ملخص مقدمة إلى أساسيات الأمن السيبراني

إعداد: إسماعيل محمد قطان

التاريخ: أكتوبر/ تشرين الأول 2025

|  |  |  |
| --- | --- | --- |



### **السرية والنزاهة والتوافر(**Confidentiality, Integrity, and Availability**)**

كل نظام أمني جيد مبني على ثلاث أفكار رئيسية - تُسمى ثالوث CIA:

#### 1- السرية (Confidentiality)

تعني الحفاظ على سرية البيانات - فقط الأشخاص المناسبين يمكنهم رؤيتها.

لماذا هي مهمة:

* تحمي من سرقة الهوية، اختراق الحسابات، المشاكل القانونية، و الإضرار بالسمعة.

كيفية حماية السرية:

* استخدام كلمات المرور والتحكم في الوصول (المستخدمين المصرح لهم فقط).
* استخدام التشفير لحماية البيانات المخزنة أو المشتركة.
* استخدام المصادقة متعددة العوامل (MFA) للحماية الإضافية.

اسأل نفسك:

* من المسموح له برؤية هذه البيانات؟
* ماذا يحدث إذا تم تسريبها؟
* هل يوجد أي قانون (مثل GDPR أو HIPAA) يحمي هذه البيانات؟

#### 2- النزاهة (Integrity)

تعني الحفاظ على البيانات صحيحة وغير متغيرة - لا يجب أن يتمكن أحد من تعديلها بدون إذن.

لماذا هي مهمة:

* البيانات الخاطئة أو المتغيرة يمكن أن تسبب أخطاء خطيرة (في السجلات الصحية، المالية، التصويت، إلخ).

نوعان من النزاهة:

* النزاهة المادية: تحمي الأجهزة التي تخزن البيانات.
* النزاهة المنطقية: تحمي البيانات من المتسللين والأخطاء البشرية.

الأدوات المستخدمة:

* مراقبة نزاهة الملفات (FIM) : تتحقق من تغيير الملفات المهمة. (File integrity monitoring)
* أنظمة إدارة قواعد البيانات العلائقية (RDBMS): تسجل من قام بتغيير أو الوصول إلى البيانات.

Relational Database Management System

كيفية الحفاظ على دقة البيانات:

* حظر الوصول غير المصرح به.
* منع التغييرات غير المصرح بها (حتى من قبل الموظفين الداخليين).
* استخدام فحوصات الأخطاء والتحقق من صحة البيانات.

#### 3- التوافر (Availability)

تعني التأكد من أن البيانات جاهزة دائماً للمستخدمين المصرح لهم.

التهديدات للتوافر:

* غير ضارة: مشاكل الأجهزة، مشاكل الشبكة، أو أعطال النظام.
* ضارة: هجمات مثل رفض الخدمة (DoS) - المتسللون يغمرون موقعاً أو خادماً لجعله غير متصل.

كيفية حماية التوافر:

* استخدام خوادم احتياطية وأنظمة زائدة.
* إجراء مراقبة الشبكة للكشف عن المشاكل مبكراً.
* استهداف وقت تشغيل عالٍ (99.999%) حتى يكون للمستخدمين دائماً إمكانية الوصول.
* إنشاء خطة استمرارية الأعمال للطوارئ.

#### قوانين حماية البيانات

* **HIPAA (الولايات المتحدة):** يحمي المعلومات الصحية.
* **GDPR (الاتحاد الأوروبي):** يحمي خصوصية البيانات الرقمية والشخصية.
* **إذا انتهكت الشركات هذه القواعد:** تواجه غرامات وعقوبات كبيرة.

### الأمن وخصوصية المعلومات (Security and Information Privacy)

#### الأصول المعلوماتية (Information Assets)

**أصل معلوماتي:** أي بيانات أو معلومات لها قيمة لشخص أو مؤسسة.

* **أمثلة:** سجلات المرضى، تفاصيل العملاء، الملكية الفكرية.
* المعلومات يمكن أن تكون مادية (ورق، أقراص) أو إلكترونية (قواعد بيانات، ملفات).

#### من البيانات إلى المعلومات

* **البيانات (Data):** حقائق أو أرقام خام - مثل مشاهدات الصفحة، المبيعات، النقرات.
* **المعلومات (Information) :** بيانات منظمة - تظهر النتائج أو الأنماط.
* **الرؤى (Insights) :** استنتاجات من تحليل المعلومات - تُستخدم لقرارات الأعمال.

**مثال:** إذا زادت المبيعات بعد تغيير ساعات المتجر → الرؤية = الساعات الجديدة فعالة.

#### الملكية الفكرية (Intellectual Property (IP))

* **التعريف:** إبداعات العقل - أفكار أو اختراعات تخص شخصاً ما.

أمثلة:

* التصاميم الصناعية
* الأسرار التجارية
* اكتشافات البحث
* معرفة الموظفين

طرق الحماية:

* قوانين حقوق النشر والعلامات التجارية وبراءات الاختراع
* اتفاقيات عدم الإفصاح (NDAs): تمنع الموظفين من مشاركة الأسرار.

#### 

#### الأصول الرقمية والحماية (Digital Assets and Protection)

* **المنتجات الرقمية:** ممتلكات الشركة غير المادية مثل: البرمجيات، الدورات عبر الإنترنت، الكتب الإلكترونية، الموسيقى، القوالب، إلخ.

**التهديدات:** القرصنة، الاختراق، الهندسة العكسية.

أدوات الحماية:

* إدارة الحقوق الرقمية (DRM Digital Rights Management): تمنع نسخ أو مشاركة الملفات.
* قانون الألفية الرقمية لحقوق النشر (DMCA Digital Millennium Copyright Act): قانون أمريكي يجعل كسر حماية DRM غير قانوني.

#### القرارات المبنية على البيانات (Data-Driven Decisions)

* الشركات تجمع وتحلل البيانات لاتخاذ قرارات أذكى.
* **التقاط البيانات:** جمع البيانات من مصادر متعددة (سجلات الخادم، أجهزة إنترنت الأشياء، الاستبيانات).
* **ارتباط البيانات:** إيجاد روابط أو أنماط (مثل Netflix تتنبأ بنجاح العروض).
* **أدوات الإبلاغ:** تحول البيانات المحللة إلى رسوم بيانية وجداول ولوحات معلومات للحصول على رؤى.

#### المعلومات السرية (Confidential Information)

معلومات يجب أن تبقى خاصة ويمكن الوصول إليها فقط للأشخاص المصرح لهم.

الأنواع الرئيسية للمعلومات السرية:

* معلومات التعريف الشخصية ( Personally Identifiable Information PII):
  + تحدد هوية الشخص.
  + أمثلة: الاسم، رقم الهوية، تاريخ الميلاد، العنوان، الهاتف.
* معلومات الشركة السرية:
  + بيانات الأعمال الداخلية.
  + أمثلة: تصاميم المنتجات، الإجراءات، سجلات الموظفين، المعلومات المالية.
* معلومات العملاء السرية:
  + بيانات يقدمها العملاء أو الشركاء.
  + تشمل PII + سجل الشراء، معلومات بطاقة الائتمان، إلخ.
* معلومات الصحة المحمية (PHI):
  + بيانات طبية مرتبطة بهوية الشخص (مثل التاريخ الطبي، الوصفات، الصور).

#### أمثلة على التعامل المهمل مع البيانات

* حفظ معلومات بطاقة الائتمان في قاعدة بيانات غير مشفرة.
* ترك ملفات المرضى في مكان عام.
* مشاركة كلمات المرور مع زملاء العمل.

#### كيفية التعامل بأمان مع البيانات السرية

* إعطاء حق الوصول فقط لمن يحتاجه.
* تشفير البيانات المخزنة أو المرسلة.
* استخدام جدران الحماية والأذونات.
* تدمير النسخ القديمة أو غير المستخدمة بشكل آمن.
* الحصول على الموافقة قبل جمع أو تخزين البيانات الشخصية.
* إخبار المستخدمين بمدة تخزين البيانات.
* استخدام كلمات مرور قوية، عدم مشاركتها أو كتابتها.
* تغيير كلمات المرور بانتظام (مثلاً كل 3 أشهر).

#### الفرق بين PII و PCI و SPI

| النوع | المعنى | مثال |
| --- | --- | --- |
| **PII** | معلومات التعريف الشخصية - تحدد هوية الشخص | الاسم، الهوية، العنوان |
| **PCI** | معلومات العميل الشخصية - تصف العميل | المعلومات الديموغرافية، تسجيل الدخول، الاتصال |
| **SPI** | معلومات شخصية حساسة - قد تسبب ضرراً إذا نُشرت | الراتب، المعتقدات السياسية، البيومترية |

### 

### التهديدات والاختراقات (Threats and Breaches)

#### 1. التهديدات المادية (Physical Threats)

* التهديدات المادية تستهدف الأجهزة (الحواسيب، الخوادم، إلخ) بدلاً من الأنظمة الرقمية.
* **أمثلة:** السرقة، التلاعب، انقطاع التيار الكهربائي، الحرائق، الفيضانات، الزلازل، الرطوبة، أو العفن.

طرق الحماية:

* قفل الأجهزة في غرف آمنة.
* استخدام قارئات البطاقات وكاميرات المراقبة.
* صيانة أنظمة إخماد الحرائق، الطاقة الاحتياطية، وأنظمة التدفئة والتهوية وتكييف الهواء.
* إنشاء واختبار خطط التعافي من الكوارث.

#### 2. تهديدات البيانات (Data Threats)

أنواع مشاكل البيانات:

* **تسريب البيانات:** تعرض عرضي للبيانات الحساسة.
* **اختراق البيانات:** سرقة متعمدة أو هجوم من قبل مجرمي الإنترنت.
* **تفريغ البيانات:** بيانات مسروقة تُباع أو تُشارك (غالباً على الويب المظلم) - تشمل PII، PHI، تفاصيل البنك، إلخ.
* **الغوص في القمامة:** البحث المادي في القمامة عن معلومات حساسة (أوراق، كلمات مرور، خطط).

**الحل:** تمزيق المستندات وتدمير الأجهزة القديمة بشكل صحيح.

#### 3. التهديدات الداخلية (Insider Threats)

* تأتي من داخل المؤسسة - عادة الموظفين أو المقاولين.
* يمكن أن تكون متعمدة (بيع المعلومات أو تخريب الأنظمة) أو عرضية (الإهمال).
* أحياناً يجند المتسللون أشخاصاً من الداخل عبر الرشوة أو الابتزاز.

#### 4. تهديدات البرمجيات (Software Threats)

الفئات الرئيسية:

1. **سرقة البرمجيات/الترخيص:** استخدام أو نسخ البرمجيات المدفوعة بشكل غير قانوني (القرصنة).
2. **الاستغلالات:** كود يستفيد من نقاط ضعف البرمجيات.
   * مثال: "التنزيلات العابرة" من مواقع مصابة.
3. **البرمجيات الخبيثة:** أي برمجية خبيثة تضر الأنظمة أو تسرق البيانات.

#### 5. البرمجيات الخبيثة (Malware)

**الأعراض الشائعة:** نظام بطيء، نوافذ منبثقة، سلوك غريب، سرقة البيانات، تسجيل كاميرا الويب/الميكروفون.

المصادر:

* مرفقات البريد الإلكتروني، روابط مزيفة، التورنت، أجهزة USB، ورسائل وسائل التواصل الاجتماعي.

نصائح الحماية:

* حافظ على تحديث البرامج.
* تجنب الروابط والمرفقات المشبوهة.
* استخدم أدوات مكافحة الفيروسات.
* احتفظ بنسخة احتياطية من البيانات بانتظام.
* استخدم كلمات مرور قوية وغيّرها بشكل متكرر.

#### 6. أنواع البرمجيات الخبيثة

| النوع | الوصف | مثال/تفاصيل |
| --- | --- | --- |
| **الفيروس** | يحتاج إلى مستخدم لفتح ملف/تطبيق للانتشار | يمكنه سرقة البيانات، تسجيل النشاط، إتلاف الملفات |
| **فيروس البرنامج** | يدخل نفسه في برنامج آخر | يصيب البرامج القابلة للتنفيذ |
| **فيروس الماكرو** | يستهدف ملفات Office (ماكرو Word، Excel) | ينشط عند فتح المستندات |
| **الفيروس الخفي** | يختبئ بنسخ نفسه في مكان آخر | يتجنب فحوصات مكافحة الفيروسات |
| **الفيروس متعدد الأشكال** | يغير كوده باستمرار لتجنب الكشف | يشكل 97% من جميع البرمجيات الخبيثة |
| **الدودة** | فيروس ينتشر ذاتياً - لا يحتاج إلى إجراء من المستخدم | يستغل نقاط ضعف النظام |
| **حصان طروادة** | يبدو شرعياً لكنه يثبت برمجيات خبيثة مخفية | مثال: تطبيق مكافحة فيروسات مزيف |
| **برامج التجسس** | تجمع البيانات الشخصية وبطاقات الائتمان وكلمات المرور سراً | يمكن استخدام الكاميرا/الميكروفون للتجسس |
| **برامج الإعلانات** | تتبعك لإعلانات مستهدفة - يمكن أن تكون غير ضارة أو خبيثة | غالباً ما تأتي مع تطبيقات مجانية |
| **برامج الفدية** | تقفل/تشفر الملفات حتى يتم دفع الفدية | يمكن استعادة الملفات من النسخة الاحتياطية |

#### 

| **type** | **Description** | **Example/Details** |
| --- | --- | --- |
| *Virus* | Needs a user to open a file/app to spread. | Can steal data, record activity, corrupt files. |
| *Program Virus* | Inserts itself into another program. | Infects executable software. |
| *Macro Virus* | Targets Office files (Word, Excel macros). | Activates when documents open. |
| *Stealth Virus* | Hides by copying itself elsewhere. | Avoids antivirus scans. |
| *Polymorphic Virus* | Constantly changes code to avoid detection. | Makes up 97% of all malware. |
| *Worm* | Self-spreading virus — no user action needed. | Exploits system weaknesses. |
| *Trojan* | Looks legitimate but installs hidden malware. | Example: Fake antivirus app. |
| *Spyware* | Secretly collects personal data, credit cards, passwords. | Can use camera/mic to spy. |
| *Adware* | Tracks you for targeted ads — can be harmless or malicious. | Often bundled with free apps. |
| *Ransomware* | Locks/encrypts files until ransom is paid. | Can restore files from backup. |

#### 7. ناقلات الهجوم (كيفية انتشار البرمجيات الخبيثة)

* **التصيد الاحتيالي:** خداع المستخدمين للكشف عن بيانات الاعتماد أو النقر على روابط سيئة.
* **هجمات Remote Desktop Protocol RDP:** المتسللون يستغلون الوصول عن بُعد إلى سطح المكتب.
* كلاهما طرق شائعة لهجمات برامج الفدية.

### 

### أنواع التهديدات (Threat Types)

#### 1. هجمات التجسس (Snooping Attacks)

المتسللون يعترضون البيانات بين الأجهزة لسرقة معلومات مثل تسجيلات الدخول، أرقام بطاقات الائتمان، أو الملفات.

الأنواع الشائعة:

* التنصت (استنشاق الحزم) \ Eavesdropping (Packet Sniffing) :  
  + يستخدم أدوات تسمى "مستنشقات الحزم" لالتقاط البيانات المرسلة عبر الشبكة.
  + يعمل بسهولة على الشبكات غير المشفرة (العامة).
  + **الوقاية:** استخدم اتصالات مشفرة (VPN، HTTPS، أو بيانات الهاتف المحمول بدلاً من Wi-Fi العام).
* الرجل في المنتصف (MITM أو هجوم على المسار) Man-In-The-Middle:  
  + المهاجم يعترض سراً الاتصال بين الضحية والخادم.
  + MITM المادي: المهاجم بالقرب منك على Wi-Fi عام.
  + MITM المنطقي: المهاجم يرسل روابط أو رسائل بريد إلكتروني مزيفة لخداع المستخدمين (التصيد).
  + أشكال أخرى: الانتحال، الاختطاف، وسرقة ملفات تعريف الارتباط.
  + **الوقاية:** استخدم HTTPS، VPN، وتجنب الروابط المشبوهة.
* هجوم إعادة التشغيل (Replay Attack):  
  + المهاجم يلتقط ويعيد استخدام "رموز الوصول" من الكيانات الموثوقة (مثل تسجيل دخول البنك).
  + يعيدون تشغيل هذه البيانات لانتحال شخصية المستخدم والحصول على الوصول.
  + **الوقاية:** استخدم التشفير، الرموز محدودة الوقت، والمصادقة متعددة العوامل.

#### 2. البرمجة النصية عبر المواقع (Cross-Site Scripting - XSS)

المتسللون يضيفون كوداً خبيثاً (عادة JavaScript) إلى مواقع موثوقة.

الأنواع:

* **XSS المنعكس Reflected:** كود خبيث مخفي في رابط URL. عند النقر، يعمل ويسرق البيانات.
* **XSS المستمر Persistent:** الكود يُحفظ على الموقع (مثل التعليقات أو المنتديات) ويؤثر على كل زائر.

الوقاية:

* التحقق من صحة وتنظيف مدخلات المستخدم.
* تعيين قواعد ملفات تعريف الارتباط وحظر وصول JavaScript.
* استخدام جدار حماية تطبيقات الويب (WAF).

#### 3. حقن SQL أو SQL Injection

المهاجمون يستخدمون أوامر SQL خبيثة للوصول إلى قاعدة بيانات الموقع أو تعديلها. يمكنهم تجاوز نماذج تسجيل الدخول أو حذف البيانات.

الوقاية:

* معاملة الاستعلامات (أوامر محددة مسبقاً وآمنة).
* استخدام الإجراءات المخزنة.
* تطبيق القوائم البيضاء (قبول المدخلات الصحيحة فقط).
* إخفاء مدخلات المستخدم حتى لا تُقرأ كشفرة.

#### 4. الشبكات الروبوتية (Botnets)

الشبكة الروبوتية هي شبكة من أجهزة الكمبيوتر المصابة (تسمى الزومبي) تُسيطر عليها المتسللون. تُستخدم لـ:

* هجمات إلكترونية واسعة النطاق (مثل DDoS).
* تعدين العملات المشفرة (باستخدام معالج الكمبيوتر الخاص بك).

**الوقاية:** حافظ على تحديث الأنظمة، استخدم مكافحة الفيروسات، وتجنب التنزيلات المشبوهة.

#### 5. رفض الخدمة (DoS) ورفض الخدمة الموزع (DDoS) أو Denial of Service (DoS) and Distributed DoS (DDoS)

هذه الهجمات تغمر الشبكة أو الموقع بحركة المرور حتى ينهار.

أنواع هجمات DoS:

* تجاوز المخزن المؤقت: حركة مرور كثيرة جداً لا يستطيع الموقع التعامل معها.
* فيضان ICMP: إشارات شبكة لا نهائية تسبب زيادة الحمل على النظام.
* فيضان SYN: طلبات اتصال غير مكتملة تعطل الخادم.

**DDoS = DoS + شبكة روبوتية:** تُستخدم آلاف الحواسيب، مما يجعله أكثر قوة وأصعب في التتبع.

**الوقاية:** استخدم جدران الحماية، تحديد المعدل، وخدمات الحماية من DDoS.

| نوع الهجوم | الهدف | الوقاية |
| --- | --- | --- |
| **التجسس** | اعتراض وسرقة البيانات | استخدم VPN، التشفير |
| **MITM** | التجسس أو تغيير الاتصال | تجنب الروابط المزيفة، استخدم HTTPS |
| **إعادة التشغيل** | انتحال شخصية المستخدم | استخدم رموز محدودة الوقت |
| **XSS** | حقن كود ويب خبيث | التحقق من المدخلات، استخدم WAF |
| **حقن SQL** | الوصول إلى قواعد البيانات أو تدميرها | معاملة الاستعلامات |
| **الشبكات الروبوتية** | التحكم في العديد من الحواسيب | استخدم مكافحة الفيروسات |
| **DoS/DDoS** | إسقاط الأنظمة بحركة المرور | استخدم أدوات الحماية من DDoS |

### 

### التصيد الاحتيالي والهندسة الاجتماعية والهجمات الأخرى Phishing, Social Engineering, and Other Attacks

**الانتحال** يحدث عندما **يتظاهر شخص ما بأنه شخص أو شيء آخر** لسرقة المعلومات.

**الهندسة الاجتماعية** هي عندما يخدع المهاجمون **الناس باستخدام علم النفس** بدلاً من اختراق التكنولوجيا - يستخدمون الخوف أو الاستعجال أو الثقة للتلاعب بالضحايا.

في الواقع، حوالي 90% من جميع الهجمات الإلكترونية تشمل الهندسة الاجتماعية بطريقة ما.

#### 1. أنواع هجمات الانتحال Types of Impersonation Attacks

1. Wi-Fi التوأم الشرير Evil Twin Wi-Fi:
   * Wi-Fi عام مزيف يبدو حقيقياً.
   * بمجرد الاتصال، يمكن للمتسللين التقاط تسجيلات الدخول والبيانات الخاصة بك.
2. المواقع المزيفة:
   * تبدو متطابقة مع المواقع الحقيقية (مثل موقع البنك الخاص بك).
   * مصممة لسرقة أسماء المستخدمين وكلمات المرور أو معلومات بطاقة الائتمان.
3. التظاهر بأنك شخص آخر:
   * قد يتصرف المتسللون مثل زميلك في العمل أو موظف بنك أو حتى مديرك.
   * هدفهم هو خداعك للكشف عن بيانات حساسة.

#### 2. تقنيات الهندسة الاجتماعية الشائعة Common Social Engineering Techniques

1. التجسس من فوق الكتف Shoulder Surfing
   * مشاهدة شاشتك أو لوحة المفاتيح في الأماكن العامة (المقاهي، المطارات).
   * يمكن للمتسللين رؤية أرقام PIN أو كلمات المرور أو تثبيت برامج خبيثة إذا تركت جهازك وحده.

**كن آمناً:** تجنب Wi-Fi العام، لا تترك الأجهزة دون رقابة أبداً، واستخدم فلاتر الخصوصية.

1. الطُعم Baiting
   * المهاجمون يستخدمون إغراءً لجعل الضحايا يصيبون أنفسهم.
   * طُعم مادي: محرك USB يُترك في مكان عام.
   * طُعم رقمي: إعلانات مزيفة أو تنزيلات "مجانية".
   * **كن آمناً:** لا تدخل أجهزة غير معروفة أو تنقر على روابط مشبوهة.
2. الذرائع Pretexting
   * المهاجم يتظاهر بأن لديه سلطة (مثل دعم تقنية المعلومات أو مدير البنك).
   * يستخدمون الخوف أو الضغط لجعلك تشارك المعلومات.
   * مثال: "سيتم قفل حسابك ما لم تعطني كلمة مرورك."

4. التصيد الاحتيالي Phishing

* + رسائل بريد إلكتروني أو نصية مزيفة تخلق الذعر أو الاستعجال.
  + الهدف هو جعلك تنقر على رابط مزيف أو تنزيل برامج خبيثة.
  + مثال: "حسابك مخترق. انقر هنا لإعادة تعيين كلمة مرورك."

الأنواع الرئيسية:

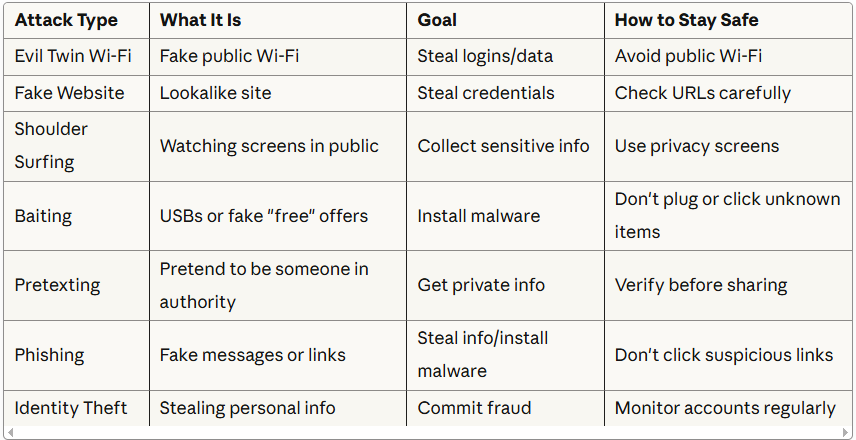
* التصيد الاحتيالي الموجه: يستهدف شخصاً محدداً.
* صيد الحيتان: يستهدف المسؤولين التنفيذيين أو كبار الموظفين.
* التصيد الصوتي: التصيد الصوتي (مكالمات هاتفية احتيالية).

#### 3. سرقة الهوية والاحتيال Identity Theft and Fraud

* **سرقة الهوية:** سرقة معلومات شخص ما الخاصة أو المالية.
* **احتيال الهوية:** استخدام المعلومات المسروقة لارتكاب جرائم (فتح حسابات، قروض، إلخ).

احمِ نفسك:

* استخدم كلمات مرور قوية وفريدة.
* حافظ على خصوصية البيانات الشخصية.
* راقب نشاط البنك والائتمان بانتظام.



### تقنيات إدارة كلمات المرور Password Management Techniques

#### 1. ما هو كسر كلمات المرور؟ What Is Password Cracking

كسر كلمات المرور يعني محاولة الحصول على كلمة المرور الصحيحة دون إذن.

الطرق الشائعة تشمل:

* **هجوم القوة الغاشمة Brute Force:** يجرب كل كلمة مرور ممكنة حتى تنجح واحدة.
* **هجوم القاموس Dictionary:** يستخدم كلمات حقيقية من القواميس أو الكتب.
* **هجوم قوس قزح Rainbow:** يستخدم تجزئات كلمات مرور محسوبة مسبقاً لتخمين كلمات مرور أخرى.

التجزئة Hashing:

* تحول كلمة المرور إلى رمز ثابت الطول (يسمى تجزئة) باستخدام خوارزمية.
* التجزئات تحمي كلمات المرور، لكن إذا تم كسر تجزئة واحدة، فقد يتم أيضاً كشف أخرى تم إنشاؤها بنفس الطريقة.

#### 2. لماذا كلمات المرور القوية مهمة

* كلمات المرور الضعيفة أو المسروقة تسبب أكثر من 80% من اختراقات بيانات الشركات.
* كثير من الناس يعيدون استخدام كلمات المرور عبر الحسابات الشخصية وحسابات العمل - خطر كبير.
* يجب أن يكون لكل حساب كلمة مرور فريدة وقوية.
* يجب على الشركات تدريب الموظفين على سلامة كلمات المرور والهجمات.

#### 3. أفضل ممارسات سياسة كلمات المرور

سياسة كلمات المرور تضع قواعد لإنشاء وإدارة كلمات المرور.

السياسات الجيدة تشمل:

* حد أدنى 12 حرفاً.
* مزيج من الأحرف الكبيرة والصغيرة والأرقام والأحرف الخاصة.
* كلمة مرور فريدة لكل حساب أو جهاز.
* تغيير كلمات المرور كل 6-12 شهراً.
* تدريب الموظفين حول التهديدات الإلكترونية.
* تذكير الموظفين: الشركة لن تطلب كلمة مرورك أبداً.

يجب على الموظفين أيضاً:

* عدم إعادة استخدام أو مشاركة كلمات المرور أبداً (حتى مع الرئيس التنفيذي أو تقنية المعلومات).
* عدم كتابة كلمات المرور أو تخزينها في ملف أبداً.
* تجنب كلمات المرور البسيطة والقابلة للتخمين.

#### 4. إعادة استخدام كلمة المرور وانتهاء الصلاحية

إعادة استخدام كلمة المرور:

* استخدام نفس كلمة المرور (أو كلمات مرور مشابهة) لحسابات متعددة.
* يسهل على المتسللين اقتحام جميع حساباتك بمجرد كشف واحدة.

انتهاء صلاحية كلمة المرور:

* تغيير كلمات المرور في كثير من الأحيان (مثل كل 90 يوماً) يمكن أن يؤدي إلى خيارات ضعيفة.
* من الأفضل استخدام كلمات مرور طويلة وقوية وفريدة وتغييرها فقط عند وجود سبب (مثل اختراق أو خطر).

### 

### المصادقة وتسجيل الدخول الموحد Authentication and SSO

#### 1. ما هي المصادقة؟

المصادقة تعني إثبات هويتك قبل الحصول على الوصول إلى نظام أو مورد.

تستخدم عوامل - معلومات تعرفها أنت (والنظام) فقط أو تمتلكها.

#### 2. المصادقة أحادية العامل (Single-Factor Authentication)

* **التعريف:** تسجيل الدخول بمعلومة واحدة فقط (عادة اسم المستخدم + كلمة المرور).
* نقاط الضعف:
  + سهلة السرقة من خلال التصيد الاحتيالي (phishing) أو مسجلات ضربات المفاتيح (keystroke loggers) (برامج خبيثة تسجل ما تكتبه).
  + إذا تم تسريب بيانات اعتمادك على الويب المظلم، يمكن للمهاجمين الوصول بالكامل إلى بياناتك.
* **مثال:** تسجيل الدخول إلى البريد الإلكتروني بكلمة مرور فقط.

#### 3. المصادقة ثنائية العامل (Two-Factor Authentication)

* **التعريف:** تتطلب بيانتي اعتماد - عادة شيء تعرفه وشيء تملكه.
* **الشكل الشائع:** مفتاح أمان (أجهزة) يُدخل في منفذ USB أو يستخدم NFC.
* الفوائد:
  + يحمي من التصيد الاحتيالي والاختطاف.
  + سهل الإعداد جداً.
* **مثال:** تسجيل الدخول بكلمة مرور + مفتاح أمان USB أو رمز يُرسل إلى هاتفك.

#### 4. المصادقة متعددة العوامل (Multi-Factor Authentication)

* **التعريف:** تستخدم عاملين أو أكثر للتحقق من هويتك.
* توفر حماية إضافية:
  + تقلل بشكل كبير من خطر الاختراق.
  + لا يمكن التقاطها بواسطة مسجلات المفاتيح.
  + تتيح لك اختيار كيفية التحقق (نص، تطبيق، بريد إلكتروني، بيومتري، إلخ).
* **ملاحظة:** MFA ليست مضمونة 100% - المتسللون لا يزالون يبحثون عن نقاط الضعف.
* **مثال:** كلمة مرور + بصمة الإصبع + OTP (كلمة مرور لمرة واحدة).

#### 

#### 5. تسجيل الدخول الموحد (Single Sign-On)

* **التعريف:** يتيح للمستخدمين تسجيل الدخول مرة واحدة للوصول إلى تطبيقات متصلة متعددة.
* **يستخدم من قبل:** الشركات ذات الأنظمة مثل Office 365 أو Salesforce.
* الفوائد:
  + وصول أسرع وأسهل للموظفين.
  + يقلل من إرهاق كلمة المرور (لا حاجة لتذكر العديد من تسجيلات الدخول).

| الطريقة | عدد العوامل | مثال | مستوى الأمان |
| --- | --- | --- | --- |
| **SFA** | 1 | اسم المستخدم + كلمة المرور | 🔴 ضعيف |
| **2FA** | 2 | كلمة المرور + مفتاح USB | 🟡 قوي |
| **MFA** | 2 أو أكثر | كلمة المرور + بصمة الإصبع + OTP | 🟢 قوي جداً |
| **SSO** | تسجيل دخول واحد لتطبيقات متعددة | تسجيل الدخول مرة واحدة → الوصول إلى جميع الأدوات | 🟡 مريح لكن يعتمد على MFA |

### 

### التحكم في الوصول والتفويض والمصادقة Access Control, Authorization, and Authentication

#### 1. عمليات الأمان الرئيسية Key Security Processes

هناك ثلاث عمليات أمان أساسية تُستخدم لحماية الوصول إلى الأنظمة والبيانات:

أ. التحكم في الوصول **Access Control**

* **التعريف:** آلية تحدد من يمكنه الوصول إلى الموارد أو البيانات أو الأنظمة.
* **الغرض:** يمنع المستخدمين غير المصرح لهم من عرض أو تعديل أو نسخ البيانات.
* يتم تنفيذه من قبل مسؤولي تقنية المعلومات لإدارة:
  + أي المستخدمين لديهم وصول.
  + ما هي الإجراءات التي يمكنهم القيام بها.
  + أي الموارد يمكنهم استخدامها.
* مبدأ الامتياز الأقل (PoLP):
  + كل مستخدم يحصل على الحد الأدنى من الأذونات اللازمة لأداء وظيفته.
* التحكم في الوصول القائم على الأدوار (Role Based Access Control RBAC):
  + يتم تعيين الوصول بناءً على الأدوار التنظيمية (الأقسام، المسميات الوظيفية، إلخ).
  + يتم تجميع المستخدمين وفقاً لأدوارهم.
  + لكل دور أذونات محددة.
  + يبسط الانضمام - يرث المستخدمون الجدد الأذونات بناءً على الدور.

ب. التفويض **Authorization**

* **التعريف:** عملية منح إذن للوصول إلى الأنظمة أو أداء إجراءات.
* تأتي بعد إعداد التحكم في الوصول.
* تضمن أن المستخدمين الذين لديهم الامتيازات الصحيحة فقط يمكنهم الدخول أو التصرف داخل نظام.
* **مثال:** قد يكون المستخدم مفوضاً للوصول إلى البريد الإلكتروني ولكن ليس خوادم قاعدة البيانات.
* العلاقة مع التحكم في الوصول:
  + التحكم في الوصول يحدد من يمكنه الحصول على الوصول.
  + التفويض يمنح أذونات محددة ضمن هذا الوصول.

ج. المصادقة **Authentication**

* **التعريف:** التحقق من هوية المستخدم قبل منح الوصول.
* يؤكد أن الشخص الذي يسجل الدخول هو حقاً من يدعي أنه.
* العملية تتضمن:
  1. إدخال بيانات الاعتماد (اسم المستخدم، كلمة المرور).
  2. التحقق من صحة تلك المعلومات مع النظام.

#### 2. عوامل المصادقة Authentication Factors

تعتمد المصادقة على واحد أو أكثر من العوامل التالية:

* **شيء تعرفه** - كلمة المرور، رقم التعريف الشخصي، أو سؤال الأمان.
* **شيء تملكه** - هاتف، مفتاح أمان، بطاقة، أو بطاقة ذكية.
* **شيء أنت** - القياسات الحيوية مثل بصمة الإصبع، الوجه، قزحية العين، أو الصوت.
* **(عامل إضافي اختياري) مكان تواجدك** - الموقع الجغرافي أو موقع الشبكة (القائم على IP/الموقع الجغرافي).

#### 3. المحاسبة الرقمية (التدقيق والمراقبة) Digital Accounting (Audit & Monitoring)

تُستخدم للتحليل الأمني، الطب الشرعي (forensics)، واستكشاف الأخطاء وإصلاحها - تساعد في اكتشاف النشاط المشبوه.

المكونات الرئيسية:

* **السجلات:** تسجيلات لمن وصل إلى ماذا، ومتى، ومن أين في النظام.
* **التتبع:** يجمع بيانات الجهاز والمتصفح (نظام التشغيل، اللغة، الامتدادات) لتحديد المستخدمين واكتشاف الأنماط غير العادية.
* **ملفات تعريف الارتباط:** ملفات صغيرة تخزن جلسات تسجيل الدخول والتفضيلات، مما يتيح الوصول الشخصي وتتبع النشاط.
* **سجل التصفح:** قائمة بالمواقع التي تمت زيارتها بمرور الوقت، تكشف عن اهتمامات المستخدم وسلوكه عبر الإنترنت.

#### 4. عدم الإنكار Non-Repudiation

يضمن أن الإجراءات أو الاتصالات لا يمكن إنكارها أو الطعن فيها لاحقاً.

يثبت أن فرداً معيناً قام بإجراء أو أرسل بيانات.

أربع طرق رئيسية:

1. **أدلة الفيديو:** الكاميرات تلتقط دليلاً على الوصول (سجلات الدخول/الخروج).
2. **القياسات الحيوية:** تؤكد هوية المستخدم من خلال السمات الجسدية (بصمة الإصبع، قزحية العين، إلخ).
3. **التوقيع:** عندما يقترن برمز الأجهزة، يصبح توقيعاً رقمياً.
   * يُستخدم لمصادقة الموقع وتأكيد سلامة الرسالة.
4. **الإيصالات:** إقرارات رقمية تظهر أن رسالة أو معاملة تم إرسالها واستلامها.

### تقوية الأجهزة

**التقوية:** عملية تأمين جهاز لتقليل نقاط الضعف.

#### طرق التقوية الرئيسية

* تعطيل ميزات الجهاز غير المطلوبة
* تحديث البرامج الثابتة للجهاز ونظام التشغيل والبرامج بانتظام
* استخدام جدران الحماية وVPN ومكافحة البرامج الخبيثة
* تمكين التحديثات التلقائية لجميع الأجهزة

#### البرامج الثابتة الأمنية Security Firmware

| المصطلح | التعريف |
| --- | --- |
| **البرامج الثابتة Firmware** | البرمجيات التي تخبر الأجهزة كيف تتصرف |
| **كلمة مرور BIOS** | نظام الإدخال والإخراج الأساسي basic input/output system - يقوم بتشغيل Windows/Linux، يجري فحوصات الأجهزة، يبدأ نظام التشغيل بحماية كلمة المرور |
| **التمهيد الآمن**  **Secure Boot** | ميزة UEFI تؤكد التوقيع الرقمي لمصنع نظام التشغيل لمنع البرامج الخبيثة أثناء التمهيد |
| **TPM** | وحدة النظام الأساسي الموثوقة Trusted Platform Module - شريحة تخزن وتدير مفاتيح التشفير، تكتشف التلاعب |
| **تشفير القرص** | يشوش بيانات القرص لجعلها غير قابلة للقراءة بدون مفتاح التشفير |

#### التشفير

* يستخدم خوارزميات لترميز النص العادي إلى نص مشفر غير قابل للقراءة
* فقط مفتاح التشفير يمكنه فك تشفيره
* يُستخدم في طبقة الشبكة ومحلياً (محركات الأقراص الثابتة، الهواتف، محركات الأقراص المحمولة)

#### **الميزات المحفوفة بالمخاطر:**

* **التشغيل التلقائي:** يسمح لمحركات الأقراص/الأقراص المُدخلة بالتشغيل تلقائياً
* **البلوتوث:** يتيح الاتصالات ونقل البيانات بين الأجهزة
* **NFC:** ينقل البيانات بمدى محدود، حماية قليلة

المنافذ الأساسية (يجب أن تبقى مفتوحة):

* المنفذ 443: حركة المرور الآمنة على الويب
* المنفذ 22: اتصالات خادم آمنة
* المنفذ 80: حركة المرور القياسية على الويب

#### التهديدات الأمنية والحماية

**هجوم اليوم صفر Zero-Day Attack:** هجوم لم يحدث من قبل (لا توجد تصحيحات متاحة بعد)

طرق الحماية:

* استخدم VPN وIDS/IPS
* قم بزيارة الشبكات/المواقع الموثوقة فقط
* اتبع معايير النظافة الأمنية

#### أدوات التقوية

| الأداة | الوظيفة |
| --- | --- |
| **مكافحة الفيروسات/البرامج الخبيثة/برامج التجسس** | اكتشاف وإزالة البرامج الخبيثة |
| **جدران الحماية** | مراقبة الاتصالات وحظر حركة المرور الضارة بناءً على القواعد المحددة مسبقاً |
| **VPNs** | تشفير حركة المرور الخارجة من جهازك |

#### 

#### مخاطر Wi-Fi العام

* غير مشفر ولا يتطلب كلمات مرور
* يمكن للمتسللين اعتراض البيانات، سرقة الهوية، استنزاف الحسابات

سلامة Wi-Fi العام:

* استخدم VPN على جميع الأجهزة
* قم بزيارة مواقع HTTPS فقط
* استخدم الهاتف كنقطة اتصال (الشبكات الخلوية مشفرة)
* عطّل الاتصال التلقائي بـ Wi-Fi
* لا تصل إلى المعلومات الشخصية/المالية

#### خطر كلمات المرور الافتراضية

* سهلة العثور عليها عبر الإنترنت في أدلة المساعدة/الأدلة
* لديها امتيازات على مستوى المسؤول
* تخفي هوية المستخدم
* عادة ما تُترك دون تغيير

**الحل:** تعطيل الحسابات المدمجة، تغيير جميع كلمات المرور الافتراضية، استخدام كلمات مرور قوية

### 

### مفاهيم التشفير Encryption Concepts

#### 1. ما هو التشفير؟

* **التشفير:** تحويل البيانات القابلة للقراءة (**النص العادي plaintext**) إلى تنسيق غير قابل للقراءة (**النص المشفر ciphertext**) باستخدام مفتاح تشفير وخوارزمية (**شفرة cipher**).
* **فك التشفير Decryption:** تحويل النص المشفر مرة أخرى إلى نص قابل للقراءة باستخدام **مفتاح فك التشفير**.
* يُستخدم **لحماية المعلومات الحساسة** من الوصول غير المصرح به.

إلزامي في صناعات معينة:

* التعليم: سجلات الطلاب
* الرعاية الصحية: السجلات الطبية
* التجارة: بيانات المستهلك أو المالية

التشفير المدمج أو الإضافي:

* بعض أنظمة التشغيل تتضمن ميزات التشفير.
* برامج التشفير من طرف ثالث متاحة للأنظمة التي لا تحتوي عليها.

#### 2. حالات البيانات والتشفير Data States and Encryption

1. البيانات في حالة السكون Data at Rest

* مخزنة على جهاز (غير قيد الاستخدام أو النقل).
* يمكن تشفيرها على:
  + مستوى الملف - تشفير ملفات محددة أو جميع الملفات.
  + مستوى التخزين/الجهاز - تشفير القرص بالكامل (مثل BitLocker).
  + مستوى السحابة - تشفير البيانات المخزنة في السحابة.
* أقل عرضة للخطر، لكن لا تزال معرضة للخطر من البرامج الخبيثة أو الهجمات المحلية.
* احمِ بـ: جدران الحماية، VPN، أدوات مكافحة البرامج الخبيثة، والتحديثات.

2. البيانات قيد الحركة (البيانات أثناء النقل) Data in Motion (Data in Transit)

* البيانات تتحرك بنشاط بين الأجهزة (مثل الكمبيوتر ↔ موقع الويب).
* محمية بواسطة HTTPS أو VPN.
* لا تزال عرضة لـ:
  + الهندسة الاجتماعية
  + هجمات الرجل في المنتصف (MitM)
  + التصيد الاحتيالي أو كسر كلمة المرور
* التشفير من طرف إلى طرف (E2EE) يضمن بقاء البيانات آمنة حتى إذا تم اعتراضها.
  + فقط المرسل والمتلقي يمكنهما فك تشفير البيانات.

#### 3. أنواع التشفير Types of Encryption

1. التشفير المتماثل (المفتاح الواحد / المفتاح الخاص) Symmetric Encryption

* يُستخدم مفتاح واحد للتشفير وفك التشفير.
* سريع وفعال، جيد لتشفير البيانات الكبيرة أو الاتصالات في الوقت الفعلي.
* الخطر: إذا تمت سرقة المفتاح الواحد، يتم كشف جميع البيانات.

**أمثلة:** 3DES، CAST

✅ **المزايا:**

* سريع، استخدام منخفض للذاكرة
* مثالي لتبادل بيانات الجلسة الآمنة

❌ **العيوب:**

* صعب مشاركة المفتاح بشكل آمن
* عرضة للخطر إذا لم تكن توزيع المفتاح محمياً

2. التشفير غير المتماثل (تشفير المفتاح العام) Asymmetric Encryption (Public Key Cryptography)

* يستخدم مفتاحين:
  + المفتاح العام (يُشارك علناً)
  + المفتاح الخاص (يُحفظ سراً)
* أبطأ، لكنه أكثر أماناً ومثالي للبيانات الصغيرة أو تبادل المفاتيح.
* الاستخدامات الشائعة:
  + المصادقة
  + الشهادات الرقمية
  + التوقيعات الرقمية
  + تبادل المفاتيح الآمن **مثال على الشفرة:** RSA

#### 4. البنية التحتية للمفتاح العام (PKI) Public Key Infrastructure

* نظام موثوق لإدارة المفاتيح العامة/الخاصة والشهادات الرقمية.
* **سلطة الشهادات (CA)** تصدر شهادات رقمية تؤكد الهوية.
* الشهادة تتضمن مفتاحاً عاماً للتشفير.
* المتلقي يستخدم مفتاحه الخاص لفك التشفير.

يُستخدم في:

* مصادقة البطاقة الذكية:
  + البطاقة الذكية تحتوي على زوج مفاتيح (عام/خاص).
  + ترسل شهادة رقمية إلى الخادم → إذا كانت موثوقة، يستخدم الخادم المفتاح العام لتشفير تحدٍ.
  + فقط المفتاح الخاص على البطاقة يمكنه فك تشفيره.

#### 5. التوقيعات الرقمية Digital Signatures

عملية عكسية للتشفير:

* المرسل يشفر توقيعاً باستخدام مفتاحه الخاص.
* المتلقي يفك التشفير باستخدام المفتاح العام.
* إذا نجح → يؤكد سلامة الرسالة وصحة المرسل.

يضمن:

* **النزاهة:** الرسالة لم تتغير
* **المصادقة:** يؤكد هوية المرسل
* **عدم الإنكار:** المرسل لا يمكنه إنكار إرسالها

#### 6. التجزئة التشفيرية Cryptographic Hashing

* تحول البيانات (كلمة المرور، الملف، الرسالة) إلى سلسلة فريدة ذات طول ثابت.
* الناتج دائماً بنفس الطول، بغض النظر عن حجم المدخلات.
* أي تغيير في البيانات → تجزئة مختلفة تماماً.

الاستخدامات:

* حماية كلمة المرور
* التحقق من سلامة البيانات
* مصادقة الملفات

سير العمل المثالي:

1. كلمة المرور → تُجزأ وتُخزن.
2. تسجيل الدخول → تُجزأ كلمة المرور مرة أخرى.
3. إذا تطابقت التجزئات → يُمنح الوصول.

**التجزئات أحادية الاتجاه:** لا يمكن عكسها إلى البيانات الأصلية.

الفوائد:

* توفير مساحة التخزين
* كشف التلاعب
* تأمين أنظمة المصادقة

### الخاتمة

هذا الملخص يغطي الأساسيات الجوهرية للأمن السيبراني، بدءاً من المفاهيم الأساسية لثالوث CIA (السرية والنزاهة والتوافر) وصولاً إلى التقنيات المتقدمة مثل التشفير والمصادقة متعددة العوامل.

النقاط الرئيسية:

1. **الحماية متعددة الطبقات ضرورية** - لا يوجد حل أمني واحد كافٍ بمفرده.
2. **الوعي البشري أمر حاسم** - معظم الاختراقات تحدث بسبب الأخطاء البشرية أو الهندسة الاجتماعية.
3. **التحديثات المنتظمة حيوية** - الحفاظ على تحديث الأنظمة والبرامج يحمي من نقاط الضعف المعروفة.
4. **التشفير أساسي** - يجب تشفير البيانات الحساسة سواء كانت مخزنة أو قيد النقل.
5. **المصادقة القوية إلزامية** - استخدام MFA يقلل بشكل كبير من مخاطر الاختراق.
6. **الخصوصية حق** - احترام وحماية البيانات الشخصية ليس فقط قانونياً بل أخلاقياً أيضاً.

**تذكر:** الأمن السيبراني ليس منتجاً - إنه عملية مستمرة تتطلب يقظة دائمة، تعليماً مستمراً، وتكيفاً مع التهديدات الجديدة.

#### **إعداد:** إسماعيل محمد قطان **التاريخ:** أكتوبر، 2025