جامعة المنارة

كلية: الهندسة

قسم: المعلوماتية

اسم المقرر: نظم المعلومات الإدارية

رقم الجلسة (١)

عنوان الجلسة

الأمان و السرية في نظم المعلومات الإدارية

إدارة المستخدمين

د. ايهاب ديباجة

م.جمال محمود

الفصل الدراسي : الأول

العام الدراسي :٢٠٢٥-٢٠٢٦

جدول المحتويات

Contents

العنوان	رقم الصفحة
مفهوم الأمان Security في نظم المعلومات	٣
بناء المستخدمين و إدارة الخيارات والصلاحيات في نظم المعلومات الإدارية	٤
خوارزمية بناء مستخدم	٦
مثال عملي	٧

الغاية من الجلسة:

- ✓ **مفهوم السرية Confidentiality في نظم المعلومات**
- ✓ **مفهوم الأمان Security في نظم المعلومات**
- ✓ **بناء المستخدمين و إدارة الصلاحيات في نظم المعلومات الإدارية**

مع تزايد اعتماد المؤسسات على نظم المعلومات الإدارية، أصبحت السرية والأمان من أهم ركائز حماية البيانات وضمان استمرارية العمليات. فقد أدت حوادث الاختراق والهجمات الإلكترونية إلى خسائر مالية وتشغيلية كبيرة، مما جعل أمن المعلومات جزءاً أساسياً من حوكمة المؤسسات المعاصرة.

مفهوم السرية Confidentiality

تشير السرية إلى حماية المعلومات من الوصول غير المصرح به، بحيث تُتاح فقط للمستخدمين الذين يمتلكون الصلاحية المناسبة.

أهداف السرية:

- حماية البيانات الحساسة والعملاء.
- منع الاستخدام غير القانوني للمعلومات.
- تعزيز الثقة في المؤسسة.

وسائل تحقيق السرية:

- إدارة الهوية والصلاحيات
- التشفير.Encryption
- سياسات الاستخدام المقبول.
- إخفاء البيانات.Data Masking

مثال تطبيقي مرتبط بالسرية:
قضية(2018) Cambridge Analytica
استُخدمت بيانات 87مليون مستخدم من Facebook دون إذن، ما كشف عن ضعف في سياسات الخصوصية والتحكم في صلاحيات التطبيقات.

مفهوم الأمان Security في نظم المعلومات :

الأمان هو مجموعة الإجراءات المصممة لحماية أصول المعلومات من التهديدات.

أنواع التهديدات الأمنية في نظم المعلومات الإدارية.:

- سوء الاستخدام الداخلي للصلاحيات.
- البرمجيات الخبيثة.(Malware)
- هجمات الفدية.Ransomware

هجوم برنامج الفدية (2017) WannaCry أصاب آلاف المؤسسات، خصوصاً قطاع الصحة البريطانيNHS ، مما أدى لإلغاء مواعيد طبية وتعطيل السجلات الإلكترونية
- الثغرات البرمجية.
- الهجمات على الشبكات..

- تثبيت التحديثات الأمنية بشكل متواصل.
- تدريب الموظفين على مواجهة التصيد الإلكتروني.
- الحريق، السرقة، الكوارث الطبيعية.
- تلف الأجهزة.

تعرضت مراكز بيانات في بعض المؤسسات للضرر بسبب انقطاع الكهرباء وعدم وجود أنظمة UPS كافية.

آليات الأمان في نظم المعلومات الإدارية

الضوابط التقنية:(Technical Controls)

- الجدران النارية.Firewalls
- أنظمة كشف الاختراق.IDS/IPS
- التشفير.
- بروتوكولات الاتصال الآمن.
- سياسات أمن المعلومات.
- إدارة المخاطر.

اختراق Yahoo (2013–2014) حيث تم تسريب بيانات ٣ مليارات حساب بسبب ضعف تقنيات التشفير.

اختراق شركة Equifax (2017) نتيجة إهمال تحديث ثغرة معروفة.

التوصيات لتعزيز السرية والأمان

١. تحديث الأنظمة بشكل دوري.
٢. تدريب الموظفين.
٣. تطبيق مبدأ أقل امتياز.
٤. إدارة الهوية والصلاحيات بشكل دقيق.
٥. إجراء اختبارات اختراق دورية.
٦. تبني خطط نسخ احتياطي قوية..

بناء المستخدمين و إدارة الخيارات والصلاحيات في نظم المعلومات الإدارية

تقوم نظم المعلومات الإدارية (MIS) على مجموعة من العناصر البشرية والتقنية التي تهدف إلى جمع البيانات ومعالجتها وتقديمها لدعم اتخاذ القرار. ومن أهم مكونات هذه الأنظمة إدارة المستخدمين، أي تحديد من يمكنه استخدام النظام، وكيف يستخدمه، وماذا يمكنه رؤيته أو تعديله. إن بناء المستخدمين وإدارة الخيارات والصلاحيات يُعدان حجر الأساس في حماية البيانات ورفع كفاءة العمل وضمان التوزيع السليم للأدوار داخل المؤسسة.

مفهوم إدارة المستخدمينUser Management

تشير إدارة المستخدمين إلى العمليات والإجراءات التي يتم من خلالها:

- إنشاء حسابات جديدة للمستخدمين.
- تنظيم الأدوار الوظيفية.
- تحديد مستويات الصلاحيات.
- متابعة الأنشطة داخل النظام.
- إيقاف أو تعديل حسابات حسب الحاجة.

أهداف إدارة المستخدمين:

١. ضمان وصول كل مستخدم فقط إلى المعلومات التي يحتاجها لأداء عمله.
٢. تقليل المخاطر الناتجة عن سوء الاستخدام أو الاختراق.
٣. رفع الكفاءة عبر تنظيم المهام وأتمتة إدارة الحسابات.
٤. تسهيل عمليات الرقابة والمراجعة.

تمر إدارة المستخدم عبر مجموعة من المراحل:

١. **طلب إنشاء مستخدم جديد (Provisioning)**
يتم تقديم طلب رسمي من رئيس القسم أو الإدارة لإنشاء حساب للمستخدم.
٢. **تحديد الدور Role Assignment**
تحديد موقع المستخدم في الهيكل التنظيمي وما يحتاجه من صلاحيات.
٣. **تفعيل الحساب Access Activation**
منح المستخدم صلاحيات محددة ضمن النظام.
٤. **مراقبة النشاط Monitoring**
مراجعة الأنشطة للتأكد من الالتزام بسياسات الأمن.
٥. **تعديل الصلاحيات Modification**
تغيير صلاحيات المستخدم عند تغيير مهامه الوظيفية.
٦. **تعطيل الحساب De-provisioning**
يتم عند مغادرة الموظف أو انتهاء الحاجة إليه.
٧. **مفهوم الأدوار Roles في نظم المعلومات**
الأدوار تمثل مستوى تنظيمي يحدد طبيعة وصول المستخدم للمعلومات.

أنواع الأدوار:

١. المستخدم العادي :وصول محدود، يقوم بمهامه اليومية.
٢. المشرف :Supervisor صلاحيات أوسع تشمل مراجعة وإدارة بعض وظائف النظام.
٣. المسؤول :Administrator يتحكم في إعدادات النظام ومراقبة المستخدمين.
٤. المدير التنفيذي :وصول إلى التقارير والتحليلات الإستراتيجية.

أهم أنواع الصلاحيات:

١. قراءة Read
٢. تحرير Edit
٣. إضافة Add
٤. حذف Delete
٥. موافقة Approval
٦. تصدير البيانات Export
٧. إدارة المستخدمين User Administration

خوارزمية بناء مستخدم جديد في نظام إداري مع مراعاة سرية متوسطة

المدخلات:

- طلب إنشاء مستخدم جديد من الإدارة المختصة.
- بيانات المستخدم الأساسية (اسم، رقم موظف، قسم، وظيفة).
- مستوى السرية المطلوب (في هذا السياق: سرية متوسطة).

الخوارزمية

١. التحقق من الطلب

```
IF request.isApproved == TRUE THEN
Proceed
ELSE
Reject request
END IF
```

الهدف :التأكد من وجود موافقة إدارية رسمية.

٢. تحديد الدور الوظيفيRole Assignment

```
role = mapUserRole(user.department, user.jobTitle)
```

الهدف :ربط المستخدم بالدور الصحيح وفق الهيكل الإداري.

٣. تحديد مستوى الصلاحيات (وفق سياسة السرية المتوسطة)

```
permissions = loadPermissions(role)
applyLeastPrivilege(permissions)
```

٤. إنشاء حساب المستخدم

```
userID = generateUserID(user.fullName)
password = generateSecurePassword()
createAccount(userID, password, role)
```

٥. معايير كلمة المرور (سرية متوسطة):
   - طول ≤ ١٠ أحرف
   - تحتوي حروف كبيرة وصغيرة
   - تحتوي رقم واحد على الأقل
   - تحتوي رمز خاص
   - تغيير إجباري عند أول تسجيل دخول

٦. تطبيق ضوابط التحقق من الهوية(Authentication)

```
EnableTwoFactorAuth(userID)
```

رسالة هاتف أو تطبيق مصادقة

٧. تطبيق ضوابط الجلساتSessions

```
sessionTimeout = 10 minutes
```

maxLoginAttempts = 5

الهدف :حماية النظام من محاولات التسلل أو الجلسات المفتوحة.

٨. تفعيل مراقبة الأحداثLogging

EnableAuditTrail(userID, actions = [login, view, edit, export])

٩. إخطار المستخدم بمعلومات الدخول

sendSecureEmail(userID, temporaryPassword)

ملاحظة :كلمة المرور تُرسل عبر قناة محمية ولا تُرسل بنص صريح.(Plain text)

١٠. الدخول الأولFirst Login

User logs in
System forces password_change()
System displays confidentiality_policy()
User must accept policy to continue

الخوارزمية بشكل مختصر(Flow Summary)

١. التحقق من الطلب.
٢. تعيين الدور الوظيفي المناسب.
٣. تحميل الصلاحيات وتطبيق مبدأ أقل امتياز.
٤. إنشاء حساب المستخدم.
٥. تفعيل المصادقة الثنائية.
٦. ضبط حدود الجلسة ومحاولات الدخول.
٧. تفعيل سجل التدقيق.
٨. إرسال بيانات الدخول المؤقتة بشكل آمن.

خوارزمية إنشاء مستخدم جديد في نظام إداري(SQL Procedure)

إنشاء جدول المستخدمين والصلاحيات (للتوضيح).

```
CREATE TABLE Users (
   UserID VARCHAR(50) PRIMARY KEY,
   FullName VARCHAR(100),
   Department VARCHAR(100),
   JobTitle VARCHAR(100),
   HashedPassword VARCHAR(255),
   RoleName VARCHAR(50),
   IsActive BIT DEFAULT 1,
   CreatedAt DATETIME DEFAULT GETDATE()
);
```

--جدول الأدوار Role-Based Access

```
CREATE TABLE Roles (
   RoleName VARCHAR(50) PRIMARY KEY,
   PermissionsLevel INT
);
```

--جدول سجل الأنشطة Audit Log

```
CREATE TABLE AuditTrail (
   LogID INT IDENTITY PRIMARY KEY,
   UserID VARCHAR(50),
   ActionType VARCHAR(50),
   ActionTime DATETIME DEFAULT GETDATE()
);
```

خوارزمية SQL لإنشاء المستخدم

```
Procedure: Create_New_User
CREATE PROCEDURE Create_New_User
(
   @FullName     VARCHAR(100),
   @Department   VARCHAR(100),
   @JobTitle     VARCHAR(100),
   @RequestedRole VARCHAR(50)
)
AS
BEGIN
   SET NOCOUNT ON;
```

التحقق من أن الدور موجود

```
   IF NOT EXISTS (SELECT 1 FROM Roles WHERE RoleName = @RequestedRole)
   BEGIN
      RAISERROR('Role does not exist.', 16, 1);
      RETURN;
   END
```

إنشاء UserID باستخدام أول ٣ أحرف من الاسم + رقم عشوائي

```
   DECLARE @UserID VARCHAR(50);
   SET @UserID = LOWER(LEFT(@FullName, 3)) + CAST(ABS(CHECKSUM(NEWID())) % 10000
AS VARCHAR);
```

إنشاء كلمة مرور مؤقتة (سيتم تغييرها عند أول دخول)

```
   DECLARE @TempPassword VARCHAR(50);
   SET @TempPassword = 'Tmp#' + CAST(ABS(CHECKSUM(NEWID())) % 999999 AS VARCHAR);
```

تشفير كلمة المرور

```
DECLARE @HashedPassword VARCHAR(255);
SET @HashedPassword = HASHBYTES('SHA2_256', @TempPassword);
```

إضافة المستخدم إلى جدولUsers

```
INSERT INTO Users (UserID, FullName, Department, JobTitle, HashedPassword, RoleName)
VALUES (@UserID, @FullName, @Department, @JobTitle, @HashedPassword,
@RequestedRole);
```

تسجيل العملية في سجل التدقيق

```
INSERT INTO AuditTrail (UserID, ActionType)
VALUES (@UserID, 'CREATE_USER');

EXEC Create_New_User
@FullName = 'Ahmed Ibrahim',
@Department = 'HR',
@JobTitle = 'HR Specialist',
@RequestedRole = 'HR_USER';
```