الوحدة 19: الأجهزة المحمولة وإنترنت الأشياء

إدارة الأجهزة المحمولة (MDM/MAM)

MDM (Mobile Device Management): يتحكم بالجهاز بالكامل - قفل عن بُعد، مسح البيانات، فرض كلمة مرور، تثبيت التطبيقات بالقوة. يستخدم في المؤسسات لحماية بيانات العمل.

MAM (Mobile Application Management): يدير التطبيقات فقط وليس الجهاز بأكمله. يمكن عزل تطبيقات العمل عن التطبيقات الشخصية (Containerization). مثلاً تطبيق بريد العمل فقط هو المُدار.

Containerization: فصل بيانات العمل عن البيانات الشخصية على نفس الجهاز باستخدام حاويات مشفرة.

نُهج امتلاك الأجهزة (BYOD/COPE)

BYOD (Bring Your Own Device): الموظف يستخدم جهازه الشخصي للعمل. يوفر تكاليف لكنه يزيد المخاطر الأمنية. يحتاج إلى MAM قوي.

COPE (Corporate Owned, Personally Enabled): الشركة تمتلك الجهاز وتسمح باستخدام شخصي محدود. تحكم كامل من MDM مع بعض الخصوصية للموظف.

CYOD (Choose Your Own Device): الموظف يختار جهازاً من خيارات محددة تملكها الشركة.

تهديدات الأجهزة المحمولة

Jailbreaking (iOS): كسر قيود نظام التشغيل للحصول على صلاحيات الجذر. يزيل الحماية المدمجة ويسمح بتثبيت تطبيقات من مصادر غير موثوقة.

Rooting (Android): الحصول على صلاحيات الجذر في Android. يسمح بتعديل النظام والتطبيقات لكنه يعرض الجهاز للاختراق.

Sideloading: تثبيت تطبيقات من خارج المتجر الرسمي. يزيد خطر تثبيت برمجيات خبيثة.

تحديد المواقع غير الآمن: استخدام GPS وشبكات Wi-Fi غير مشفرة لتتبع الموقع.

مثال: فحص جهاز Android باستخدام adb

```
adb devices
adb shell
adb install app.apk
adb logcat -d > logs.txt
```

`adb devices` - قائمة الأجهزة المتصلة عبر USB أو TCP. يظهر معرف الجهاز وحالته (device/unauthorized).

`adb shell` - فتح قشرة تفاعلية على الجهاز للوصول إلى نظام الملفات وتشغيل أوامر Linux (مثل `su` للجذر).

`adb install app.apk` - تثبيت تطبيق من ملف APK مباشرة. مفيد للاختبار الأمني قبل النشر.

`adb logcat -d > logs.txt` - تفريغ سجلات النظام (logcat) إلى ملف. يستخدم لتحليل سلوك التطبيقات واكتشاف الثغرات.

IoT و SCADA

IoT (إنترنت الأشياء): أجهزة متصلة بالإنترنت مثل الكاميرات وأجهزة التحكم. غالباً ما تكون ضعيفة أمنياً بسبب مواردها المحدودة وعدم وجود تحديثات.

مشاكل أمن IoT: كلمات مرور افتراضية، نقص التشفير، عدم وجود تحديثات تلقائية، بروتوكولات غير آمنة (MQTT بدون TLS).

SCADA (Supervisory Control and Data Acquisition): أنظمة التحكم الصناعي (مصانع، كهرباء، مياه). تستخدم بروتوكولات مثل Modbus و DNP3. أي اختراق لها خطر على السلامة العامة.

مثال: كشف أجهزة IoT في الشبكة

```
nmap -sS -p 80,443,8080,22 192.168.1.0/24
nmap -A 192.168.1.50
```

`-p 80,443,8080,22` - فحص المنافذ الشائعة للأجهزة الذكية (واجهات ويب و SSH).

`192.168.1.0/24` - مسح الشبكة المحلية بالكامل للكشف عن الأجهزة المتصلة.

`-A` - فحص متقدم (Aggressive): كشف نظام التشغيل، الإصدارات، وتتبع المسار. يكشف أجهزة IoT حتى لو غير معروفة.

Quick Quiz (MCQ)

1. What does MDM (Mobile Device Management) allow administrators to do?
   a) Encrypt network traffic
   b) Enforce security policies and remotely manage mobile devices
   c) Monitor wireless signals
   d) Block all internet access

   Answer: b

2. What is jailbreaking in the context of mobile devices?
   a) Installing antivirus software
   b) Removing software restrictions imposed by the operating system
   c) Encrypting the device storage
   d) Updating the operating system

   Answer: b

3. What does BYOD stand for and what is its primary security concern?
   a) Backup Your Online Data - data loss

b) Bring Your Own Device - mixing personal and corporate data

c) Buy Your Own Disk - hardware failure

d) Build Your Own Directory - access control

Answer: b

4. What type of systems do SCADA and ICS typically control?

a) Office email servers

b) Industrial and critical infrastructure systems

c) Home wireless routers

d) Personal laptops

Answer: b

5. What is the most common security vulnerability in IoT devices?

a) Strong encryption

b) Default credentials and lack of firmware updates

c) High processing power

d) Excessive memory allocation

Answer: b