الوحدة السادسة

مقدمة في أمن المعلومات والخصوصية

والجرائم المعلوماتية

**أمن المعلومات** : العلم الذي يختص بحماية المعلومات وانظمتها من المخاطر التي تهددها

اخطار تواجه المعلومات :

* خطر كشف المعلومات السرية
* خطر الحرمان المعلومات
* خطر تغيير المعلومات

**عناصر أمن المعلومات CIA:**

* السرية :
* التكاملية وسلامة المحتوى: التاكد من الحفاظ على دقة وسلامة البيانات والمعلومات من التغيير
* استمرارية الخدمات وتوفر المعلومات : ان المعلومات وانظمتها بكل خدمتها متاحة عند الحاجه

**مهددات أمن المعلومات :**

**البرامج الخبيثة:** برامج تسبب الضرر للنظام او للمستخدم

1. الفيروسات : برامج صممت لالحاق الضرر بالحاسب لتدمير البيانات وحذفها او تشفيرها ولها القدرة على الانتشار من ملف للاخر داخل الحاسب
2. الديدان : مثل الفيروسات لكن لها خاصية الاعتمادية على نفسها والتكاثر تلقائياً في النظام او الشبكة مما يجعله بطيئ اومتوقف
3. برامج الفدية Ransomware: تقوم بتشفير كامل للمفلات والمعلومات وتطلب مقابل ماد لفك التشفير
4. برامج التجسس : لها القدرة على التخفي والمتابعة وسرقة الهوية وتسجيل الضغطات على الكيبورد
5. برامج الاعلانات : شبيهه بالتجسس لكن الهدف منها نشر الاعلانات وجمع بيانات المستخدمين
6. برامج الاحتيالية والبلاغ الكاذب:اعلانات منبثقه تتظاهر بانها برامج مكافحة فيروسات وهي بالاساس تصيب النظام
7. برامج البوت نت : برامج تعمل في جهاز الضحية بهدف استخدامه للهجوم على طرف ثالث يسمى الضحية بوت والمهاجم بوت ماستر
8. احصنة طروادة: برامج تحقن ببرامج اخرى لتحملها للنظام وتكون خاملة لفترات طويلة دون اكتشاف امرها
9. القنابل المنطقية: برامج تبقى خاملة حى يتحقق الشر المنطقي كازيارة موقع البنك عندها تتم مراقبته وسرقة المعلومات
10. الابواب الخلفية " المستترة " :ثغرات توضع عمداً اثناء التطوير لمتابعة مشاكل التعليمات

**من أين تاتي البرامج الخبيثة ؟ :**

وسائط التخزين القابلة للازالة

رسائل ومرفقات البريد

تنزيل ملفات من الانترنت

زيارة المواقع الملوثة

الشبكات الملوثة والمنافذ المفتوحة

**المخترقين " الهاكرز" :** المهاجمون الذين يدخلون للانظمة بهدف الاخلال او التسريب او التعديل او التجسس على المعلومات

1. المخترقين الداخليين : موظفين يقومون باختراق انظمة المنظمة التي يعملون لديها بهدف التسريب او التعديل او مساعدة مخترقين خارجيين
2. المخترقين الخارجيين :

* **محترفيين** مثل

ذوي القبعات السوداء : القصد من اختراقهم التخريب

ذوي القبعات البيضاء:القصد من اختراقهم ايجاد الثغرات

ذوي القبعات الرمادية: يكونون بالاصل من القبعات البيضاء ثم في اوقات معينة يتحولون للسوداء

* **غير محترفين او اطفال برمجيات** :يحاولون الاختراق والتخريب باستخدام برامج جاهزة

أهم اشكال الهجمات الالكترونية على أنظمة المعلومات :

* هجمات استغلال الثغرات : **الثغرات** **هي اخطاء غير مقصودة في التعليمات البرمجية للبرنامج او النظام**  وعادة م يستغلها المخترقون للدخول للنظام
* هجمات بالبرامج الخبيثة
* هجمات حجب الخدمة : يقوم المخربين بارسال كمية هائلة من الاوامر لتعطيله وحجب خدماته تستخدم في شبكات البوت نت
* هجمات الهندسة الاجتماعية : اختراق عقل المستخدم بطرق نفسية اجتماعية ممايساعد لجمع المعلومات منه

اساليب غير الكترونية : لاتحتاج لاجهزة الكترونية ليتم التواصل بين المخترق والضحية

البحث في المهملات - مراقبة الضحية من الخلف- التتبع والتمثيل

اساليب الكترونية: يكون التواصل الكتروني بين المهاجم والضحية

التمثيل عبر الهاتف- التصيد الالكتروني-مواقع انترنت وهمية " نوع من التصيد الالكتروني"

**الخصوصية :**  قدرة الافراد او المجموعات عبى التحكم بالمعلومات الخاصة بهم ومنع الاخرين من الاطلاع عليها الا برغبتهم

مهدداتها :

الشركات وجمع البيانات - الخصوصية في الشبكات الاجتماعية -التنمر الالكتروني - سرقة وفقد الاجهزة - سرقة الهوية عل الانترنت

**طرق الوقاية والحماية :**

* التاكد من تحديث نظام التشغيل
* استخدام برامج مضادة للبرامج الخبيثة
* استخدام جدار ناري
* تشفير البيانات : ترميز البيانات من نصوص او ملفات بحيث يصبح الشكل الظاهري لها غير مفهوم
* اجراءات التحقق والمصادقة

شي يعلمه المستخدم : كلمة المرور والارقام السريه

شي يملكه المستخدم : البطاقات واجهزة الجوال

شي هو جزء من المستخدم او يستطيع عمله : بصمات الحيويه مثل الاصبع او العين او الصوت او التوقيع

* النسخ الاحتياطي
* الثقافه والتوعية

**استراتيجيات الحماية في المنظمة:**

* الحماية المادية
* حماية البينة التحتية لتكنولوجيا المعلومات
* التثقيف وتوعية المستخدمين
* وثيقة سياسة امن المعلومات
* الانذار المبكر والقدرة علة التعامل مع حالات الهجوم والكوارث
* التعافي السريع بعد الهجمات والكوارث

**الجريمة الالكترونية:** هي اي فعل يخالف الانظمة والقوانين ويستخدم لارتكابه الحاسب الالي وشبكات وتقنيات مختلفة يتضمن اختراق الانظمة ومواقع الانترنت وصناعة البرامج الخبيثة ونشرها وتسريب المعلومات السرية