ملخص

المبحث الأول: المفاهيم العامة للأمن المعلوماتي

المطلب الأول: تعريف الأمن المعلوماتي وأهميته

الأمن المعلوماتي هو مجموعة من القوانين، والإجراءات، والوسائل التقنية والتنظيمية اللي تهدف لحماية المعلومات من أي تهديد، سواء كان سرقتها أو تعديلها أو حتى الاطلاع عليها من طرف ناس ما عندهمش الحق في ذلك. هذا يشمل:

1. البُعد التقني :اللي يتعلّق بأنظمة الحماية.
2. البُعد التنظيمي :اللي يتعلّق بالسياسات واللوائح.
3. البُعد البشري :اللي يتعلّق بوعي الموظفين واهتمامهم.

أهمية الأمن المعلوماتي :الأمن المعلوماتي مهم باش يحمي المؤسسات من أي هجوم أو تهديد إلكتروني. إذا ما كانش الحماية الكافية، ممكن تضيع البيانات المهمة وتخسر سمعة المؤسسة أو حتى تتعرض لخسائر مالية.

أمثلة على الأهمية:

- مثلاً، لو مؤسسة ما حميتش بيانات زبائنها، يمكن تحصل على سرقة معلومات شخصية ومالية وهذا ممكن يضرّ سمعتها.
- إذا كانت البيانات ضايعة أو تم تعديلها، ممكن قرارات المؤسسة تكون خاطئة وتسبب مشاكل كبيرة

المطلب الثاني: أهداف الأمن المعلوماتي

1. **السرية:(Confidentiality)** الهدف هو حماية المعلومات من الاطلاع غير المصرح به. يعني، لازم تكون المعلومات متاحة فقط للأشخاص اللي عندهم الحق يشوفوها.
    - مثال :في مستشفى، مريض ما يحبش بياناته تكون مكشوفة للناس الآخرين، فيجب حماية معلوماته عن المرض والعلاج.
2. **السلامة أو النزاهة:(Integrity)** الهدف هو ضمان أن البيانات تبقى صحيحة ومش متلاعب فيها. يعني أي تغيير في البيانات لازم يكون من طرف شخص موثوق.
    - مثال :إذا كان فيه تقرير مالي في شركة، لازم البيانات تكون صحيحة، وما تكونش هناك أي تغييرات قد تؤدي لتضليل القارئ.
3. **التوافر:(Availability)** الهدف هو ضمان أن البيانات متاحة في أي وقت وبدون مشاكل.
    - مثال :في بنك، إذا كان النظام المالي ما يشتغلش في وقت معين، الناس ما يقدرونش يسحبوا فلوسهم وهذا يتسبب في خسائر كبيرة.

الأهداف الأخرى:

.1تعزيز الثقة الرقمية :نفترض عندك مؤسسة بنكية كبيرة، والناس دايرين تعاملات بنكية عبر الإنترنت. إذا كانت هادي المؤسسة عندها نظام أمني قوي (كيما تشفير البيانات) وزبائنها يعرفوها تحمي معلوماتهم الخاصة، رح يكون عندهم

ثقة أكبر في التعامل مع هاد البنك. **مثلاً**، زبون يحط بياناته البنكية عبر الإنترنت، وبفضل حماية المؤسسة، يعرف أن معلوماته مش رح تروح لناس ما عندهمش حق فيها. هادي الثقة تخلي الزبائن يرجعو ويديرو معاملات أكتر مع البنك. في الأسواق الرقمية، هادي الثقة تُعتبر ميزة تنافسية، لأن الزبائن رح يختارو المؤسسات اللي يحسو أنها تحترم بياناتهم.

.2الامتثال للتشريعات والمعايير :مثال على الامتثال للتشريعات: عندك مستشفى تتعامل مع بيانات طبية حساسة. إذا ما التزمتش بالمواصفات الأمنية، كيما مثلاً قوانين حماية البيانات الشخصية(، يمكن يتعرض المستشفى لغرامات ضخمة. **مثلا**، لو تم تسريب بيانات مرضى أو اطلاع شخص غير مخول على معلوماتهم، رح يتعرض المستشفى للمسؤولية القانونية. بصح إذا التزمت المستشفى بالقوانين ووضعت أنظمة أمان متطورة، رح تكون أكثر مصداقية وتجنب العقوبات القانونية، وبالطبع رح تحافظ على سمعتها في السوق.

.3ضمان استمرارية الأعمال :نفترض عندك شركة تجارية كبيرة. يوم من الأيام، تعرضت الشركة لتهديد سيبراني ووقع هجوم على أنظمتها. إذا ما كان عندهم خطة استرجاع وحماية، ممكن تكون الشركة توقفت لساعات أو أيام، وهذا رح يأثر على مبيعاتهم وعلاقتهم مع الزبائن. لكن إذا كان عندهم خطة متكاملة للطوارئ والنسخ الاحتياطي، ممكن يواجهوا الموقف بسرعة ويعودوا للعمل في أقرب وقت. **مثلاً**، لو كانت الشركة عندها نسخ احتياطية للبيانات المهمة على سيرفر بعيد، إذا حصلت مشكلة في النظام، يقدروا يسترجعوا كل شيء ويستمروا في عملهم من دون توقف كبير، مما يساعدهم في الحفاظ على استمرارية الأعمال وتقليل الخسائر.

المبحث الثاني: التهديدات والمخاطر المرتبطة بالأمن المعلوماتي

المطلب الأول: التهديدات التقنية

- الفيروسات :برامج تخريبية تدمّر البيانات أو تتسبب في خلل بالنظام.
  - مثال :فيروس يهاجم جهاز كمبيوتر ويخرب الملفات الموجودة فيه.
- الديدان :برامج تنتشر عبر الشبكة وتستهلك موارد الجهاز.
  - مثال :دودة تنتشر من جهاز لجهاز آخر عبر الإنترنت وتستنفد قدرة النظام على العمل بشكل طبيعي.
- أحصنة طروادة :برامج تدّعي أنها شرعية لكن في داخلها أكواد ضارة.
  - مثال :برنامج يظهر على أنه مضاد للفيروسات لكنه في الواقع يحمل فيروس لتخريب النظام.
- هجمات حجب الخدمة :(DoS) هجوم يهدف لإغراق النظام بطلبات كبيرة لدرجة أنه ما يقدرش يقدّم الخدمات.
  - مثال :الهجوم على مواقع الإنترنت الشهيرة مثل فيسبوك لتوقف الخدمة.

المطلب الثاني: التهديدات البشرية والطبيعية

- الخطأ البشري :الموظف يخطئ، مثل أنه يمسح ملف مهم أو يرسل معلومات حساسة.
  - مثال :موظف يمسح قاعدة بيانات كاملة عن غير قصد.
- السلوك المتعمد :مثل الموظف الذي يسرق أو يبيع معلومات سرية.
  - مثال :موظف داخل شركة يسرّب معلومات عن مشاريع الشركة لمنافسين.
- الكوارث الطبيعية :مثل الزلازل أو الفيضانات التي تدمّر المعدات وتُفقد البيانات.

- مثال :زلزال يهدم مخزن بيانات شركة ويؤدي لفقدان كل الملفات.

المبحث الثالث: استراتيجيات وأساليب الحماية المعلوماتية

المطلب الأول: الحلول التقنية لأمن المعلومات

- الجدران النارية :(Firewalls) هي حاجز أمني بين الإنترنت والشبكة الداخلية، تمنع الدخول الغير مصرح به.
  - مثال :الجدار الناري يحمي الشبكة من هجوم إلكتروني من الخارج.
- برامج مكافحة الفيروسات :تكشف وتحمي من الفيروسات والبرمجيات الخبيثة.
  - مثال :برنامج مضاد للفيروسات يكشف فيروس جديد ويمنع انتشاره.
- تقنيات التشفير :تحوّل المعلومات إلى صيغة مشفّرة.
  - مثال :لو أرسلت رسالة عبر الإنترنت، التشفير يمنع أي شخص آخر من قراءتها.
- أنظمة كشف التسلل :(IDS) تحلل حركة المرور داخل الشبكة للكشف عن أي نشاط مشبوه.
  - مثال :النظام يكشف محاولات لاختراق الشبكة عبر مراقبة الأنماط غير الطبيعية.

المطلب الثاني: السياسات والإجراءات التنظيمية

- تحديد صلاحيات الوصول :يعني كل موظف عنده صلاحيات معينة للوصول للبيانات.
  - مثال :الموظف في قسم المحاسبة ما يقدرش يفتح ملفات الأبحاث العلمية.
- إعداد سياسات مكتوبة :تتضمن القواعد، مثل سياسة كلمات المرور.
  - مثال :لازم كل موظف يغير كلمة المرور كل 3 أشهر.
- التوعية والتكوين :تدريب الموظفين على كيفية حماية المعلومات.
  - مثال :تنظيم ورش عمل لتعليم الموظفين كيفية التعامل مع البريد الإلكتروني بأمان.

المطلب الثالث: دور المستخدم في الحفاظ على أمن المعلومات

- الوعي الأمني :معرفة الموظفين بكيفية حماية المعلومات.
  - مثال :عدم فتح روابط مشبوهة في البريد الإلكتروني.
- الإبلاغ الفوري عن الحوادث :إذا كان في هجوم أو مشكلة، يجب على الموظف إبلاغ المسؤول فوراً.
  - مثال :إذا اكتشف الموظف أن جهازه مصاب بفيروس، يجب أن يخبر قسم الأمن.
- المشاركة في تدريبات المحاكاة :تدريب الموظفين على كيفية التعامل مع الهجمات المعلوماتية.
  - مثال :تنظيم تمرين يحاكي هجوم إلكتروني لكي يتدرب الموظفون على كيفية التصرف.