المحاضرة الثانية: أمن نظم المعلومات المحوسبة

أولا: تصنيف مخاطر نظم المعلومات المحوسبة

نظم المعلومات المحوسبة تواجه مجموعة واسعة من المخاطر التي يمكن تصنيفها إلى عدة أنواع رئيسية:

1- **مخاطر الكوارث الطبيعية:** تشمل الحرائق، الزلازل، الفيضانات، والأعاصير، والتي يمكن أن تسبب تدميرا فعليا للبنية التحتية لنظم المعلومات.

2- **مخاطر بشرية:** تتضمن الأخطاء البشرية، مثل الإعدادات غير الصحيحة أو التعامل غير الآمن مع البيانات، إلى جانب التهديدات الخبيثة مثل الاختراقات والتجسس الإلكتروني.

3- **مخاطر فنية:** ترتبط بالأعطال التقنية، سواء كانت في العتاد أو البرمجيات أو الشبكات.

4- **مخاطر التشغيل:** تشمل الأخطاء في العمليات اليومية، وعدم توفر الكوادر المدربة بشكل كافٍ أو ضعف الإجراءات التنظيمية اللازمة لحماية البيانات.

ثانيا: مفهوم أمن المعلومات

أمن المعلومات هو مزيج من السياسات والإجراءات والأدوات التي تهدف إلى حماية البيانات الرقمية من أي تهديدات. يشمل ذلك الحفاظ على:

1- **السرية:** ضمان الوصول إلى المعلومات من قِبل الأشخاص المخولين فقط.

2- **النزاهة:** الحفاظ على دقة واكتمال المعلومات، وضمان عدم التعديل عليها بشكل غير مصرح به.

3- **التوافر:** التأكد من أن المعلومات والخدمات متاحة عند الحاجة.

ثالثا: عناصر أمن المعلومات

يشمل أمن المعلومات أربعة عناصر أساسية:

1- **السرية (Confidentiality):** تحمي المعلومات من الوصول غير المصرح به.

2- **النزاهة (Integrity):** تضمن أن تبقى المعلومات دقيقة وغير متأثرة بأي تعديل غير مرغوب.

3- **التوافر (Availability):** تهدف إلى تأمين الوصول المستمر إلى المعلومات.

4- **الموثوقية (Authenticity):** التحقق من هوية الأطراف المتعاملة مع المعلومات لضمان أمان التعاملات.

رابعا: معايير وسياسات أمن المعلومات

تشمل سياسات أمن المعلومات استراتيجيات متكاملة تحمي النظام من المخاطر المتعددة. وتركز هذه السياسات على حماية أربعة جوانب رئيسية:

1- حماية العتاد (Hardware Security)

تشمل حماية أجهزة الكمبيوتر والخوادم وأجهزة الشبكة من السرقة أو التلف. يمكن تحقيق ذلك من خلال تأمين المواقع الفعلية للأجهزة، واستخدام أنظمة الرقابة والتحكم المادي.

2- حماية الأفراد (Personnel Security)

يشمل تدريب وتوعية الموظفين حول المخاطر الأمنية، واتباع إجراءات التحقق من الهوية للوصول إلى البيانات الحساسة. هذا العنصر يعتمد أيضا على التحلي باليقظة وتطبيق سياسات مكافحة الهندسة الاجتماعية.

3- حماية البرمجيات (Software Security)

تتضمن حماية البرامج من التهديدات مثل الفيروسات وبرامج التجسس والهجمات الخبيثة. يتم ذلك من خلال تثبيت التحديثات، واستخدام برمجيات الحماية مثل جدران الحماية وبرامج مكافحة الفيروسات.

4- حماية قواعد البيانات (Database Security)

تهدف إلى حماية البيانات المخزنة من الوصول غير المصرح به والتعديل. تستخدم تقنيات مثل تشفير البيانات، وأنظمة إدارة الوصول، وتطبيقات النسخ الاحتياطي لضمان حماية البيانات واستردادها عند الحاجة.