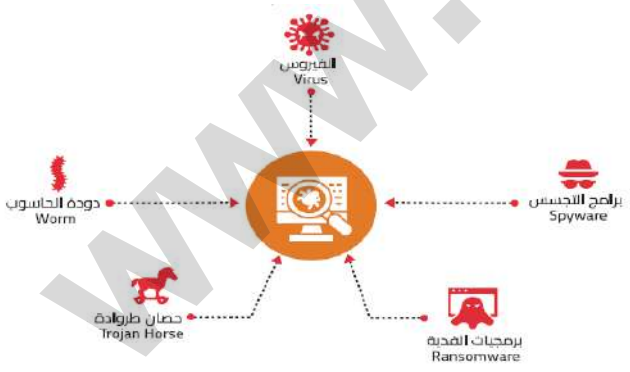
وزارة التربية و التعليم
مديرية التربية والتعليم للواءي الطيبة والوسطية
مدرسة الخراج الثانوية المختلطة
ملخص شامل الدرس الثاني: تهديدات الأمن السيبراني – الصف التاسع

الأمن السيبراني: هو مجموعة من الإجراءات والتقنيات التي تحمي **الأنظمة والشبكات والبيانات** من الهجمات والاختراقات، **وتهدف إلى الحفاظ على:**

- **سرية البيانات** (حمايتها من الاطلاع غير المصرّح).
- **سلامة النظام والبيانات** (منع التلاعب أو التغيير غير المصرّح).
- **توافر الخدمة** (إستمرارية عمل الخدمات دون انقطاع).
- **الخصوصية** (حماية معلومات الأفراد من الكشف أو الاستخدام الخاطئ).
- **اكتشاف الهجمات والاستجابة لها.**

أهم تهديدات الأمن السيبراني

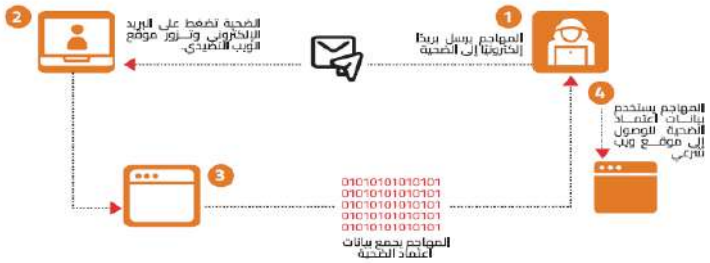


الشكل (2-1): بعض أنواع البرمجيات الخبيثة

1. البرمجيات الخبيثة(Malware)

برامج ضارة تهدف للتخريب أو التجسس أو سرقة البيانات، ومن أمثلتها:

- **الفيروسات :(Viruses)** تُصيب الملفات وتتكاثر عند تشغيل الملف المصاب.
- **الديدان :(Worms)** تنتشر عبر الشبكات تلقائيًا دون تدخل المستخدم.
- **برامج الفدية :(Ransomware)** تُقفل النظام أو تُشفّر الملفات وتطلب فدية لفكها.
- **برامج التجسس :(Spyware)** تراقب نشاط المستخدم وتسرق معلومات حساسة.



الشكل (2-2): عملية الهجوم بالتصيُّد الاحتيالي

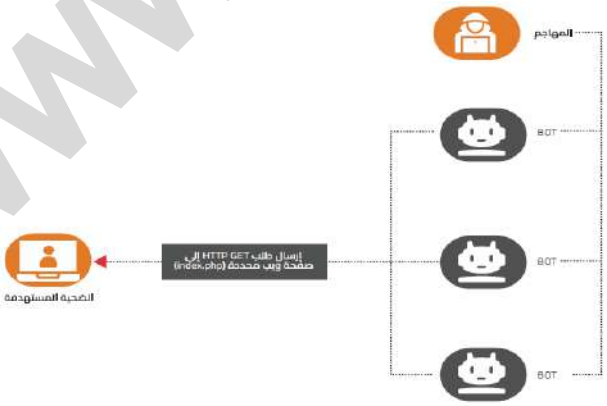
2. التصيد الاحتيالي (Phishing)

محاولات خداع للحصول على معلومات حساسة (مثل كلمات المرور والبيانات البنكية) عبر رسائل بريد/روابط/مواقع مزيفة تنتحل صفة جهة موثوقة.

3. الثغرات الأمنية(Security Vulnerabilities)

نقاط ضعف في الأجهزة أو البرامج أو الشبكات أو الإجراءات قد يستغلها المهاجمون، ومن أنواعها:

- **ثغرات برمجية :(Software)** أخطاء في الكود أو ضعف التحقق من البيانات المدخله الى البرنامج.
- **ثغرات الشبكة :(Network)** مثل ضعف إعدادات الشبكة أو ضعف التشفير.
- **ثغرات إجرائية :(Procedural)** ضعف السياسات أو خطوات العمل (مثل ضعف التحقق من الهوية لمنح االوصول).
- **ثغرات الأجهزة :(Hardware)** نقاط ضعف في المعدات مثل بعض الثغرات الشهيرة **(Meltdown / Spectre).**



الشكل (2-4): هجمات حجب الخدمة الموزعة

4. حجب الخدمة الموزعة (DDoS)

إغراق خادم أو موقع بطلبات هائلة متزامنه عبر أجهزة مخترقة **(Botnet)** لتعطيله ومنع المستخدمين من الوصول إليه.

الشكل (2-5): بعضُ طرقِ سرقةِ الهُويّة

5. سرقة الهوية(Identity Theft)

استخدام بيانات شخصية مسروقة (اسم، رقم وطني، حسابات، بطاقات) لانتحال شخصية الضحية، وقد تحدث عبر تصفح غير آمن، تسريبات بيانات، أو نشاط برمجيات خبيثة.

6. الهندسة الاجتماعية(Social Engineering)

التلاعب النفسي لاستدراج الأفراد لكشف معلومات حساسة أو تنفيذ إجراءات خاطئة تطلب من المهاجمين، عبر بناء الثقة ثم استغلالها.

الفرق بين الهجوم الإلكتروني والاعتداء الإلكتروني

- **الهجوم الإلكتروني :**محاولة غير مشروعة للوصول للأنظمة أو تعطيلها أو اختراقها.
- **الاعتداء الإلكتروني :**يركز أكثر على **إيقاع ضرر مباشر** وقد يكون نتيجة للهجوم أو جزءًا منه (مثل ابتزاز، تشهير، تهديد).

وسائل الحماية من تهديدات الأمن السيبراني

- **تنقسم وسائل الحماية إلى نوعين رئيسيين:**

1. **الحماية المادية (Physical Security):** تهدف إلى حماية الأجهزة والمعدات ومواقع التخزين ومنع الوصول غير المصرّح به للأماكن التي تحتوي على أجهزة وبيانات حساسة.
2. **الحماية الرقمية (Digital Security):** تهدف إلى حماية البيانات والأنظمة الإلكترونية من الهجمات مثل الاختراقات والبرمجيات الضارة وسرقة البيانات.

أمثلة على وسائل الحماية

أولًا: وسائل مادية

- **ضوابط الوصول الفيزيائي :**أقفال ومفاتيح وبطاقات دخول وبصمة أو مسح الوجه لتقييد الدخول للمناطق الحساسة.
- **المراقبة بالفيديو :**كاميرات أمنية لمتابعة المداخل والمناطق الحساسة.
- **الحراس الأمنيون :**تأمين المواقع والتحقق من الهويات.
- **الحماية من الكوارث الطبيعية :**إجراءات لحماية المعدات والبيئة من الحوادث مثل الحرائق والزلازل والفيضانات.

ثانيًا: وسائل رقمية

- **التشفير (Encryption)** لحماية البيانات أثناء النقل والتخزين.
- **المصادقة متعددة العوامل (MFA)** لتعزيز التحقق من هوية المستخدم.
- **جدران الحماية (Firewalls)** لمنع الوصول غير المصرح به إلى الشبكات.
- **برامج مضاد الفيروسات (Antivirus)** لمواجهة البرمجيات الخبيثة.

التكامل بين الحماية المادية والرقمية لحماية البيانات

- الجمع بين النوعين يوفّر **طبقات أمن** تقلل نقاط الضعف وتحسّن حماية البيانات.
- **يشمل التكامل إجراءات مثل :**
  - **ماديًا:** حماية الأجهزة ووسائط التخزين، وأنظمة مراقبة، والتخلص الآمن من البيانات/الأجهزة لمنع استرجاعها.
  - **رقميًا:** التشفير، مضادات الفيروسات ومكافحة الاختراق، تفعيل جدران الحماية، والتحديثات الأمنية المنتظمة.
  - **ممارسات جيدة للأمان :**كلمات مرور قوية وفريدة، التوعية الأمنية، النسخ الاحتياطي المنتظم، وخطط الاستجابة للحوادث.

بالتوفيق للجميع

معلمة المادة: هنادي وديان