفضلها أحياناً بسبب الصعوبات التي تواجهه أثناء عمله، حيث يتطلب ذلك معدات خاصة ومعدات كبيرة وأحياناً أخرى يتطلب عمله ان يكون واضحاً ومكشوفاً ويمكن أجمال التهديدات المحتملة لعملية بث البيانات على النحو التالي:-

1- استعمال أجهزة استقبال من قبل المسترق تعمل على نفس ترددات المرسلات المستعملة في بث البيانات بين مراكز الحاسبات، وقد تتباين إمكانية هذه المستقبلات ألا أن عملها يتطلب ان تكون قريبة من مراكز الحاسبات في اغلب الأحيان.

2- اعتراض خط حزمة المايكرويف المستخدمة في نقل البيانات.

5- 4 إجراءات أمن الاتصالات:-

تستخدم خطوط الاتصال كمسار لتدفق المعلومات بين مختلف نقاط التقاط المصدر والاستلام ونقاط التحويل في شبكة المعلومات، ويوفر العدد الكبير من منتجي خطوط الاتصالات والتنوع الهائل فيما يعرضون إمكانيات واسعة تساعد مصممي الشبكة على الاختيار من بين عدد متزايد من نظم المكونات وقد يحول حجم الشبكة والعوامل الجغرافية الأخرى دون تجهيز الشبكات بخطوط اتصال من شركة منتجة واحدة. وهنا تبرز مشكلة التوافق وضرورة اعتماد مستوى معين من القياسية للمحافظة على كمال البيانات. وقد يكون من المفيد هنا التعرف على بعض المعايير التي تحدد الخصائص التشغيلية لخطوط الاتصال لكي نتعرف على مكان الخطر واحتمالات الانتهاك الموجودة. وتنطبق هذه المعايير على جميع فئات خطوط الاتصال.

1 - نطاق الترددات BANDWIDTH:-

مقياس سعة خط الاتصال معبراً عنه بعدد الأرقام الثنائية في الثانية (BPS: BITS PER SECOND) أو عدد التمثيلات في الثانية (CPS: CHARACTER PER SECOND) وتستخدم لتحديده ثلاث مجموعات قياس هي:-

- أ- نطاق ضيق: عشرات التمثيلات في الثانية.
- ب- نطاق صوتي: مئات الى الآف التمثيلات في الثانية.
- ج- نطاق عريض: عشرات الى مئات الآلاف من التمثيلات في الثانية.

2 - النقاط النهائية:

معيار تحديد عدد النقاط التي يصل بينها خط الاتصال، فيكون:

أ- بين نقطتين: خط اتصال واحد يصل بين نقطتين نهائيتين.

ب- متعدد النقاط: خط اتصال واحد يصل بين ثلاثة نقاط نهائية او اكثر،

منفصلة او متباعدة جغرافياً.

1- القنوات:

معيار لتحديد عدد قنوات المعلومات التي تبث على خط الاتصال

أ- قناة مفردة: حيث يستخدم كل نطاق الترددات (السعة) في خط الاتصال

لقناة معلومات واحدة.

ب- متعدد القنوات: حيث تقسم كل سعة خط الاتصال الى قنوات متعددة لبث

المعلومات وذلك باستخدام أساليب الإرسال المتعدد بتقسيم الوقت او

بتقسيم الترددات.

2- طريقة البث:

معيار لتحديد الطريقة التي تنقل بها المعلومات على خط الاتصال. ويكون

على شكل:-

أ- متناظر (منطقي): هو الشكل السائد حالياً، وفيه تستخدم أجهزة الموائمة

لتحويل المعلومات الرقمية من أجهزة نقاط المصدر و الاستلام او أجهزة

نقاط التحويل إلى شكل مناسب يمكن بثه على خط الاتصال مباشرة.

ب- رقمي: هو الشكل الأحدث، وفيه توضع المعلومات الرقمية القادمة من أجهزة نقاط المصدر والاستلام والتحويل، للبت المباشر على خط الاتصال، وبذلك تنتفي الحاجة إلى الاستعانة بأجهزة المواءمة. ولا تزال تجري حالياً عمليات بحث وتطوير إمكانيات استيعاب الترجمة الرقمية للصوت والأشكال الأخرى من المعلومات على خطوط الاتصال الرقمية.

3- اتجاه البث:-

هو معيار لقدرة خط الاتصال وأجهزة المصدر / الاستلام على البث في اتجاه واحد أو في كلا الاتجاهين. وهناك ثلاثة أساليب يشيع استخدامها هي:

أ- بث في اتجاه واحد SIMPLEX: أي اتصال في اتجاه واحد بين النقطة أ والنقطة ب بحيث تكون أي من أجهزة أ و/ او ب غير قادرة على نقل تدفق الحركة في الاتجاه العكسي.

ب- بث متقطع في الاتجاهين TWO - TERNATE: أي القدرة على نقل تدفق الحركة في كلا الاتجاهين من أ الى ب، او من ب الى أ ولكن ليس في وقت واحد.

ج- بث متزامن في اتجاهين TWO-WAY SIMULTANEOUS

أي القدرة على نقل تدفق الحركة في كلا الاتجاهين من أ الى ب، ومن ب إلى أ في وقت واحد.

أسئلة الفصل الخامس

- 1- ما هي أهم مكونات نظام الاتصالات.
- 2- ما هي عناصر أمن الاتصالات، اشرح واحدة باختصار.
- 3- عدد أهم العوارض التي تعطي مؤشر احتمال وجود مسترق على خط الاتصال الهاتفي.
- 4- ما المقصود بنطاق الترددات، وضح ذلك باختصار.

EBSCOhost®

EBSCOhost®

الفصل السادس الفيروس

6- 1 المقدمة:-

اشتهرت فيروسات الحاسب بقدرتها على الأذى وإحداث الأضرار، حيث ان بعضها يحذف الملفات، أو يقوم بأعمال تخريبية، وبعضها يسبب إزعاجاً بسيطاً فقط، وبعضها لا يلاحظه المستخدم العادي ابداً، ويكفي أن يتمكن البرنامج من إعادة إنتاج نفسه حتى يعتبر فيروساً. وحتى الفيروسات غير المؤذية تسبب بعض الأذى، فهي تستهلك مساحات تخزين على القرص، وجزاً من ذاكرة الحاسب، وتشغل جزءاً من طاقة المعالج، وبالتالي فهي تؤثر على سرعة وكفاءة الجهاز. إضافة إلى ذلك، ان برامج كشف الفيروسات وأزالتها، تستهلك أيضاً موارد الجهاز. ويرى الكثير من المستخدمين، ان برامج مكافحة الفيروسات تبطئ عمل الجهاز بشكل ملحوظ، وهي اكثر تطفلاً عليه من الفيروسات ذاتها، وبعبارة أخرى، تؤثر الفيروسات في عالم الحاسبات، حتى إذا لم تكن تفعل شيئاً.

6- 2 تعريف الفيروس:-

هو عبارة عن برنامج له أهداف تدميرية تهدف إلى إحداث أضرار جسيمة بنظام الحاسب سواء البرامج او الماديات. ومثل أي برنامج تطبيقي آخر، يتم تصميمه وكتابته بإحدى لغات البرمجة من قبل أحد المخربين بهدف إحداث أكبر ضرر ممكن بنظام الحاسب. ولتنفيذ ذلك يتم إعطاءه القدرة على ربط نفسه بالبرامج الأخرى وكذلك إعادة إنشاء نفسه حتى يبدو وكأنه يتكاثر ويتولد ذاتياً

كما ان له القدرة على الانتشار بين برامج الحاسب المختلفة وفي مواقع مختلفة في الذاكرة لتحقيق أهدافه التدميرية.

6- 3 بداية نشوء الفيروس:-

ظاهرة فيروس الحاسب ليست جديدة بل تعود إلى نهاية الأربعينيات، وقد يكون أحد أول الاختصاصيين في علم الكمبيوتر (جون فون نيومان) هو أول من فكر بالأمر إذ نشر مقالاً حول الموضوع في سنة 1949، ثم ظهرت بعض عوارض الفيروس في أوائل الخمسينات ألا أنها بقيت محدودة لان أجهزة الحاسب لم تكن مرتبطة بعضها ببعض في تلك الأيام، وبقي الأمر سراً حتى سنة 1983 عندما تفشى الفيروس في نظام التشغيل UNIX. وقد أثارت ضجة على الساحة العلمية والعملية حيث ظهرت بعض الحوادث الفردية للهواة من صغار المبرمجين قاموا بزرع فيروسات في شبكات الحاسب لشركات تتعامل في مجالات علمية وتطبيقية حساسة. فقد قام روبرت موريس عندما كان طالباً في السنة النهائية بجامعة كورنيل وعمره 23 عاماً بأعداد برنامج المدمر الذي عطل آلاف الحاسبات وأدى ذلك إلى تكليف الشركات الأمريكية ما لا يقل عن 100 مليون دولار ولم تسلم حتى أكبر شركات الحاسب من هذا الفيروس.

وهناك عدة قصص لبداية الفيروس، إذ يقال انه اكتشف عن طريق مبرمج هندي الأصل قام ببرمجة هذا البرنامج الخفي من اجل المحافظة على برنامجه وهو أحد برامج الطباعة استخدم وقتها للصحفيين، حيث أراد حماية برنامجه من النسخ فقام بعمل هذا البرنامج الخفي الذي يدخل على الملفات التشغيلية في

حالة النسخ وتكبير حجم الملفات ومن ثم يقوم بعملية تخريب للملفات التنفيذية. وكان هذا حافزاً للمبرمجين لبرمجة هذا النوع من البرامج وهو للمحافظة على برامجهم.

وعليه فإن البداية الحقيقية لظهور الفيروس يصعب تحديدها. وقد يعتبر عام 1978 أو قبلها بقليل بداية ظهوره. كما أن مشكلة الفيروس بدأت تتعد مع استخدام البريد الإلكتروني باستخدام وسائل الاتصالات COMMUNICATION التي أدت إلى ربط عدد من أجهزة الحاسب بشبكة (NETWORK) والاتصال من خلالها من قبل الآلاف المستخدمين الذين يشتركون في نظام الحاسب وعبر مسافات بعيدة جداً. وقد يكون الفيروس المسمى بفيروس كارت عيد الميلاد (CHRISTMAS CARD). كمثال يوضح انتشار الفيروس خلال (عبر) الشبكة الأكاديمية الأوروبية. هذا الفيروس انتشر في إيران وانتشر كرسالة بريد إلكتروني يقوم هذا الفيروس برسم كارت عيد الميلاد على الشاشة وفي نفس الوقت يقوم بقراءة عناوين المشتركين في الشبكة ويقوم بإرسال نسخة من نفسه إلى هؤلاء المشتركين في الشبكة وانتقل هذا الفيروس بسرعة بالبريد الإلكتروني إلى نظام شمال أمريكا وأدى إلى توقف النظام عن العمل إلى أن قام خبراء بعزل والتخلص من هذا الفيروس.

6- 4 الاسم (فيروس):-

لم تأت تسمية فيروس الحاسب بهذا الاسم عبثاً أو من قبيل الصدفة إذ أن من المعروف ان كلمة الفيروس تطلق على الفيروسات التي تنقل الأمراض من

شخص مريض إلى آخر، وتتكاثر داخل الجسم وتسبب تدمير الأجهزة العضوية. وحيث ان عمل الفيروس الخاص بالحاسبة مشابه لذلك، إذ انه عبارة عن برنامج يربط نفسه ببرامج أخرى ويتكاثر داخل النظام ويتسبب في تدميره لذلك أطلق عليه اسم فيروس.

وهناك بعض التشابه بين الفيروس العضوي وفيروس الحاسب منها الآتي:-

1- يتكاثر الفيروس العضوي ويتسبب في إنشاء فيروسات جديدة كذلك فيروس الحاسب يقوم بإعادة إنشاء نفسه (REPRODUCE IT SELF).

2- عندما تنتقل العدوى إلى الجسم قد يبقى الجسم مدة طويلة دون ظهور اعراض المرض عليه. كذلك تقوم برامج الحاسب بأداء وظائفها لمدة طويلة دون ظهور أخطاء نتيجة وجود الفيروس.

3- يقوم الفيروس العضوي في بعض الحالات بتغير شكله بحيث يصعب اكتشافه كذلك يقوم فيروس الحاسب بتغير شكله ويصعب اكتشافه.

ولغرض التقليل من تأثير الفيروسات يجب اتباع إجراءات وقائية عند البدء باستخدام الحاسب أو عند شراء برامج معينة. قد لا توفر هذه الإجراءات الحماية الكاملة لكنها تتيح للمستخدم افضل استخدام والتقليل من الأضرار الناتجة من الفيروس إلى حد كبير في حالة الإصابة به. وقد تؤدي هذه الإجراءات في حالة الالتزام التام بها إلى التخلص من أية آثار ضارة من الفيروس.

وتختلف إجراءات الوقاية حسب نوع الجهاز ونوع نظام التشغيل وحسب درجة تعرض النظام للإصابة بالفيروس، وان الأجهزة المرتبطة بشبكة الحاسب NETWORK تكون اكثر تعرض للإصابة بالفيروس من الجهاز المنفرد والغير مرتبط بالشبكة.

6- 5 صفات (خصائص) الفيروس:-

ان من بعض صفات الفيروس هي:-

1- القدرة على الانتشار:- كما بينا سابقاً بان وسائل الاتصال الحديثة مكنت الفيروس من الانتقال والانتشار بسرعة إلى ملايين المستخدمين عبر شبكة الحاسبات (NETWORK) كذلك انتقال الفيروس من جهاز إلى آخر عن طريق نسخ البرامج المحتوية على الفيروس.

2- القدرة على الاختفاء:- يستخدم الفيروس وسائل متعددة للاختفاء، من هذه الوسائل ارتباطه بالبرامج الشائعة الاستخدام. كما ان هنالك فيروسات تدخل الى الحاسب كملفات مخفية HIDDEN FILES بحيث لا يستطيع المستخدم ملاحظة وجودها عن طريق عرض الفهرس DIRECTORY. بعض الفيروسات تستقر في الذاكرة مما يصعب على المستخدم ملاحظتها وتبقى في هذا المكان إلى ان تشير الساعة إلى تاريخ معين عندئذ تقوم بتشغيل نفسها وتنفذ أعمالها التدميرية. وهنالك فيروسات تقوم بإخفاء أية آثار لوجودها حيث تبقى البرامج التي تحتوي على الفيروس تعمل بكفاءة دون أخطاء لمدة طويلة وفي نفس الوقت يقوم الفيروس بالانتقال من برنامج إلى برنامج آخر.

3- القدرة على التدمير:- قد يحمل الحاسب برنامج يكون الفيروس مرتبط به وينتقل الفيروس إلى الذاكرة ويبقى ساكناً هناك إلى ان يجد المحفز الذي يجعله يعمل وقد يكون المحفز هو تاريخ يوم معين في ساعة الحاسبة او كلمة معينة او إشارة أو أي شئ آخر يجعل الفيروس يعمل ويبدأ الفيروس بالتدمير.

4- القدرة على الاختراق:- يتميز فيروس الحاسب بإمكانيته إلى اختراق المواقع التي قد يقوم المستخدم بنفسه بتحميل هذه البرامج وإدخال الفيروس إلى النظام دون ان يشعر.

6- 6 أعراض الإصابة بالفيروس:-

هنالك مشاكل قد تحصل في الحاسب يعود بعضها إلى علة برمجية أو حالات سوء في أداء الأجزاء المادية لوظائفها ولكن وجود عارض أو أكثر تشبه عوارض الفيروسات الحاسوبية وان احتمال وجود الفيروس يزداد مما يوجب فحص النظام بأحد البرامج المضادة للفيروس. ومن الأعراض التي تصاحب وجود الفيروس ما يلي:-

1- تغير في عدد الملفات، إذ تقوم بعض أنواع الفيروس بحذف الملفات عشوائياً أو وفق تعليمات محددة، فإذا اختفى أحد الملفات من فهرس الملفات بدون سبب ظاهر عندها وجب الشك بوجود فيروس وكذلك في حالة وجود ملفات لا مبرر لوجودها.

2- توقف النظام عن العمل.

3- عرض رسالة خطأ فجائية غير مألوفة وخاصة عند ظهور رسائل تشير إلى

استخدام الأقراص والبرامج بشكل متكرر دون ان يتم استعمالها من قبل المستخدم فهذا يعني أن الفيروس يحاول الوصول إلى هذه الأقراص او البرامج لتلويثها.

4- بطأ تشغيل النظام، وتنفيذ البرامج يستغرق وقت اكثر من المعتاد، إذ يؤثر سلباً على وقت التنفيذ بعدة ثواني.

5- التعامل مع القرص اكثر من الطبيعي ويلاحظ ان مصابيح السواقات الخاصة بالقرص تضاء عدة مرات اكثر من المعدل الطبيعي وبدون سبب ظاهر.

6- ظهور حروف غريبة عند الضغط على مفاتيح معينة في لوحة المفاتيح (keyboard) أو عدم ظهور حروف على الإطلاق.

7- انخفاض ذاكرة النظام إذ تنخفض ذاكرة النظام نظراً لان الفيروس يحتل جزءاً من هذه الذاكرة فإذا ظهرت رسالة تدل على عدم وجود ذاكرة لتشغيل احد البرامج الكبيرة فهذا يدل على وجود فيروس.

8- الأيقونات يتغير مظهرها.

9- عمليات الوصول إلى الأقراص تستغرق وقتاً طويلاً لا تحتاجه مثل هذه المهام البسيطة مثلاً تخزين صفحة من نص قد يستغرق ثانيتين ولكن في حالة عدم وجود فيروس لا يستغرق عادة اكثر من ثانية واحدة.

10- تغيير في حجم البرامج التنفيذية فبعض الفيروسات تدخل إلى البرامج التنفيذية وتتناسخ فيها مما يؤدي إلى زيادة حجم البرامج.

6- 7 تصنيف البرمجيات الماكرة MALWARE:

تم إطلاق اسم فيروسات الحاسبات على عائلة متنوعة من البرامج الماكرة MALWARE وهي مشتقة من عبارة Malicious -logic software. ويمكننا تصنيف البرمجيات الماكرة إلى أربعة أنواع رئيسية هي الفيروسات Viruses والدود Worms وأحصنة طروادة Trojan horses وبرامج الإنزال Droppers.

الفيروس هو برنامج كمبيوتر مصمم عمداً ليقترن ببرنامج آخر، بحيث يعمل الفيروس عندما يعمل ذلك البرنامج ومن ثم يعيد إنتاج نفسه باقترانه ببرامج أخرى. ويقترن الفيروس بالبرنامج الأصلي بالصاق نفسه به أو باستبداله أحياناً. وقد يغير الفيروس نفسه عند إعادة الإنتاج، فيظهر كنسخة معدلة عن النسخة التي قبلها كلما كرر العملية.

تختلف الدودة عن الفيروس بنقطة مهمة جداً، فبينما يكرر الفيروس نفسه بواسطة تنفيذ برنامج مصاب، تستغل الدودة فجوات في نظام التشغيل للقيام بهجوم مباشر. وتعتبر الدودة المصممة من قبل روبرت موريس في عام 1988 من أشهر أنواع الدود، حيث قام هذا البرنامج بشل مئات الحاسبات والخدمات التعليمية والحكومية المرتبطة مع بعضها عبر الشبكة الدولية للمعلومات Internet وتصيب برامج الدود على الغالب الحاسبات المتوسطة Mini والكبيرة Mainframe ، ألا ان هذا لا يمنع من كونها قابلة للعمل على الحاسبات الشخصية وشبكاتهما.

والدودة برنامج لا يلوث برامج أخرى. إذ تنسخ الدودة نفسها من وإلى الأقراص المرنة، أو عبر الشبكات، ويعتمد بعضها على الشبكة في إنجاز عملها. تستخدم إحدى أنواع الديدان (وهي الدودة المضيفة host worm) الشبكة لنسخ نفسها فقط إلى أجهزة الحاسب المتصلة بالشبكة، بينما توزع الدودة الشبكية network worm أجزائها إلى عدة حاسبات وتعتمد على الشبكة فيما بعد لتشغيل هذه الأجزاء. ويمكن ان تظهر الديدان على حاسبات منفصلة فتسرخ نفسها إلى أماكن متعددة على القرص الصلب.

أما النوع الثالث من البرامج الماكرة فقد سمي باسم حصان طروادة، نسبة للأسطورة الإغريقية الواردة في ملحمة الأوديسا لهوميروس، حيث ترك الجيش الإغريقي حصاناً خشبياً ضخماً كهدية لسكان طروادة، وكان يختبئ داخله مجموعة من الجنود الأشداء بعد أن تظاهروا بإنهاء الحصار الطويل. وعندما رحل الجيش وأدخل السكان الحصان إلى داخل أسوار المدينة، خرج الجنود منه وانقضوا على الحامية، وسقطت المدينة في أيدي الإغريق. وكما امتاز حصان طروادة بمظهره الخارجي المسلم وغير المسلح بينما احتوى بداخله على أسلحة فتاكة، تعتمد برامج أحصنة طروادة على المبدأ ذاته، فهي تختبئ ضمن برامج يبدو مظهرها بريئاً، وعندما يشغل المستخدم واحداً من هذه البرامج ينشط الجزء الماكر ويقوم بعمل معين مصمم له. ومن أشهر برامج حصان طروادة هو ذلك البرنامج المزيف الذي يوجد في تعليمة LOGIN.EXE الخاصة ببرامج إدارة الشبكات من النوع Netware، حيث يقوم هذا البرنامج بالطلب من

المستثمر إدخال الاسم وكلمة السر ومن ثم يقوم بتخزينها في مكان سري في ذاكرة الحاسب، ثم يعلم المستثمر بأنه قد أخطأ في عملية إدخال كلمة السر، وبالتالي فعملية الدخول لم تتم (لاحظ ان كلمة السر- لا تظهر على الشاشة أثناء طباعتها وبالتالي لا يتمكن المستثمر من التأكد من انه قد ادخلها بشكل صحيح) ثم يقوم حصان طروادة او البرنامج المزيف بإخفاء نفسه واعادة تأهيل البرنامج LOGIN.EXE الأصلي ليستخدمه المستثمر في محاولته الثانية للدخول والتي ستتم بنجاح. وبالرغم من كون هذا البرنامج لا يقوم بأي عمل تخزيني إلا انه قابل للتعديل، وببساطة لتكرار نفسه لأكثر من مرة أو للاستفادة من كلمات السر التي تم جمعها مما يجعله شديد الخطورة.

أما برامج الإنزال (droppers) فقد صممت لمراوغة برامج مكافحة الفيروسات، وتعتمد على التشفير غالباً لمنع اكتشافها. ووظيفة هذه البرامج عادة نقل وتركيب الفيروسات، فهي تنتظر لحظة حدوث أمر معين على الحاسب لكي تنطلق وتلوته بالفيروس المحمول في طياتها. وينتمي مفهوم قنبلة (bomb) الحاسب إلى هذه الفئة، إذ تبنى القنابل ضمن البرمجيات الماكرة كواسطة لتنشيطها. وتبرمج القنابل لتنشط عند حدوث حدث معين. تنشط بعض القنابل في وقت محدد اعتماداً على ساعة الحاسب. فيمكن برمجة قنبلة مثلاً لمسح كافة الملفات ذات الامتداد DOC من القرص الصلب في ليلة راس السنة الميلادية، أو لعرض رسالة على الشاشة في اليوم المصادف لعيد ميلاد شخصية مشهورة. وتعمل بعض القنابل تحت شروط أو أحداث أخرى، فيمكن ان تنتظر القنبلة إلى

ان يتم تشغيل برنامج معين عشرين مرة مثلاً وعندها تمسح الملفات الخاصة بهذا البرنامج. ومن وجهة النظر هذه تعتبر القنابل مجرد برامج جدولة زمنية مأكرة.

6- 8 أخطار الفيروس:-

الفيروسات لا تظهر صدفة، بل يكتبها مبرمجون ذوو مهارات عالية عادة، ثم يجدون طريقة لنشرها في أجهزة المستخدمين الغافلين عنها. وكلما أصبحت برامج مكافحة الفيروسات أقوى، زاد المبرمجون من جهودهم لتطوير فيروسات أذكى للتحايل عليها. والهدف من تطوير الفيروسات بالنسبة للكثير من مؤلفيها ليس أكثر من تحدي والرغبة في إثبات تفوقهم، بينما هو للبعض الآخر التلذذ بإثارة حيرة الآخرين وشكوكهم في الحاسب، أو إزعاجهم، وحتى إيذائهم! وهذا أمر سيئ جداً، إذ يمكنهم أن ينجسوا أموالاً طائلة إذا وجهوا مواهبهم لمساعدة الشركات على حل مشاكلها بدلاً من هدرها في أعمال لا طائل منها، مثل تطوير الفيروسات.

ان الفيروس يسبب أخطاراً شديدة وان هذه الأخطار تشمل:-

1- أخطار الفيروس على البرامج software.

2- أخطار الفيروس على المكونات hardware.

1- أخطار الفيروس على البرامج software:- ان البرامج هي

وسيلة الانتقال الرئيسة للفيروس. وان اكبر خطر للفيروس يتمثل في توقف

البرامج أو تعديل وظائفها نتيجة نسخ أوامر الفيروس مكان جزء من أوامر

البرامج ويظهر هجوم الفيروس على البرامج التي تعمل على نظام التشغيل DOS. ويعمل الفيروس على الآتي:-

أ- إبطاء تشغيل الحاسبة:-

قد يؤدي الفيروس في بعض الأحيان إلى إبطاء تشغيل الحاسبة وتستغرق العمليات التي يؤديها مدة أطول من المفروض أن يستغرقها. وقد يكون هذا التأخير غير ملحوظ عند تنفيذ عمليات منفصلة ويتم ملاحظته عندما يؤدي الحاسب مجموعة من العمليات كالبحث عن بيانات معينة أو طباعة تقارير الخ...

ب - تدمير قطاع التحميل Boot sector:-

يقوم الفيروس بتدمير قطاع التحميل الذي يكون في مكان محدد وثابت في القرص. ويقصد بقطاع التحميل هو ذلك الجزء من القرص الذي يحتوي على الأوامر والإشارات التي يستخدمها الحاسب لكي يبدأ في العمل. ان تحطيم هذا القطاع او تغيير الأوامر المخزونة فيه يجعل القرص غير قادر على تشغيل النظام (unbootable) وعندما نتعامل مع القرص المرن تكون هذه الحالة محتملة. ان في حالة التعامل مع القرص الصلب تصبح هنالك مشكلة كبيرة ويكون العلاج لها والوحيد هو إعادة تجهيز القرص Reformat مما يؤدي الى فقدان جميع البرامج والبيانات المخزونة ولهذا من الضروري الاحتفاظ بنسخ احتياطية من البرامج والبيانات.

ج - تدمير جدول توزيع الملفات File Allocation Table :-

ان جدول توزيع الملفات (File Allocation table) هو منطقة على القرص يستخدمها نظام التشغيل لتتبع أماكن الملفات المخزنة على القرص والقطاعات الخالية التي يمكن تخزين الملفات الجديدة عليها. وهذا الجدول يكون دائماً في مكان ثابت على القرص، لذلك يسهل على الفيروس مهاجمته. وفي هذه الحالة يمكنه مسح هذا الجدول وبالتالي يصعب الوصول إلى أي ملف على القرص. كما يمكنه تغيير المعلومات الموجودة في هذا الجدول مثلاً تغيير المعلومات الخاصة بالمساحة التخزينية المتاحة على القرص بإنقاصها عن المساحة الفعلية المتاحة وبالتالي لا يستطيع المستخدم التعامل إلا مع جزء صغير من المساحة التخزينية للقرص. وكمثال على ذلك فيروس STONED الأكثر انتشاراً في الحاسبات الشخصية، والذي يقدر كونه سبباً لـ 50% من الإصابات في الولايات المتحدة، انتقل هذا الفيروس إلى الولايات المتحدة من نيوزلندا، وقد صمم ليطلع عبارة تشجع ترويج الماريجوانا، ويقوم بتكرار نفسه طوال فترة ستة أعوام. ما زال هذا الفيروس موجوداً ويتابع انتشاره، حيث يصيب جدول مواقع الملفات FAT file Allocation Table أثناء تكراره نفسه مما يجعل القرص الصلب غير قابلاً للقراءة، وبالتالي تضيع كافة المعلومات الموجودة على القرص الصلب على الرغم من ان مصمم هذا الفيروس لم ينوي ان يسبب هذا الأذى لاحد، ولكن بعد الإصابة يصبح هذا الحاسب كأي حاسب قد تعرض لتخريب متعمد.

د - تحطيم الفهرس الرئيسي Root Directory :-

يقوم نظام التشغيل DOS بتنظيم الملفات المخزونة على القرص عن

طريق الفهارس Directories والفهارس الفرعية Subdirectories. هذه الطريقة في تنظيم الملفات تجعل الوصول إلى أي ملف على القرص سهلاً. حيث يصبح من السهل الوصول إلى الفهرس الفرعي المطلوب وعرض الملفات الموجودة به دون الحاجة إلى عرض جميع الملفات المخزونة على القرص. وتظهر أهمية ذلك بوضوح عندما يزيد عدد الملفات زيادة كبيرة. لذلك فإن الفهرس الرئيسي Root Directory يمثل هدفاً استراتيجياً للفيروس حيث يمكن أن يؤدي تغيير حرف واحد (byte) في هذا الفهرس إلى عدم التمكن من الوصول إلى أي ملف على القرص رغم وجود الملفات فعلياً.

هـ - التجسس على النظم:-

في نظم شبكات الحاسب التي تستخدم أجهزة الاتصال (Modems) في الربط بين أجهزة الحاسب في الأماكن المختلفة، فإن الفيروس عند انتقاله إلى هذا النظام يقوم بالسماح للمخرب الذي قام بتصميمه بالدخول إلى النظام والحصول على أي بيانات سرية وذلك بهدف تحقيق مكاسب شخصية له سواء كانت مادية أو معنوية. حيث يقوم الفيروس في وقت محدد بالاتصال بالمخرب تلفونياً والسماح له بالدخول إلى النظام.

2- أخطار الفيروس على المكونات Hardware:-

أن الفيروس يسبب أخطار شديدة لمكونات الحاسب Hardware. وقد تصل الخطورة إلى إجهاد الأجزاء الميكانيكية للحاسب بما قد يسبب تدميرها. فمثلاً برنامج يعطي أمراً لجهاز التحكم في وحدة الأقراص Disk drive لتوجيه

راس القراءة والكتابة read / write head الى مكان بعيد في اتجاه مركز القرص وهذا يؤدي في بعض الحالات إلى تثبيت راس القراءة والكتابة وعدم قدرته على الحركة وقراءة المسارات Tracks الموجودة على القرص. ولكي يتم أعادته إلى الوضع الطبيعي يتطلب الأمر إصلاح العطل ميكانيكياً.

إضافة إلى ذلك هنالك برامج يمكنها التحكم في الطابعة بحيث يتم تغيير اتجاه الطابعة. وهذا يؤدي إلى تجمع الورق داخل الطابعة وربما إلى تعطلها. كما ان هناك برنامج فيروس يسمح مسار التحكم Control Track الخاص بالقرص الصلب وهذا يجعل القرص غير صالح.

وهنالك برامج أخرى لا تسبب عطلاً مادياً بصورة مباشرة ولكنها تؤدي إلى تآكل أجزاء معينة في مكونات الحاسبة مما يقلل من عمرها الافتراضي. حيث ان بعض الفيروسات الساكنة في الذاكرة يمكنها ان تقلل من حجم الذاكرة الموقته المتاح بدرجة كبيرة. ويؤدي هذا إلى تعامل الذاكرة مع القرص عدداً كبيراً من المرات حتى يستطيع تحميل البرامج المطلوبة وهذا يؤدي إلى استهلاك وحدة الأقراص بعد فترة وجيزة.

6- 9 أكثر الفيروسات انتشاراً:-

أن سعي وسائل الإعلام وراء السبق الصحفي يجعلها تبالغ أحياناً في وصف خطورة بعض الفيروسات التي تنتشر من حين إلى آخر وتعظيمهم لمبرمجي هذه الفيروسات شجع الكثيرين منهم على إنتاج المزيد من الفيروسات الجديدة جرياً وراء الشهرة الإعلامية. فمبرمج الفيروسات، كما هو معروف، إنسان يتمتع

بذكاء شديد ويعاني في الوقت ذاته من مرض نفسي، ويهدف من وراء إنشاء الفيروسات ونشرها أما إلى الشهرة أو رؤية العالم يعاني من الخسائر بسببه. ومن أكثر الفيروسات انتشاراً منها:-

1- الفيروس Worm Explorer Zip :-

ظهرت أول حالة إصابة بهذه الدودة في إسرائيل في السابع من شهر حزيران 1999 ثم انتشرت بشكل واسع خلال أسبوع واحد في كل من ألمانيا، وفرنسا والنرويج وجمهورية التشيك والولايات المتحدة. ويصنف الخبراء الدودة Worm Explore Zip بأنها أخطر من فيروس ميلسيا وفيروس تشيرنوبل.

2- الفيروس (ATAKA (A.K.A. IE0199.exe) :-

هذا الفيروس هو من نوع حصان طروادة، أرسل كملف مرفق بالبريد الإلكتروني إلى الكثير من المستخدمين بعد تزوير عنوان البريد الإلكتروني للمرسل ليبدو صادراً من شركة مايكروسوفت.

3- الفيروس (A.K.A Happy99.exe) W32/Ska :-

فيروس من نوع دودة، أرسل أول مرة إلى عدد من مجموعات الأخبار. يوجد ضمن ملف باسم Happy99.exe، ويظهر عند تشغيله رسالة على الشاشة تهنيئ بحلول السنة الميلادية 1999 Happy New Year مع رسوم الألعاب نارية. كان سبب تكاثره الرئيسي تبادله ضمن مجموعات الأخبار، لكنه يمكن ان ينشر- ذاته أيضاً بالتصاقه برسائل البريد الإلكتروني وإرساله كملف مرفق بدون علم

المستخدم. بمجرد تشغيل الملف Happy99.exe تظهر رسوم ألعاب نارية على شاشة المستخدم.

4- الفيروس Laroux:-

فيروس ماكرو (فيروس ماكرو هو عبارة عن برنامج مصمم للعمل مع تطبيق معين أو عدة تطبيقات تشترك بلغة برمجة واحدة) لبرنامج اكسل Excel. ظهر هذا الفيروس في عام 1996. يصبح فعالاً حالما يحمل برنامج اكسل المصاب به، ويتنقل العدوى إلى أي مصنف اكسل يفتحه المستخدم.

5- الفيروس W32.CIH:-

ظهرت عائلة هذا الفيروس في عام 1998 من جنوب شرق آسيا. وتوجد منه حالياً ثلاثة نماذج معروفة وهو منتشر على نطاق واسع، ويصيب ملفات ويندوز 95. يتضمن الفيروس شحنة خطيرة جداً تعمل في اليوم السادس والعشرين من كل شهر.

لقد بينا أن هنالك العديد من الفيروسات التي تؤثر على الحاسبات التي نستخدمها. ونظراً لخطورتها يجب استمرار استخدام إجراءات الوقاية منها إضافة إلى استخدام واحداً من برامج اكتشاف وإزالة الفيروسات الشهيرة المتوفرة كبرامج McAfee أو Norton AntiVirus أو Dr. Salamon وغيرها من البرامج لتبقى الحاسبات بدون تلويث من قبل الفيروسات. أو استخدام أحدث إصدارات لمعالجة الفيروسات حيث ان برامج

الفيروسات الجديدة تظهر بشكل مستمر ومعها تظهر معالجات للفيروسات، وعليه ينبغي متابعة التطورات الحاصلة في هذا المجال.

6- 10 وصايا لتجنب الاصابة بالفيروس:-

1- يجب التأكد والحرص عند استخدام الأقراص المرنة خصوصاً إذا لم تكن معروفة المصدر (نسخة غير أصلية) حيث ان % 80 من الفيروسات تنتقل بهذه الطريقة

2- يجب التأكد من رفع الأقراص من مشغل الأقراص (DRIVER) عند تحميل النظام لانه إذا كان هذا القرص يحتوي على فيروس من النوع الذي يصيب منطقة التحميل (BOOT SECTOR) فانه سوف يصيب الحاسبة حتى وان لم يكن هذا القرص قرص نظام (SYSTEM DISK).

3- يجب التأكد من البرامج التي تدخل الحاسبة من قبل الأصدقاء والمعارف وذلك بفحصها قبل إدخالها الحاسبة فلفيروس يتتشر- عادة عندما نقوم بتشغيل الحاسبة من قرص مصاب او عندما نقوم بتنفيذ برنامج مصاب.

أسئلة الفصل السادس

- 1- ما هو الفيروس، ولماذا سمي بهذا الاسم.
- 2- ما هي أهم صفات الفيروس.
- 3- عدد أهم أعراض الإصابة بالفيروس.
- 4- ما هي أخطار الفيروس على البرامج.
- 5- ما هي أخطار الفيروس على المكونات.
- 6- عدد أهم الوصايا اللازم اتخاذها لتجنب الإصابة بالفيروس.

EBSCOhost®

EBSCOhost®

الفصل السابع الأمن التقني

7- 1 المقدمة:-

من المعروف ان مركز الحاسبة يتضمن العديد من الأجهزة والمعدات التي تكون بحاجة إلى صيانة دورية وكذلك عند حصول الأعطال. هذه الصيانة تجرى من قبل مهندسي الصيانة الذين يقومون بزيارات دورية ومتكررة.

أن هذه الأجهزة والمعدات تتضمن معلومات مكثفة تجعلها عرضة للاستغلال ومثيرة لشهية الطامعين للحصول عليها واستغلالها بصورة غير قانونية مما يؤثر على أمانة مركز الحاسبة.

سيتم من خلال فقرات هذا الفصل توضيح ما يتعلق بأمن الأجهزة والمعدات.

7- 2 من أجهزة الحاسبة الإلكترونية:-

قبل التطرق إلى أمن أجهزة الحاسبة الإلكترونية، لابد من الإشارة والتعرف على الأمور التالية:-

1- الحاسبات الرئيسية Main Frame:-

الحاسبات الرئيسية هي اكبر أسرع الحاسبات المستعملة في يومنا هذا، وهناك عدد من الخصائص التي يتميز بها الحاسب الرئيسي فهو: