مفهوم الامن السيبراني

محاضرة 5 \ الصف الثاني \كلية الحقوق

اولاً: تعريف الامن السيبراني

الأمن السيبراني، المعروف أيضًا باسم أمن المعلومات، يشير إلى مجموعة من التقنيات، السياسات، والممارسات المصممة لحماية و**الشبكات** ، **الأجهزة**، **البرامج**، و**البيانات** من الهجوم، الضرر، أو الوصول غير المصرح به. يتضمن هذا تطبيق تدابير لحماية البنية التحتية الرقمية وتأمين البيانات الحساسة، سواء كانت تتعلق معلومات شخصية، مالية، أو حكومية.

ثانياً: التطور الزمني لمجال البحث في الامن السيبراني

- **المراحل الأولى:** في بدايات الحوسبة، كان **الأمن السيبراني** مقتصرًا على الحماية من الفيروسات والبرمجيات الخبيثة. كانت المخاوف الأمنية محدودة نظرًا لانخفاض عدد المستخدمين ونطاق استخدام الشبكات.
- **التطور مع الإنترنت:** مع انتشار الإنترنت في التسعينيات، زادت الحاجة لتطوير تقنيات أمنية أكثر تعقيدًا. ظهرت التحديات الجديدة مثل هجمات الفيشينج، التجسس الإلكتروني، وهجمات الحرمان من الخدمة (DDoS).
- **العصر الحديث:** في الوقت الراهن، يتضمن **الأمن السيبراني** تقنيات متطورة مثل التشفير، الأمان السحابي، والكشف عن التهديدات بالذكاء الاصطناعي. الهجمات السيبرانية أصبحت أكثر تعقيدًا وتتطلب استجابات أمنية متطورة.

****التصيد الإلكتروني أو التصيد الاحتيالي أو التصيّد ((Phishing)هو محاولة للحصول على معلومات حساسة مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقة الائتمان (والأموال)؛ غالبًا لأسباب ضارة، وذلك بالتنكر ككيان جدير بالثقة في اتصال إلكتروني. المصطلح الإنجليزي Phishingهو كلمة مستحدثة أُنشئت باعتبارها مُجَانِسَةً لفظيةً لكلمة fishingالتي تعني "صيد الأسماك"؛ بسبب تشابه استخدام الطعم في محاولة للقبض على الضحية.**

****هجمات الحرمان من الخدمة (Distributed Denial of Service (DDoS))**

ثالثاً: اهمية الامن السيبراني في عصر الانترنيت

- **حماية البيانات الشخصية:** في عالم يتزايد فيه التواصل الرقمي، يصبح من الضروري حماية المعلومات الشخصية مثل الهويات، كلمات المرور، وتفاصيل الحسابات المصرفية.
- **أمن المؤسسات:** يعد الأمن السيبراني ضروري لحماية المعلومات والأصول التجارية من التهديدات مثل التجسس الصناعي والهجمات على البنية التحتية.
- **التأثير على السياسة الوطنية:** يلعب دورًا حيويًا في حماية البنى التحتية الوطنية والأمن القومي من الهجمات الإلكترونية والتخريب.
- **الثقة في التكنولوجيا:** يساعد في بناء الثقة بين المستخدمين والخدمات التكنولوجية، مما يسمح بتوسع الأمن السيبراني لحماية استخدام الأنظمة الرقمية بأمان.

انواع الامن السيبراني وتشمل:

1. امن الشبكة 2. امن البيانات 3. امن التطبيقات 4. امن النهايات

أمن الشبكة يتعلق بحماية البنية التحتية للشبكة والبيانات المتدفقة عبرها. هذا يشمل تدابير مثل:

- **جدران الحماية:** لمنع الوصول غير المصرح به.
- **نظام كشف التسلل:** لرصد الأنشطة المشبوهة والتحذير منها.
- **أمن VPN:** لتأمين الاتصالات عبر الإنترنت.

أمن البيانات يركز على حماية البيانات من التسريب، التلف، أو الاستخدام غير المشروع. يتضمن:

- **التشفير:** لحماية **البيانات** أثناء النقل والتخزين.
- **إدارة البيانات:** لضمان أن البيانات تُستخدم وتُخزن بشكل آمن.
- **النسخ الاحتياطي:** لضمان استعادة البيانات في حالة الخسارة.

أمن التطبيقات يتعامل مع الأمن في مرحلة تطوير البرامج وبعد نشرها. يشمل:

- **اختبار الاختراق:** لتحديد الثغرات الأمنية في التطبيقات.
- **تحديثات الأمان:** لإصلاح الثغرات والحفاظ على أمان التطبيقات.
- **الحماية ضد البرمجيات الخبيثة:** لمنع تثبيت البرمجيات الضارة.

أمن النهايات يهتم بحماية **أجهزة الكمبيوتر** والأجهزة المتصلة بالشبكة. يتضمن:

- **برامج مكافحة الفيروسات:** لمسح ومنع البرمجيات الخبيثة.
- **إدارة التحديثات:** للتأكد من أن جميع الأجهزة تستخدم أحدث البرامج والإصلاحات الأمنية.
- **التحكم في الوصول:** لضمان أن المستخدمين المصرح لهم فقط يمكنهم الوصول إلى الأجهزة والبيانات.

يعد فهم هذه الانواع من الامن السيبراني حاسماً لضمان حماية شاملة ضد مجموعة متنوعة من التهديدات الرقمية مما يساعد على تطوير استراتيجية امنية تتناسب مع الاحتياجات وتحمي من المخاطرالسيبرانية المتزايدة