أمن المعلومات
Information security

الفصل الخامس

أمن المعلومات
Information Security

- **من منطلقٍ أكاديمي** : العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.
- **ومن جهةٍ تقنية**، مجموعة الوسائل والأدوات والإجراءات اللازم توفيرها؛ لضمان حماية المعلومات من الأخطار الداخلية والخارجية.
- **من الناحية القانونية**: هو محلُّ دراساتٍ وتدابيَر حماية سرية وسلامة محتوى وتوافر المعلومات، ومكافحة أنشطة الاعتداء عليها، أو استغلال نظمها في ارتكاب الجريمة، وهو هدف تشريعات حماية المعلومات من الأنشطة غير المشروعة، وغير القانونية، التي تستهدف المعلومات ونظمها، كجرائم الكمبيوتر والإنترنت.

أمن المعلومات
Information Security

إن مفهوم أمن المعلومات ينطوي على الآتي:

- إجراءات إدارية وفنية.
- المحافظة على المكونات المادية للحاسب الآلي.
- المحافظة على المكونات غير المادية للحاسب الآلي.
- ضوابط لإضفاء الشرعية على حدود وصلاحية استخدام المعلومات والأجهزة.
- الحماية ضدَّ السرقة، أو التوقُّف، أو التلف المُتعمَّد أو غير المُتعمَّد، أو التخريب، أو التبديل، أو الاختراق، أو مجرد الاطلاع عليها من دون تصريح بالاستخدام.

أهمية أمن المعلومات

- **الحاجة للارتباط بنظم الاتصالات والإنترنت**، وعدم إمكانية عزل الأجهزة عن الشبكات المحلية والشبكات واسعة النطاق.

- **اعتماد مختلف المنظمات على المعلومات** (المعلومات مصدر ثروة المنظمات)

- **صعوبة تحديد الأخطار والتحكم بها، أو متابعة المجرمين ومعاقبتهم** لعدم توافر حدود جغرافية عند استخدام الإنترنت والاتصالات الإلكترونية.

- **النمو المتزايد في التطبيقات الإلكترونية** وظهور التجارة الإلكترونية والإدارة الإلكترونية التي تحتاج إلى بيئة معلوماتية آمنة .
- **كثرة التهديدات المعلوماتية وتنوعها، وتعدد مصادرها**، كالجرائم الإلكترونية، واختراق الشبكات، والفيروسات بأنواعها.

عناصر أمن المعلومات

إن المحافظة على المعلومات يتطلب توافر عناصر أساسية هي:

١) **السرية أو الموثوقية :** ضمان حفظ المعلومات المخزنة أو المنقولة عبر الشبكة وعدم الاطلاع عليها أو استخدامها من قبل أشخاص غير مخولين بذلك.

٢) **التكاملية وسلامة المحتوى :** التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به في أي مرحلة من مراحل المعالجة أو الإرسال والاستقبال.

٣) **استمرارية توافر المعلومات أو الخدمة :** أن تكون المعلومات متوفرة عند الحاجة إليه

٤) **عدم إنكار التصرف المرتبط بالمعلومات ممن قام به Non-repudiation:** ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها أنَّه هو الذي قام بهذا التصرف ، بحيث يمكن إثبات أن تصرفاً ما قد تمَّ من شخص ما في وقت محدد .

مواطن الخطر والاعتداءات

- **الأجهـزة** :وهي كافة المعدات والتجهيزات المادية التي تتكون منها نظم المعلومات، كالحواسيب، والشاشات، والطابعات، ووسائط التخزين المادية وغيرها
- **البرامــج** : وهي الأوامر المرتَّبة في نسق معين لإنجاز الأعمال
- **المعطيـات** : وتشمل كافة البيانات المدخلة والمعلومات المستخرجة، وتمتدُّ بمعناها الواسع للبرمجيات المخزنة داخل النظم.
- **الاتصـالات:** وتشمل شبكات الاتصال التي تربط أجهزة التقنية ببعضها البعض محلياً وإقليمياً ودولياً
- **العنصر البشري:** هو محور الخطر، إن كان ذلك المستخدم أو الشخص الموكلة إليه مهام تقنية معينة تتصل بالنظام، فإدراك هذا الشخص لحدود صلاحياته، وآليات التعامل مع الخطر، وسلامة الرقابة على أنشطته وفق حدود حقوقه القانونية، مسائل رئيسة يُعنى بها نظام الأمن الشامل

مصطلحات خاصة بعالم الجرائم الإلكترونية

- **التهديد** :ويعني الخطر المُحتمل الذي يُمكن أن يتعرَّض له نظام المعلومات، وقد يكون مصدره شخصاً: كالمتجسس، أو المجرم المحترف، أو المخترق ((Hackers، أو شيئاً يهدّد الأجهزة، أو البرامج، أو المعطيات، وقد يكون حدثاً: كالحريق، وانقطاع التيار الكهربائي، والكوارث الطبيعية .

- **الهجمات** :مصطلح لوصف الاعتداءات بنتائجها، أو بموضع الاستهداف، فنقول: هجمات إنكار الخدمة ، أو هجمات إرهابية ، أو هجمات البرمجيات ، أو هجمات الموظفين الحاقدة، أو الهجمات المزاحية.

- **الجرائم الإلكترونية** Cyber crimeوهو الدالُّ على مختلف جرائم الحاسوب والإنترنت في الوقت الحاضر، بالرغم من أنَّ استخدامه بدايةً كان محصوراً بجرائم شبكة الإنترنت وحدها

- **إرهاب العالم الإلكتروني Cyber Terrorism**، وهو هجمات تستهدف نظم الحاسوب والمعطيات لأغراض دينية، أو سياسية، أو فكرية، أو عرقية، وفي حقيقتها جزء من الجرائم الإلكترونية **Cyber crime**

- **حرب المعلومات** Information warfare، وقد ظهر في بيئة الإنترنت؛ للتعبير عن اعتداءات تعطيل المواقع، وإنكار الخدمة، والاستيلاء على المعطيات،

المخاطر والتهديدات المحتملة

مخاطر خرق الحماية المادية:

- التفتيش في مخلَّفات التقنية Dumpster diving ويُقصد به قيام المهاجم بالبحث في مخلفات المنظمة من المهملات، والمواد المتروكة، بحثاً عن أيّ شيءٍ يساعده على اختراق النظام.

- التنصت على المكالمات الهاتفية : Wiretapping والمقصود هنا ببساطة الاتصال السلكي المادي مع الشبكة، أو توصيلات النظام لجهة استراق السمع، أو السرقة والاستيلاء على المعطيات المتبادلة عبر الأسلاك.

- إنكار أو إلغاء الخدمة : Denial or Degradation of Service والمقصود هنا إلحاق الضرر المادي بالنظام لمنع تقديم الخدمة.

مخاطر خرق الحماية المتعلقة بالأفراد

- **انتحال صلاحيَّات شخص مفوّض** :والمقصود هنا الدخول إلى النظام بواسطة استخدام وسائل التعريف العائدة لمستخدم مخوّل بهذا الاستخدام، كاستغلال كلمة سر أواسم أحد المستخدمين.

- **الهندسة الاجتماعية** :تعني أن أنشطة الحصول على معلومات تهيئ الاختراق، وذلك من خلال علاقات اجتماعية، وذلك باستغلال الشخص لأحد مستخدمي النظام بإيهامه بأيّ أمر يؤدي إلى حصول هذا الشخص على كلمة مرور، أو على أية معلومة تساعد في تحقيق إعتدائه.

- **قرصنة البرمجيات** :تتحقق عن طريق نسخها من دون تصريح، أو استغلالها على نحوٍ ماديٍّ من دون تخويلٍ بهذا الاستغلال، أو تقليدها ومحاكاتها والإنتفاع المادي بها على نحوٍ يخلُّ بحقوق المؤلف

مخاطر خرق الحماية المُتصلة بالاتصالات والمعطيات

- **النسخ غير المُصرَّح به للمعطيات** :يمكن الاستيلاء على كافة أنواع المعطيات من بيانات ومعلومات وأوامر وبرمجيات، وغيرها... عن طريق النسخ.

- **تحليل الاتصالات** :تقوم الفكرة هنا على مراقبة أداء النظام، ومتابعة ما يتمُّ فيه من اتصالات.

- **المصائد أوالابواب الخلفيَّة** :عبارة عن ثغرة برمجية يمكن للمخترق الوصول من خلالها إلى النظام، فهي ببساطة مدخل مفتوح تماماً كالباب الخلفي للمنزل الذي يتسلَّل منه السارق.

- **البرمجيات الخبيثة** :كالفيروسات Viruses، وحصان طروادة Trojan Horses، والدودة الإلكترونية Warms، والقنابل المنطقية Logic Bombs، والشيء المشترك بين هذه البرمجيات أنَّها برمجياتٌ ضارَّةٌ تُستغلُّ للتدمير وذلك لتدمير النظام، أو البرمجيات، أو المعطيات، أو الملفات، أو الوظائف

ما هي التهديدات المحتملة لأمن المعلومات؟

أولاً- الاختراق: عملية اقتحام الأنظمة أو الشبكات الخاصة بأفراد أو منظمات خاصة أو حكومية بمساعدة بعض البرامج المتخصصة في فك وسرقة **كلمات المرور** بهدف الاطلاع على المعلومات، أو تخريبها، أو سرقتها .

كلمة المرور (Password)

هي مجموعة من الرموز التي تسمح للدخول إلى الحاسوب، أو الموارد على شبكة الاتصال أو المعلومات.

فوائد كلمة المرور:

- تسمح للمستخدمين المصرح لهم فقط لدخول النظام.
- إدارة وتحديد هوية الأشخاص بفاعلية والتدقيق في عملية الوصول.
- حفظ وحماية المعلومات.
- حماية المعلومات الشخصية الخاصة بك

إجراءات الوقاية من عمليات الاختراق

١) تطبيق إجراءات أمنية مشددة.

٢) الاستعانة بالمكاتب الاستشارية المتخصصة في أمن المعلومات.

٣) توعية العاملين في المنشأة بخطورة الاختراقات.

٤) استخدام كلمة مرور مكونة من عدة حروف وأرقام خاصة يصعب التنبؤ بها.

٥) الاحتفاظ بنسخة أصلية ومحدثة من برامج مكافحة الفيروسات.

٦) تجنب تحميل برامج غير معروفة المصدر، أو غير موثوقة.

ما هي خواص الفيروسات؟

١) **التضاعف**: زيادة عدد العمليات إلى ملايين العمليات مما يسبب البطء أو توقف الحاسب عن العمل.

٢) **التخفي**: حتى لا ينكشف ويصبح غير فعال.

٣) **إلحاق الأذى**: يتراوح الأذى بمسح جميع المعلومات المخزنة، إلغاء بعض ملفات النظام..الخ

أضرار الإصابة بالفيروسات و البرامج الخبيثة:

١. تعطيل الحاسوب.

٢. ظهور شاشة الموت الزرقاء.

٣. سرقة النقود إلكترونياً.

٤. بعض الأمور المزعجة للمستخدم مثل تغير سطح المكتب و حذف الملفات.

٥. سرقة البيانات.

٦. إتلاف البرمجيات و التسبب في الحرمان من استخدام بعض الخدمات.

٧. بطئ عمل الحاسب وبطئ الاتصال بالإنترنت.

أعراض الإصابة بالفيروسات و البرامج الخبيثة:

- تباطؤ أداء الحاسوب.
- زيادة حجم الملفات، أو زيادة زمن تحميلها للذاكرة .
- ظهور رسائل تخريبية على الشاشة، أو الرسوم أو صدور بعض الأصوات الموسيقية.
- حدوث خلل في لوحة المفاتيح كأن تظهر على الشاشة أحرف ورموز غير التي تم ضغطها أو حدوث قفل للوحة المفاتيح .
- ظهور رسالة ذاكرة غير كافية لتحميل برنامج كان يعمل سابقاً بشكل عادي.
- سعة الأقراص أقل من سعتها الحقيقية.

طرق مواجهة مهددات أمن المعلومات

١- اختيار موقع مناسب للأجهزة.

٢- توفير مصدر احتياطي للطاقة الكهربائية.

٣- استخدام وسائل التحقق الشخصية.

- تحديد شخصية المستخدم : (الرقم السري، البطاقات ممغنطة، الصفات البيولوجية).
- تحديد صلاحية المستخدم وحدود تداول المعلومات: (جهاز الكشف عن بصمة الإصبع، جهاز الكشف عن اليد، جهاز الكشف عن ملامح الوجه، جهاز التعرف على الصوت).

طرق مواجهة مهددات أمن المعلومات

٤- **جدران الحماية** هو حاجز بين الحاسب الآلي والعالم الخارجي، يقوم بتصفية البيانات القادمة من الخارج بناءً على مقاييس معينة مثل حجم البيانات والعنوان **IP Address** والبروتوكول الذي تم استعماله والمنفذ الذي تستخدمه البيانات للدخول إلى الحاسب الآلي.

- يقوم الجدار الناري Firewall بغلق المنافذ التي لا يحتاج إليها المستخدم أو التطبيق لاستخدامها على الإنترنت وبذلك يمنع الفيروسات والاختراقات من تلك المنافذ.

- **أشهر برامج جدران الحماية:**

١. Zone Alarm Security Suite
٢. Outpost Firewall
٣. Windows Firewall
٤. Kaspersky Internet Security
٥. Norton 360, Norton IS.

طرق مواجهة مهددات أمن المعلومات

٥- النسخ الاحتياطي (Backup)

- قد نتعرض لفقدان بعض البيانات أو الملفات المهمة أو الضرورية عن طريق:
  - حذفها من غير قصد.
  - تعرضها للعطب.
- لذلك نحتاج لعمل نسخة احتياطية من ملفات النظام، ثم في حالة فقدان أو تلف الملفات يكون باستطاعتنا استعادة الملف المحذوف من النسخة الاحتياطية.

طرق مواجهة مهددات أمن المعلومات

٥- برامج الحماية من الفيروسات :

- استخدام البرمجيات المضادة للفيروسات على كافة أجهزة الكمبيوتر المتصلة بالإنترنت وتحديث هذه البرمجيات.
- العديد من برامج مكافحة الفيروسات تدعم التحديثات التلقائية لتعريفات الفيروسات. ومن المستحسن استخدام هذه التحديثات التلقائية عندما تكون متاحة.

تقوم برامج مكافحة الفيروسات بعملها من خلال:

- **تقنية البحث عن الفيروسات.**
- **تقنية تفحص السلوك ومحاولة الكشف عن الفيروسات غير المعروفة.**
- **تقنية اختبار التكامل مراقبة جميع الملفات الموجودة على الجهاز لرصد أي تغيير يحدث.**

طرق مواجهة مهددات أمن المعلومات

٦- التشفير :

- العلم الذي يستخدم الرياضيات للتشفير وفك تشفير البيانات.
- عملية تحويل المعلومات إلى شفرات غير مفهومة وغير ذات معنى، لمنع الأشخاص غير المرخص لهم من فهمها.
- يمكن من تخزين المعلومات الحساسة أو نقلها عبر الشبكات غير الآمنة- مثل الإنترنت- وعليه لا يمكن قراءتها من قبل أي شخص ما عدا الشخص المرسل لـه.

- **ما هي أهداف التشفير؟**
- **السرية أو الخصوصية.**
- **تكامل البيانات: حفظ المعلومات من التغيير (حذف أو إضافة أو تعديل) من قبل الأشخاص الغير مصرح لهم بذلك.**
- **إثبات الهوية: إثبات هوية التعامل مع البيانات (المصرح لهم).**

طرق مواجهة مهددات أمن المعلومات

٧- وجود قسم أو إدارة لأمن المعلومات :

ما هي مهام قسم أمن المعلومات؟

١) مراقبة النظام والتأكد من سلامته من النواحي الأمنية، لاكتشاف محاولات الدخول غير المشروع

٢) متابعة السياسات الأمنية وتحديثها

٣) التأكد من مصادر البرامج

٤) وضع خطة طوارئ ومتابعتها واختبارها وتطويرها

٥) تثقيف الموظفين بأهمية أمن المعلومات وبالأخطار المحتملة.