مبادئ أساسية في أمن المعلومات

أولاً : مقدمة في أمن المعلومات

قبل أن نتحدث عن الاختراق... يجب أن نفهم أولاً ماذا نحاول أن نحمي.

Information System = Data + People + Devices + Network

- **أمن نظم المعلومات يعني حماية هذا النظام بالكامل، وليس فقط حماية جهاز أو كلمة مرور.**

1- مفهوم أمن المعلومات

أمن المعلومات هو مجموعة الممارسات والتقنيات المستخدمة لحماية المعلومات الرقمية من:

الوصول غير المصرح به , التغيير أو التعديل , السرقة , التلف أو التعطيل

وهو لا يقتصر على البرمجيات فقط، بل يشمل:

الحماية المادية للأجهزة , السياسات الإدارية , ضوابط الوصول , التطبيقات , الشبكات , الإجراءات التنظيمية

وفق تعريف **(NIST)**

فهو حماية المعلومات وأنظمة المعلومات من الوصول أو الاستخدام أو الكشف أو التعديل أو التعطيل غير المصرح به.

2- لماذا أصبح أمن المعلومات ضرورة؟

التحول الرقمي المتسارع أدى إلى:

زيادة حجم البيانات – انتشار الحوسبة السحابية – تعدد الأجهزة الذكية – ظهور إنترنت الأشياء **(IoT)** – توسع سطح الهجوم **(Attack Surface)**

كلما زادت الأنظمة تعقيداً، أصبح تأمينها أكثر صعوبة.

3- المخاطر المعاصرة

- الخطأ البشري (ما يزال من أكبر أسباب الاختراق)
- الجرائم الإلكترونية
- تسريب البيانات
- سرقة الملكية الفكرية
- الغرامات القانونية الناتجة عن خرق الخصوصية
- فقدان البيانات اليوم قد يعني:
- خسارة مالية
- فقدان ثقة العملاء
- أضرار قانونية جسيمة

ثانياً: عناصر أمن المعلومات الأساسية

1- سرية البيانات – Confidentiality

هي ضمان أن المعلومات لا يمكن الاطلاع عليها إلا من قبل الأشخاص المخولين.

بمعنى: من يحق له أن يرى البيانات؟

حسابك البنكي – درجاتك الجامعية – صورك الشخصية

كيف تتحقق السرية؟

التشفير – كلمات المرور – التحكم في الوصول – سياسات تصنيف البيانات

تصنيف البيانات :

- البيانات العامة

متاحة للجميع. مثال: البيانات الصحفية – وصف الوظائف.

- البيانات الداخلية

مخصصة لموظفي المؤسسة فقط. مثال: المذكرات الداخلية – خطط العمل.

البيانات السرية

تتطلب تصريحاً خاصاً. مثال: أرقام البطاقات البنكية – ملفات العملاء.

البيانات المقيدة

أعلى درجات الحساسية.

تسريبها قد يؤدي إلى:

غرامات قانونية – اتهامات جنائية – خسائر استراتيجية

مثال: الأبحاث العلمية – الملكية الفكرية.

2- التكاملية – Data Integrity

لو دخلت اليوم فوجدت معدلك تغير من 85 إلى 55...

هل المشكلة سرية أم تكاملية؟ الإجابة: تكاملية.

لتعريف : هي ضمان دقة البيانات ومنع تعديلها دون إذن.

بمعنى: هل البيانات صحيحة ولم يتم العبث بها؟

ماذا تشمل التكاملية؟

- الحفاظ على ترتيب البيانات
- الحفاظ على موثوقيتها
- ضمان عدم تغييرها أثناء النقل
- ضمان إمكانية تتبع مصدرها

مثال :

تحميل برنامج + التحقق من Hash.

- **Hash هو بصمة رقمية للملف.**
- **إذا تغير حرف واحد... تتغير البصمة بالكامل.**

كيف تتحقق التكاملية؟

- دوال التجزئة (Hash Functions)
- التوقيع الرقمي
- صلاحيات دقيقة
- سجلات تتبع (Logs)

3- الوثوقية – Authentication

هي عملية التأكد من هوية الشخص أو الجهاز الذي يطلب الدخول للنظام.

بمعنى: هل أنت فعلاً الشخص الذي تدّعي أنك هو؟

أنواع المصادقة :

- شيء يعرفه العميل

كلمة المرور وهي الأكثر شيوعاً.

- شيء يملكه العميل

هاتف – رمز تحقق – Token

- شيء يمثله العميل

بصمة – قزحية العين – التعرف على الوجه

كلما زادت عوامل المصادقة، زادت قوة الحماية.

4- السماحية – Authorization

هي تحديد ما إذا كان المستخدم يملك الإذن للوصول إلى مورد معين أو تنفيذ عملية معينة.

الفرق المهم:

Authentication → من أنت؟

Authorization → ماذا يُسمح لك أن تفعل؟

مثال:

في نظام الجامعة:

الطالب: يعرض درجاته فقط.

الأستاذ: يدخل الدرجات.

المدير: يعدل بيانات النظام.

5- صلاحيات الدخول – Access Control

هي مجموعة القواعد التي تسمح أو تمنع المستخدم من الوصول إلى المعلومات.

قد تعتمد على: نوع المستخدم – مستوى الحساسية – موقع المستخدم – وقت الدخول .

بمعنى:

Authorization = القرار

Access Control = التطبيق العملي للقرار

6- عدم الإنكار – Non-Repudiation

هو ضمان عدم قدرة الشخص على إنكار قيامه بإرسال أو تنفيذ عملية معينة.

أهميته:

المعاملات البنكية – العقود الإلكترونية – المراسلات الرسمية

إذا أرسل شخص رسالة رسمية، يجب أن يكون هناك دليل يثبت ذلك.

7- التوقيع الإلكتروني – Digital Signature

هو إثبات رقمي يؤكد أن المرسل هو بالفعل الجهة التي تدّعي إرسال البيانات.

يعتمد على:

- مفاتيح تشفير (عام وخاص)
- شهادات إلكترونية
- ماذا يحقق التوقيع الرقمي؟
- إثبات الهوية
- ضمان سلامة البيانات
- منع الإنكار

8- الوجودية العالية – High Availability

هي ضمان استمرار عمل النظام دون توقف.

لماذا هي مهمة؟

نظام آمن لكنه متوقف = نظام فاشل.

كيف تتحقق؟

- توزيع الأحمال (Load Balancing)
- خوادم احتياطية
- نسخ احتياطي دوري
- بنية تحتية موزعة

هذه العناصر لا تعمل منفصلة، بل مترابطة و أي خلل في عنصر واحد يؤثر على النظام بالكامل .

في هذا الخطط :

User → Network → Server → Database

- **في أي نقطة نطبق السرية؟**
- **في أي نقطة نطبق التكاملية؟**
- **في أي نقطة نطبق المصادقة؟**

أمن المعلومات ليس برنامج حماية فقط، بل هو:

تصميم هندسي – إدارة مخاطر – سياسات تنظيمية – وعي بشري – تطبيق معايير عالمية

المهندس الناجح لا يبني نظامًا يعمل فقط , بل يبني نظامًا يعمل بأمان، بثقة، وباستمرارية.