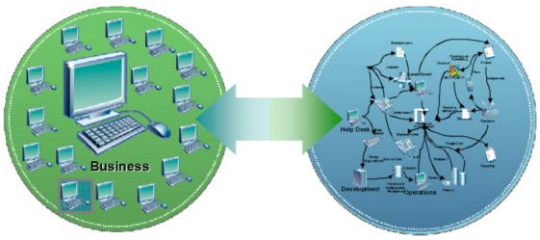
كلية إدارة الأعمال
FACULTY OF BUSINESS ADMINISTRATION

مقرر
تظم المعلومات الإدارية
Management Information Systems
MIS

أ. د. طاهر ياسر جلسي

الفصل الثالث عشر

أمن المعلومات والتحكم



أمـــن المعلومات وعناصره

- استخدام اصطلاح **أمن المعلومات Information Security** وإن كان استخداما قديما وسابقا لولادة وسائل تكنولوجيا المعلومات، إلا أنه وجد استخدامه الشائع بل والفعلي، في نطاق أنشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال، إذ مع شيوع الوسائل التقنية لمعالجة وخزن البيانات وتداولها والتفاعل معها عبر شبكات المعلومات – وتحديدا الإنترنت– احتلت أبحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة، بل ربما أمست أحد الهواجس التي تؤرق مختلف الجهات.
- **ولكن: ما الذي نحميه – بوجه عام – بالنسبة للمعلومات؟؟**

3

أمن المعلومات(Information Security)

- **أمن المعلومات:**
  - **من زاوية أكاديمية،** هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.
  - **ومن زاوية تقنية،** هي الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. وهو العلم الذي يدرس كيفية توفير تدابير حماية سرية وسلامة المعلومات وكيفية مكافحة أنشطة الاعتداء عليها واستغلال نظمها.
  - **ومن زاوية قانونية،** فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت).

4

عناصر أمن المعلومات

- إن أغراض أبحاث واستراتيجيات ووسائل أمن المعلومات – سواء من الناحية التقنية أو الأدائية - وكذا هدف التدابير التشريعية في هذا الحقل، هو ضمان توفر العناصر التالية لأية معلومات يراد توفير الحماية الكافية لها:

1. **السرية أو الموثوقية CONFIDENTIALITY:** وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.
2. **التكاملية وسلامة المحتوى INTEGRITY:** التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغيره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.
3. **استمرارية توفر المعلومات أو الخدمة AVAILABILITY:** التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.
4. **عدم إنكار التصرف المرتبط بالمعلومات ممن قام به Non-repudiation:** ويقصد به ضمان عدم انكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها انكار أنه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من شخص ما في وقت معين.

5

عمليات المعلومات الرئيسة المتصلة بأمن المعلومات

- تتعدد **عمليات التعامل مع المعلومات** في بيئة النظم وتقنيات المعالجة والاتصال وتبادل البيانات، ولكن يمكن بوجه عام تحديد العمليات الرئيسة التالية:

2-1 تصنيف المعلومات Information classification:

- وهي عملية أساسية لدى بناء أي نظام أو في بيئة أي نشاط يتعلق بالمعلومات وتختلف التصنيفات حسب المنشأة مدار البحث، فمثلا قد تصنف المعلومات إلى معلومات متاحة، وموثوقة، وسرية، وسرية للغاية أو قد تكون معلومات متاح الوصول اليها وأخرى محظور التوصل إليها وهكذا.

2-2 التوثيق Documentation:

- وتتطلب عمليات المعلومات أساسا اتباع نظام توثيق خطي لتوثيق بناء النظام وكافة وسائل المعالجة والتبادل ومكوناتها. وبشكل رئيس فإن التوثيق لازم وضروري لنظام التعريف والتخويل، وتصنيف المعلومات، والأنظمة التطبيقية. وفي إطار الأمن، فإن التوثيق يتطلب أن تكون استراتيجية أو سياسة الأمن موثقة ومكتوبة وأن تكون إجراءاتها ومكوناتها كاملة محل توثيق، إضافة إلى خطط التعامل مع المخاطر والحوادث، والجهات المسؤولة ومسؤولياتها وخطط التعافي وإدارة الازمات وخطط الطوارئ المرتبطة بالنظام عند حدوث الخطر.

6

إدارة أمن ورقابة المعلومات وخطواتها

- **يستخدم مصطلح أمن المعلومات Information security بالمفهوم الواسع للدلالة على حماية كل من التجهيزات المادية Hardware للحاسوب وغير المادية (البرمجيات) Software والتسهيلات والبيانات والمعلومات من سوء استخدام أطراف غير مصرح لهم بذلك**، ويهدف أمن المعلومات إلى تحقيق ثلاثة أهداف رئيسية:
  - **تأمين الخصوصية Confidentiality**.
  - **إتاحة المعلومات Availability**.
  - **الكمال Integrity**.
- **وتتضمن إدارة أمن المعلومات Information Security Management (ISM) أربع خطوات رئيسية وهي:**
  1. **تحديد التهديدات** Threats التي يمكن أن تهاجم موارد معلومات المنظمة.
  2. **تحديد المخاطر** Risks التي يمكن أن تنجم عن تلك التهديدات.
  3. **إعداد سياسة أمن المعلومات** Information Security Policy (ISP).
  4. **تطبيق إجراءات رقابة** Controls لمنع حدوث المخاطر أو الحد منها.
- **وفيما يلي توضيح لتلك الخطوات:**

7

إدارة أمن ورقابة المعلومات وخطواتها

1-تحديد التهديدات:

- يمكن أن يتمثل التهديد في شخص أو منظمة أو برنامج أو حدث من المتوقع أن يكون لهم ضرر محتمل لموارد معلومات المنظمة، ويمكن أن تكون تلك الأخطار من داخل أو من خارج المنظمة، كما يمكن أن تكون مقصودة أو غير مقصودة، وتشير استطلاعات الرأي المنفذة من قبل جمعية أمن الكمبيوتر إلى أنَّ 49% من حوادث أمن المعلومات أتت من مستخدمين شرعيين، كما أنَّ التهديدات الداخلية أكثر خطراً وضرراً من التهديدات الخارجية نظراً لمعرفة منفذيها بتفاصيل نظام المعلومات.

8

إدارة أمن ورقابة المعلومات وخطواتها

2-تحديد المخاطر Risks:

- حدد Mcleod & Schell أربع أنواع من المخاطر وهي:
  1. **سرقة وإفشاء معلومات بشكل غير مشروع**
  2. **استخدام غير مشروع**
  3. **تدمير وإيقاف غير مشروع لخدمة معينة**
  4. **تغيير غير مشروع**

أين تتجه المخاطر والاعتداءات في بيئة المعلومات؟

1. **الأجهـزة:** وهي كافة المعدات والأدوات المادية التي تتكون منها النظم، كالشاشات والطابعات ومكوناتها الداخلية ووسائط التخزين المادية وغيرها.
2. **البرامـج:** وهي الاوامر المرتبة في نسق معين لإنجاز الاعمال، وهي إما مستقلة عن النظام أو مخزنة فيه.
3. **المعطيـات:** إنها الدم الحي للأنظمة، وما سيكون محلا لجرائم الكمبيوتر، وتشمل كافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظم. والمعطيات قد تكون في طور الادخال أو الاخراج أو التخزين أو التبادل بين النظم عبر الشبكات، وقد تخزن داخل النظم أو على وسائط التخزين خارجه.
4. **الاتصـالات:** وتشمل شبكات الاتصال التي تربط أجهزة التقنية بعضها بعض محليا ودوليا، وتتيح فرصة اختراق النظم عبرها كما أنها بذاتها محل وموطن للاعتداء.

9

إدارة أمن ورقابة المعلومات وخطواتها

3-إعداد سياسة أمن المعلومات:

- يمكن تعريف سياسة أمن المعلومات ISP بأنها **مجموعة من القواعد أو التعليمات المحددة والمعمول بها في منظمة ما، وتهدف تلك السياسة إلى تدنية خطر حوادث المعلومات.**
- كل المعلومات (بغض النظر عن الشكل أو التنسيق) المستخدمة لدعم أنشطة الأعمال هي معلومات الشركة. إن معلومات الشركة هي أصل من أصول الشركة ويجب أن تكون محمية من الضياع والتخريب (خلال فترة صلاحيتها) ومنظمة من قبل المصرح لهم بذلك، ويجب صيانة المعلومات بأسلوب آمن ودقيق وموثوق به وإتاحتها بسهولة للاستخدام المرخص، ويجب تصنيف المعلومات بالاعتماد على متطلبات حساسيتها ووضعها القانوني والاحتفاظ بها ووفقًا لنوع الدخول المطلوب من قبل الموظفين المرخص لهم.
- إن أمن المعلومات هو حماية البيانات من الإفشاء أو التحوير أو الإزالة. ويجب حماية المعلومات نظراً لقيمتها وخصوصيتها وحساسيتها للشركة فضلاً عن مخاطر إزالتها أو إفشائها. ويجب أن تكون المعلومات محدثة ومحمية -كحد أدنى- بحيث يتمكن الأفراد المرخص لهم فقط من تعديلها وإزالتها.

10

➢ كيفية توفير الحماية لنظام المعلومات

1. وضع كلمة سر أو الرمز أو الرقم الشخصي للولوج إلى الملفات الهامة أو حتى للنظام وعدم استخدام كلمة المرور لأكثر من مستخدم للحاسب أو النظام.
2. تثبيت أو تحميل برنامجاً أو أكثر لمقاومة الفيروسات الإلكترونية الضارة.
3. مراعاة الإجراءات الأمنية لحماية الدخول إلى شبكة الإنترنت والتأكد من مصادر البريد الإلكتروني، فإذا كان الحاسب خاص بدائرة أو منشأة ويضم بيانات هامة سرية لا بد من زيادة الإجراءات الأمنية بتحميل البرامج المضادة للفيروسات والاختراق والجداران النارية وتشفير الرسائل الإلكترونية.
4. حماية مواقع التجارة الإلكترونية للحفاظ على بيانات الزبائن وأرقام بطاقات الائتمان، والحفاظ على طلبات الشراء من التغيير أثناء إرسالها من العميل إلى قاعدة بيانات الموقع، والحفاظ على الفواتير أثناء إرسالها من موقع الشركة إلى العميل.

11

➢ كيفية توفير الحماية لنظام المعلومات

5. اعتماد بصمة الإصبع أو بصمة العين والصوت التي تتميز بعدم تكرارها من شخص لآخر حيث أن لكل إنسان بصمة إصبع وبصمة عين لا تتطابق مع إنسان آخر.
6. تحديد نطاق الاستخدام Authorization : وهو ما يعرف بالتخويل أو التصريح باستخدام قطاع ما من المعلومات في النظام، كما يتحكم بالدخول والوصول إلى المعلومات أو أجزاء من النظام.
7. إجراء النسخ الاحتياطي Backup : وهي عبارة عن إنشاء نسخة إضافية من المواد المخزنة على إحدى وسائط التخزين سواءً داخل النظام أو خارجه، وتخضع عملية الحفظ أو النسخ الاحتياطي إلى مجموعة من القواعد محددة وموثقة يجري الالتزام بها لضمان توحيد معايير الحفظ وحماية النسخ الاحتياطية.

12

➢ المخاطر والمصاعب التي تواجه أي نظام معلومات

1. **العبث: والغش بالبيانات.**
2. **خداع بروتوكول الإنترنت: أي التخفي باستغلال بروتوكولات النقل باستخدام برامج خاصة مثل برامج الاختراق والقرصنة والفيروسات وملفات الكوكيز.**
3. **التقاط كلمات السر: سابقاً كانت عن طريق تخمين كلمات السر نتيجة لضعفها أو لكونها مطابقة لاسم شخص أو تاريخ ميلاده مثلاً، وحديثاً أصبحت تُستخدم برامج تجري سلسلة من الاحتمالات باستخدام الحروف أو الأرقام أو الاثنين معاً بمجرد تحديد عدد الخانات المطلوبة أو القصوى لكلمات السر المُستخدمة على النظام.**
4. **استقبال الرسائل الإلكترونية غير معروفة المصدر.**
5. **تحميل البرامج المجانية: من مواقع غير متخصصة بالبرمجيات وينتج عنها عدم الكشف أو التأكد من خلو ملفاتها من الفيروسات أو ملفات التجسس.**

13

➢ أسباب ضعف أي نظام معلومات

1. **الاعتداء على حق التخويل: ويحدث ذلك عند تعدي أي موظف للحدود التي تم تخويله للعمل عليها على النظام مما يؤدي إلى احتمال العبث ولو كان عن غير قصد بملفات قد تكون بالغة السرية أو الأهمية مما يسئ إلى أمن النظام.**
2. **دخول شخص غير مصرح له: إلى النظام باستخدام كلمة سر مستخدم مشروع مما يتيح تجاوز الحدود المخولة للموظف أو زراعة ملفات تجسسية مثل (حصان طروادة) الذي يعمل كبرنامج لمعالجة النصوص فيما يقوم بنسخ معلومات النظام في ملف يُتاح بعدها للإطلاع لأي مخترق للنظام.**
3. **اعتراض الاتصالات: في هذه الحالة يتم اعتراض البيانات المنقولة عبر الشبكة مثلاً ليتم تعديلها بما يتوافق مع غرض الاعتداء.**
4. **عدم الإقرار بالقيام بالتصرف: يتمثل هذا الخطر في عدم اعتراف الجاني أو المذنب بأنه من قام بارتكاب الخطأ كأن يُعطي كلمة السر لشخص غير مخول له باستخدام النظام ثم يقوم بإنكار أنه قد فعل ذلك مما يشتت خطة النظام لمقاومة الأخطار التي تستهدفه.**
5. **إرسال كمية كبيرة من الرسائل الإلكترونية :إلى بريد الموقع المُستهدف ليتم إرباك النظام وإضعاف برامج حماية المعلومات مثل: البرامج المضادة للفيروسات أو الاختراق.**

14

➢أنواع الفيروسات

تتنوع الفيروسات بتنوع الغرض أو نوع التخريب الذي صُنعت من أجله، ويمكن توضيح أشهر أنواعها كما يلي:

١. حصان طراودة: هو جزء صغير من الكود يضاف إلى البرمجيات ولا يخدم الوظائف العادية التي صممت من أجلها هذه البرمجيات ولكنه يؤدي عملا تخريبياً للنظام، والنظام لا يشعر بوجوده حتى تحين اللحظة المحددة لعمله.

٢. القنابل المنطقية: هي أحد أنواع حصان طراودة وتُصمم بحيث تعمل عند حدوث ظروف معينة أو لدى تنفيذ أمر معين، مثلاً: (عند بلوغ عدد الموظفين في الشركة عدداً معيناً من الموظفين، إذا تم رفع اسم المخرب (واضع القنبلة) من كشوف الراتب)، وتؤدي القنبلة في هذه الحالة إلى تخريب بعض النظم أو إلى مسح بعض البيانات أو تعطيل النظام عن العمل.

٣. القنابل الموقوتة: هي نوع خاص من القنابل المنطقية وهي تعمل في ساعة محددة أو في يوم معين، مثلاً: (عندما يوافق اليوم الثالث عشر من الشهر يوم الجمعة).

٤. باب المصيدة: هذا الكود يوضع عمداً بحيث يتم- لدى حدوث ظرف معين - تجاوز نظم الحماية والأمن في النظام، ويتم زرع هذا الكود عند تركيب النظام بحيث يعطي المخرب حرية تحديد الوقت الذي يشاء لتخريب النظام فهو يظل كامناً غير مؤذ حتى يقرر المخرب استخدامه، وكمثال على ذلك إقحام كود في في نظام الحماية والأمن يتعرف على شخصية المخرب ويفتح له الأبواب دون إجراء الفحوص المعتادة.

٥. الديدان: هي عبارة عن كود يسبب أذى للنظام عند استدعائه، وتتميز الدودة بقدرتها على إعادة توليد نفسها، بمعنى أن أي ملف أو جهاز متصل بالشبكة تصل إليه الدودة يتلوث، وتنتقل هذه الدودة إلى ملف آخر أو جهاز آخر في الشبكة وهكذا تنتشر الدودة وتتوالد.

15

➢أهم طرق الوقاية من الفيروسات

1. تجهيز عدة نسخ من البرمجيات (نسخ احتياطية) وحفظها بحيث يمكن استرجاع نسخة نظيفة (غير ملوثة بالفيروس) من البرنامج عند الحاجة.

٢. الاحتفاظ بسجل لكل عمليات التعديل في برامج التطبيقات بحيث يتم تسجيل جميع وقائع نقل البرامج، وبخاصة تلك البرامج المجلوبة من خارج المؤسسة.

٣. يجب توعية المستخدمين بعدم تحميل أي برنامج مجلوب من الخارج في حاسباتهم الشخصية، لأن تلك هي الوسيلة الأسرع لدخول الفيروسات إلى النظم، وخاصة البرامج المجانية المنتشرة على الكثير من مواقع شبكة الإنترنت غير الموثوق بها أو غير المؤمنة.

٤. فحص البرمجيات أو اختبارها قبل السماح بنشرها على جهاز غير متصل بالشبكة، ويجب أن يتضمن الاختبار البحث عن أي سلوك غير مفهوم في البرنامج كأن يُصدر رسائل غير مفهومة أو في غير مناسبتها.

5. فحص البريد الإلكتروني (الرسائل الواردة) قبل فتحه وخاصة البريد الوارد من عناوين إلكترونية غير معروفة بالنسبة إليك، والجدير بالذكر أن البرامج المجانية والبريد الإلكتروني هما الوسيلة الأكثر انتشاراً لانتقال الفيروسات عبر شبكة الإنترنت.

6. تحميل البرامج المضادة للفيروسات (النسخة الأصلية) وذلك لأن هذه البرامج تقوم بالتأكد من عدم وجود الفيروسات المعروفة، وتكون عديمة الفائدة في مواجهة الفيروسات الجديدة إلا إذا تم تحديث البرنامج من موقع الشركة المنتجة أو المصنعة له على شبكة الإنترنت، ولا يتم التحديث بشكل صحيح إلا إذا كان البرنامج أصلياً.

16

ومن أشهر البرامج المضادة للفيروسات: (برنامج كاسبر سكاي Kaspersky، برنامج النورتون Norton، مكافي Macafee، باندا Panda)

(ملاحظة)

- **يجب تشغّيل البرامج المضادة للفيروسات بصورة دورية وتثبّيت خيارات تفحص جميع المجلدات والأقراص والذاكرة والبريد الإلكتروني للتأكد من تفحص كل مواقع الجهاز.**

17