ملخص الوحدة 2: الأمن السيبراني

البرمجة والذكاء الاصطناعي، تانية ثانوي بكالوريا

مهندس رحيم

2-1 تقنيات التشفير والمصادقة

- **HTTPS بيشتغل إزاي؟**: HTTP + تشفير **TLS** = **HTTPS:**
- **ثلاث مراحل**
  - TLS handshake (1**
  - TLS handshake (2**
  - **3) تبادل البيانات:** البيانات تتشفر وتتبادل بمفتاح الجلسة المشترك
- **ليه الاتنين؟**: **التشفير بالمفتاح العام (public-key):** مناسب لـ **مشاركة المفتاح بأمان**
- **المصادقة متعددة العوامل (MFA)**
  - البنك الإلكتروني: باسورد (معرفة) + one-time password (حيازة).
  - السوشيال ميديا: باسورد (معرفة) + SMS (حيازة).
  - لابتوب الشركة أو دخول مبنى: smart card (حيازة) + بصمة (سمات حيوية).
  - الشراء الأونلاين: باسورد (معرفة) + كود 3-D Secure أو تأكيد الكارت (حيازة).
- **ربط التقنيات ببعض**
  - **Encryption:** يمنع الغير من قراءة المحتوى.
  - **Digital signature:** يكشف التلاعب وانتحال المرسل
  - **Digital certificate:** يتأكد إن الطرف التاني حقيقي.
  - **MFA:** يمنع الدخول غير المصرح به.
  - **التهديد ← التقنية:** اعتراض المحتوى ← تشفير · تعديل البيانات أو انتحال المرسل ← توقيع رقمي · توجيهك لموقع مزيف ← شهادة رقمية · تسرب الباسورد ← MFA/2FA

HTTPS	HTTP + تشفير TLS (تشفير + كشف تلاعب + تحقق من الطرف الآخر)
TLS handshake	إجراء إنشاء الاتصال الآمن
Common-key (symmetric)	نفس المفتاح للتشفير وفكّه — سريع للبيانات الكبيرة
Public-key cryptography	مفتاح عام للتشفير ومفتاح خاص لفك التشفير
Digital certificate	تثبت إن الطرف الآخر حقيقي (تصدرها CA)
Digital signature	تكشف التلاعب وتحقق عدم التنصل
Non-repudiation	عدم قدرة المرسل على إنكار الإرسال
Multi-factor authentication	دمج عاملين أو أكثر: معرفة/حيازة/سمات حيوية
Two-factor authentication (2FA)	المصادقة الثنائية: عاملين مستقلين من نوعين مختلفين (معرفة / حيازة / سمات حيوية)
Session key	مفتاح الجلسة: مفتاح متماثل كل طرف بيشتقّه في المصافحة، وعمره ما بيتبعت على الشبكة
Chain of trust	سلسلة الثقة: الربط من شهادة الموقع لحد جهة إصدار موثوقة، والمتصفح بيتأكد منه

2-2 تصميم أمان الشبكات

- **Firewall (جدار الحماية):** نظام أو برنامج بيراقب حركة المرور و**بيسمح أو يمنع** الاتصال حسب قواعد معمولة مسبقاً
- **VPN**: بيعمل **نفق (tunnel) مشفّر** عبر الإنترنت للاتصال بشبكة من مكان بعيد.
- **DMZ**: منطقة بتتحط فيها الخوادم المكشوفة للخارج (ويب

- **Defense in depth (الدفاع في العمق)**
  - **الطبقة 1
  - **الطبقة 2
  - **الطبقة 3
  - **الطبقة 4
  - الفكرة: لو طبقة وقعت
- **Zero trust**: **ما تثقش في أي اتصال

Firewall	يسمح/يمنع الاتصال حسب قواعد
VPN	نفق مشفّر آمن عبر الإنترنت
DMZ	منطقة معزولة للخوادم العامة
Defense in depth	طبقات حماية متعددة
Zero trust	ما تثقش في أي اتصال وتحقق دايماً
Perimeter	المحيط الأمني: حدود الشبكة
Endpoint	جهاز طرفي (كمبيوتر/موبايل)

2-3 الاستجابة للحوادث وإدارة المخاطر

- **Security incident (حادث أمني)**
  - **Information leak:** تسرب معلومات شخصية أو سرية.
  - **Data tampering:** تغيير بيانات في النظام بدون تصريح.
  - **Service outage:** انقطاع الخدمة بسبب هجوم على الخادم.
- **مراحل الاستجابة الست (التسلسل العام)**
  - **1) Preparation:** تحضير الإجراءات والفريق مسبقاً.
  - **2) Detection:** اكتشاف وتأكيد حصول الحادث.
  - **3) Containment:** تحديد نطاق التأثير عشان الضرر ما ينتشرش (مثلاً عزل الجهاز المصاب).
  - **4) Eradication:** إزالة سبب الحادث (مثلاً حذف malware).
  - **5) Recovery:** إرجاع الأنظمة للوضع الطبيعي (مثلاً من backup نظيف).
  - **6) Prevention of recurrence:** تحليل السبب وإجراءات تمنع التكرار.
- **تقييم المخاطر: Risk:** = احتمال حدوث مشكلة مستقبلاً وتأثيرها.
- **مثال: برمجية فدية (ransomware) في مدرسة**
  - **الموقف:** ransomware شفّر ملفات نظام سجلات الطلبة
  - **إحنا فين؟:** التحضير فات
  - **غلطة شائعة:** ترجّع الباك أب فوراً قبل ما تشيل التهديد
  - **الأولويات:** هجوم فدية تاني (تأثير كبير) غالباً أهم من انقطاع كهربا قصير (تأثير صغير).

Security incident	حدث يؤثر على سرية المعلومات أو سلامتها أو توافرها، أو يخالف سياسة أمنية
Containment	احتواء الضرر ومنع انتشاره
Eradication	إزالة سبب الحادث
Recovery	إرجاع النظام للحالة الطبيعية
Risk	احتمال حدوث مشكلة وتأثيرها
Impact	حجم الضرر لو الخطر حصل
Likelihood	احتمال حدوث الخطر
Risk matrix	مصفوفة تقييم المخاطر: جدول درجة التأثير × درجة الاحتمالية لترتيب المخاطر



ذاكر المادة كلها مجاناً

شرح كل الدروس، أسئلة بالإجابات، بنك على نمط الوزارة، وامتحان بشكل الوزارة

zerooneacademy.com

مهندس رحيم