الدرس: أمن الشبكات والمعلومات

يشير أمن الشبكات والمعلومات إلى الإجراءات والتقنيات المستخدمة لحماية البيانات والأنظمة والشبكات من الوصول غير المصرح به أو التلاعب أو التخريب .وبالنسبة لطلبة إدارة قواعد البيانات والتكنولوجيا المالية، فإن الأمن عنصر أساسي لحماية البيانات المالية الحساسة

2المفاهيم الأساسية للأمن

.1السرية (Confidentiality): حماية البيانات من الوصول غير المصرح به .الأساليب: التشفير، التحكم في الوصول، المصادقة

2 السلامة (Integrity): ضمان أن البيانات صحيحة وغير معدّلة بشكل غير قانوني .الأساليب: القيم التجزئية(Hashing) ، التوقيعات الرقمية2.3 .

3 التوافر (Availability) :ضمان وصول المستخدمين المخوّلين إلى البيانات في أي وقت .الأساليب: النسخ الاحتياطي، التكرار، خطط التعافي

2.4 .المصادقة (Authentication): التأكد من هوية المستخدم أو الجهاز .الأمثلة: كلمات المرور، البصمة، الرسائل المؤقتة 2.5 .التفويض (Authorization) :تحديد ما يمكن للمستخدم القيام به .مثال: صلاحيات 3:

3 .التهديدات الشائعة

3.1 البرمجيات الخبيثة (Malware) الفيروسات، الفدية، التجسس

3.2التصيد الاحتيالي (Phishing) رسائل تهدف لسرقة كلمات السر

33حقن (SQL Injection) SQL إدخال أوامر ضارة داخل استعلام

3.4 .SQL هجمات حجب الخدمة (DDoS) إغراق الخادم بطلبات كثيرة

3.5 .هجوم الرجل في الوسط (MITM) التجسس على الاتصال بين طرفين

4. الأمن في قواعد البيانات

4.1التحكم في الوصول باستخدام GRANT REVOKE

4.2 التشفير للبيانات أثناء النقل وفي التخزين:

4.3 .النسخ الاحتياطي والاسترجاع حماية من ضياع البيانات

4.4 .التدقيق (Auditing) متابعة من يقوم بتعديل البيانات

5. تقنيات أمن الشبكات

5.1الجدار الناري (Firewall): تصفيّة ومنع الاتصالات غير المصرح بها

5.2 .الشبكات الخاصة الافتراضية (VPN): تأمين الاتصال عن بعد

5.3 .أنظمة كشف/منع التسلل IDS/IPS: مراقبة وايقاف الهجمات

5.4 .البروتوكولات الآمنة : HTTPS – SSH – TLS.

6.أفضل الممارسات:

- ✓ كلمات مرور قوية
- ✓ تفعيل المصادقة الثنائية تحديث الأنظمة باستمرار
- ✓ تقليل الصلاحيات تدريب دوري على الأمن