وزارة التربية و التعليم
مديرية التربية والتعليم للواءي الطيبة والوسطية
مدرسة الخراج الثانوية المختلطة
ملخص شامل الدرس الأول: أمن البيانات والمعلومات – الصف التاسع

1. ما المقصود بأمن البيانات والمعلومات؟

هو مجموعة **سياسات وإجراءات وتقنيات** تهدف إلى حماية البيانات والمعلومات من الوصول غير المصرّح به وسوء الاستخدام أو التعديل أو العبث أو التعطّل أو الفقدان أو التلف.

2. الفرق بين أمن المعلومات والأمن السيبراني

- **أمن المعلومات :**يركز على حماية **المعلومات نفسها** سواء كانت رقمية أو ورقية.
- **الأمن السيبراني :(Cyber Security)** أوسع، ويركّز على حماية **الأنظمة والشبكات والأجهزة** في الفضاء الرقمي من الهجمات.
-

3. أهمية أمن البيانات والمعلومات

يساعد على:

- **الحفاظ على الخصوصية :**حماية البيانات الشخصية والحساسة من التسريب.
- **ضمان النزاهة (سلامة المعلومات) :**منع التلاعب بالبيانات لتبقى صحيحة ودقيقة.
- **ضمان التوافر :**بقاء المعلومات والخدمات متاحة عند الحاجة، وتقليل تأثير هجمات مثل حجب الخدمة.**(DoS)**
- **حماية الأصول :**لأن البيانات من أهم أصول المؤسسات.
- **الامتثال للقوانين :**مثل **GDPR**و **CCPA**التي تلزم المؤسسات بحماية بيانات المستخدمين.

الشكل (1-1): الركائز الثلاث لأمن المعلومات

4. ركائز أمن المعلومات الثلاث (CIA)

- **السرية :(Confidentiality)** لا يطّلع على المعلومات إلا المصرّح لهم.

أمثلة أدوات: التشفير، كلمات المرور، **MFA**، صلاحيات الوصول.

- **النزاهة :(Integrity)** بقاء المعلومات صحيحة دون تعديل غير مصرح.

أمثلة: أذونات الوصول، إدارة الهوية والوصول**(IAM)** ، التوقيع الرقمي.

- **التوافر :(Availability)** وصول المستخدمين المصرح لهم للخدمات والمعلومات وقت الحاجة.

أمثلة: النسخ الاحتياطي، خطط الطوارئ، الحماية من**DoS** ، صيانة الأنظمة.

5. عناصر/مجالات رئيسية في أمن المعلومات والأمن السيبراني

- **أمن التطبيقات :(Application Security)** حماية التطبيقات وفحص الثغرات (مثل أدوات فحص الثغرات).
- **الأمن السحابي :(Cloud Security)** حماية البيانات والخدمات على السحابة، والتحكم بالوصول والمراقبة.
- **التعافي من الكوارث :(Disaster Recovery)** خطة لاستعادة الأنظمة والبيانات بعد كارثة أو هجوم.
- **الاستجابة للحوادث :(Incident Response)** خطوات التعامل مع الحوادث مثل الاختراق أو تسريب البيانات، وقد يشمل أنظمة مثل **SIEM** للرصد والتحليل.
- **أمن البنية التحتية :(Infrastructure Security)** حماية الشبكات والخوادم والأجهزة وتحديثها وتأمينها.

- **إدارة الثغرات :(Vulnerability Management)** اكتشاف الثغرات وتقييمها ومعالجتها بشكل مستمر.

6. كلمات المرور: لماذا مهمة؟ وأفضل الممارسات

أفضل الممارسات لحماية الحسابات:

- **طول كلمة المرور :**يفضّل 12 حرفًا أو أكثر.
- **التعقيد :**مزج حروف كبيرة وصغيرة وأرقام ورموز.
- **التنوع :**تجنب الكلمات الشائعة مثل.**"password123"**
- **التحديث الدوري** عند الاشتباه أو حسب سياسة الجهة.
- **عدم إعادة الاستخدام** لنفس كلمة المرور في أكثر من حساب.
- **حفظها بشكل آمن)**عدم كتابتها في أماكن مكشوفة.**(**

بالتوفيق للجميع

معلمة المادة: هنادي وديان