الوحدة 26: حماية البيانات والخصوصية

Data Classification

تصنيف البيانات حسب درجة الحساسية هو أساس الأمن. يساعد في تحديد مستوى الحماية المطلوب لكل نوع:

Public: بيانات عامة متاحة للجميع (لا ضرر من نشرها). مثال: الكتيبات التعريفية، الأسعار العامة.

Internal: بيانات داخلية للمؤسسة فقط (غير مصرح بها للخارج). مثال: سياسات الموارد البشرية، جداول الرواتب الداخلية.

Confidential: بيانات سرية (تسريبها يسبب ضررًا ماليًا أو قانونيًا). مثال: بيانات العملاء، العقود.

Restricted: بيانات مقيدة للغاية (تسريبها يسبب ضررًا بالغًا). مثال: الأسرار التجارية، براءات الاختراع.

Top Secret: بيانات سرية للغاية (أضرار كارثية على المستوى الوطني). مثال: معلومات استخباراتية عسكرية.

مصطلح إضافي:**PII (Personally Identifiable Information):** أي بيانات يمكن استخدامها لتعريف شخص (الاسم، البريد، رقم الهوية، رقم جواز السفر).

Data Lifecycle

دورة حياة البيانات تمر بمراحل:

1. **Create:** إنشاء البيانات.
2. **Store:** تخزينها.
3. **Use:** استخدامها في العمليات.
4. **Share:** مشاركتها مع أطراف أخرى.
5. **Archive:** أرشفتها بعد انتهاء الحاجة.
6. **Destroy:** إتلافها بشكل آمن.

Data Destruction

طرق إتلاف البيانات بأمان لضمان عدم استرجاعها:

- **Clearing:** مسح البيانات بإعادة تعيين القيم (مثل Format بسرعة). يمكن استرجاعها بأدوات متخصصة.
- **Purging:** مسح عميق باستخدام Degaussing (مجال مغناطيسي قوي) أو الكتابة فوق البيانات عدة مرات. غير قابل للاسترجاع.
- **Physical Destruction:** إتلاف مادي (تمزيق الأقراص، حرق، طحن). أضمن طريقة.
- **Cryptographic Erasure:** حذف مفتاح التشفير الخاص بمفتاح التشفير (KEK) يجعل البيانات مشفرة وغير قابلة لفك التشفير.

معايير المسح: 3) **DoD 5220.22-M** مرات كتابة)، **NIST 800-88** (طرق معتمدة).

(DLP (Data Loss Prevention

أنظمة منع فقدان البيانات تراقب وتمنع نقل البيانات الحساسة عبر:

- Network DLP: يراقب حركة الشبكة (بريد، HTTP).
- Endpoint DLP: يراقب نهايات الأجهزة (USB، طباعة).
- Storage DLP: يفحص البيانات المخزنة. يعمل بالكشف عن أنماط مثل أرقام بطاقات الائتمان (PCI).

(Encryption (BitLocker / TLS

BitLocker: تشفير كامل للقرص في Windows (AES-128 أو AES-256). يستخدم TPM (Trusted Platform Module) لحفظ مفاتيح التشفير بشكل آمن. يمكن دمجه مع Modern Standby للأجهزة المحمولة.

TLS (Transport Layer Security): تشفير الاتصالات بين المتصفح والخادم (HTTPS). يوفر السرية (Confidentiality)، التكامل (Integrity)، والمصادقة (Authentication). الإصدارات: TLS 1.2 / 1.3 (يجب تجنب SSL 3.0 و TLS 1.0).

Full Disk Encryption (FDE): تشفير كل القطاعات على القرص بما في ذلك نظام التشغيل والملفات المؤقتة.

File-Level Encryption: تشفير ملفات محددة فقط (مثل EFS في Windows).

مثال: إدارة BitLocker باستخدام manage-bde

```
manage-bde -status C:
manage-bde -on C: -RecoveryPassword -RecoveryKey D:\
```

يشرح الأمر كالتالي:

`manage-bde -status C:` : يعرض حالة تشفير القرص C.

`-on C:` : تشغيل التشفير على القرص C.

`-RecoveryPassword` : إنشاء كلمة استرداد.

`-RecoveryKey D:\` : حفظ مفتاح الاسترداد على القرص D.

مثال: cipher /w لمسح المساحة الفارغة

```
cipher /w:C:\
```

`cipher /w:C:\` : يكتب بيانات عشوائية فوق المساحة الفارغة للقرص C لضمان عدم استرجاع الملفات المحذوفة.

مثال: استخدام shred في Linux

```
shred -v -n 3 -z secrets.txt
```

يشرح الأمر كالتالي:

`shred` : أداة تمزيق الملفات.

`-v` : يعرض التقدم.

`-n 3` : يكتب بيانات عشوائية 3 مرات.

`-z` : يكتب أصفارًا في النهاية لإخفاء التمزيق.

`secrets.txt` : الملف المراد إتلافه.

مثال: تشفير باستخدام GPG

```
gpg --symmetric --cipher-algo AES256 secret.docx
gpg --output secret.docx --decrypt secret.docx.gpg
```

يشرح الأمر كالتالي:

`gpg --symmetric` : تشفير بمفتاح سري واحد (Symmetric).

`--cipher-algo AES256` : استخدام خوارزمية AES-256.

`--decrypt` : فك التشفير.

`--output secure.docx` : اسم الملف الناتج.

(Quick Quiz (MCQ

1. Which data classification level represents the most sensitive data requiring the highest level of protection?
   a) Public
   b) Internal
   c) Confidential
   d) Restricted

   Answer: d

2. What is the final stage of the data lifecycle?
   a) Archive
   b) Store
   c) Share
   d) Destroy

   Answer: d

3. What does DLP (Data Loss Prevention) do?
   a) Encrypts all network traffic
   b) Monitors and prevents unauthorized transfer of sensitive data
   c) Manages firewall rules
   d) Blocks malware installation

   Answer: b

.4 What is BitLocker?

a) A network encryption protocol

b) A full disk encryption feature for Windows operating systems

c) A firewall application

d) A backup utility

Answer: b

.5 What does the shred -n 3 command do to a file?

a) Deletes the file 3 times

b) Overwrites the file data 3 times before deletion to prevent recovery

c) Compresses the file into 3 parts

d) Creates 3 backup copies

Answer: b