امنية الشبكات ومفهوم التهديدات الشبكية:

:Network security and the concept of network threats

أمنية الشبكات، مفهوم التهديدات الشبكية، وأنواعها

أمنية الشبكات (Network Security)، مع التركيز حصريًا على مفهوم التهديدات الشبكية (Network Threats) وأنواعها. سأعتمد هنا على توضيح المفاهيم الأساسية في مجال الأمن السيبراني، مع شرح واضح وأمثلة عملية. المعلومات مبنية على معايير دولية مثل NIST (National Institute of Standards and Technology) و ISO 27001 للأمن المعلوماتي.

1. أمنية الشبكات (Network Security)

أمنية الشبكات هي مجموعة الإجراءات، التقنيات، والسياسات المصممة لحماية بنية الشبكة الحاسوبية من الوصول غير المصرح به، التعديل غير المصرح به، أو التعطيل. تشمل الشبكات هنا أي نظام مترابط من الأجهزة (مثل الحواسيب، الخوادم، والأجهزة المحمولة) الذي يتبادل البيانات عبر وسائط سلكية أو لاسلكية، مثل الإنترنت أو الشبكات المحلية (LAN).

- أهداف أمنية الشبكات الرئيسية (مبدأ CIA Triad):

1- السرية (Confidentiality): ضمان أن البيانات متاحة فقط للأشخاص المصرح لهم، من خلال التشفير (Encryption) لمنع التجسس.

2- السلامة (Integrity): حماية البيانات من التعديل أو التزييف، باستخدام آليات التحقق مثل الهاش (Hashing) للكشف عن أي تغيير.

3- التوافر (Availability): ضمان استمرارية الوصول إلى الشبكة والخدمات، حتى في حال الهجمات التي تهدف إلى التعطيل.

هذه الأهداف تُكمل بأهداف إضافية مثل التحقق من الهوية (Authentication) والتحكم في الوصول (Access Control).

- أهمية أمنية الشبكات:

في عصر الرقمنة، أصبحت الشبكات عماد الاقتصاد والحياة اليومية (مثل البنوك، الرعاية الصحية، والحكومات). بدون أمن قوي، يمكن أن تؤدي الثغرات إلى خسائر مالية هائلة (مثل هجوم WannaCry في 2017 الذي أثر على ملايين الأجهزة)، سرقة بيانات شخصية، أو تعطيل خدمات حيوية. وفقًا لتقرير Verizon DBIR 2023، 74% من الانتهاكات الأمنية تبدأ من خلال الشبكات. يشمل الأمن الشبكي أدوات مثل الجدران النارية (Firewalls)، أنظمة كشف الاقتحام (IDS/IPS)، والبرمجيات المضادة للفيروسات، بالإضافة إلى السياسات البشرية مثل التدريب على الوعي الأمني.

- مكونات أمنية الشبكات الأساسية (باختصار):

الأجهزة الأمنية: جدران نارية، موجهات آمنة (Secure Routers).

البرمجيات: برامج التشفير (مثل SSL/TLS)، وأنظمة المراقبة (SIEM - Security Information and Event Management).

الإجراءات: التحديثات الدورية، النسخ الاحتياطي، والتدقيق الأمني (Auditing).

الهدف النهائي هو تقليل المخاطر إلى أدنى مستوى مقبول (Risk Management).

2. مفهوم التهديدات الشبكية (Network Threats)

التهديدات الشبكية هي أي حدث أو نشاط يهدف إلى استغلال الثغرات (Vulnerabilities) في الشبكة لإلحاق الضرر، سرقة المعلومات، أو تعطيل الخدمات. يُعرف التهديد كـ"إمكانية وقوع حدث يؤثر سلبًا على أمن الشبكة"، وفقًا لتعريف NIST. هذه التهديدات قد تكون متعمدة (مثل هجمات الهاكرز) أو غير متعمدة (مثل أخطاء المستخدمين أو الكوارث الطبيعية).

- خصائص التهديدات الشبكية:

1- الأصل: داخلي (من موظفين أو أجهزة مصابة داخل الشبكة) أو خارجي (من مهاجمين عبر الإنترنت).

2- الدوافع: مالية (سرقة بيانات للبيع)، سياسية (هجمات إرهابية سيبرانية)، تجسس (دولي أو تجاري)، أو تخريب (انتقام شخصي).

<u>التأثيرات:</u>

1- مالية: خسائر مباشرة (مثل دفع فدية في هجمات Ransomware) أو غير مباشرة (فقدان الثقة من العملاء).

2- تشغيلية: تعطيل الخدمات، مما يؤدي إلى توقف الأعمال (مثل هجوم DDoS على بنك).

3- قانونية وأخلاقية: انتهاك الخصوصية، غرامات قانونية (مثل GDPR في أوروبا)، أو ضرر سمعي.

4- أمنية: سرقة بيانات حساسة، مما يؤدي إلى جرائم أكبر مثل الاحتيال أو الهجمات الإرهابية.

<u>كيفية حدوثها:</u> تستغل الثغرات مثل البرمجيات غير المحدثة، كلمات مرور ضعيفة، أو عدم تشفير البيانات. وفقًا لتقرير IBM 2023، متوسط تكلفة انتهاك أمني يصل إلى 4.45 مليون دولار، معظمها بسبب التهديدات الشبكية.

- **<u>الفرق بين التهديد والثغرة والمخاطر:</u>**

1- التهديد (Threat): الخطر المحتمل (مثل فيروس).

2- الثغرة (Vulnerability): الضعف في النظام (مثل برنامج قديم).

3- المخاطر (Risk): احتمال وقوع التهديد × شدته (يُقاس ويُدار).

3. أنواع التهديدات الشبكية

تصنف التهديدات إلى فئات رئيسية بناءً على الطريقة والأثر. إليك التفصيل للأنواع الشائعة، مع أمثلة، آلية العمل، والتأثيرات:

1. التهديدات المتعلقة بالبرمجيات الضارة (Malware Threats):

الوصف: برامج مصممة لإلحاق الضرر أو السيطرة على الشبكة دون إذن. تنتشر عبر البريد الإلكتروني، المواقع، أو الأجهزة المصابة.

- **الأنواع الفرعية:**

1- الفيروسات (Viruses): تُضاف إلى ملفات شرعية وتنتشر عند الفتح، مما يعدل أو يحذف البيانات (مثل ILOVEYOU في 2000 الذي أصاب ملايين الحواسيب).

2- الديدان (Worms): تنتشر تلقائيًا عبر الشبكة دون تدخل مستخدم، مثل WannaCry الذي استغل ثغرة في Windows وطالب بفدية.

3- التروجان (Trojans): تتنكر كبرامج مفيدة لسرقة البيانات (مثل تطبيقات مزيفة على الهواتف).

4- البرمجيات الجاسوسة (Spyware): تراقب النشاط وتسرق معلومات مثل كلمات المرور.

التأثيرات:

1- سرقة بيانات، تبطيء الشبكة، أو السيطرة الكاملة (Botnets للهجمات الجماعية).

2- الانتشار: 90% من الهجمات تبدأ بـMalware، وفقًا لـKaspersky.

2. هجمات لرفض الخدمة (DoS/DDoS Attacks):

الوصف: إغراق الشبكة بحركة مرور زائدة لتعطيل الخدمات، مما يمنع الوصول الشرعي. DDoS هي النسخة الموزعة باستخدام آلاف الأجهزة المصابة (Botnet).

آلية العمل: إرسال طلبات وهمية مستمرة (مثل SYN Flood) حتى ينهار الخادم.

أمثلة: هجوم DDoS على GitHub في 2018 الذي بلغ 1.3 تيرابت/ثانية، أو هجمات على مواقع حكومية.

التأثيرات: توقف المواقع أو الخدمات لساعات أو أيام، خسائر مالية (مثل 100,000 دولار/ساعة للشركات الكبرى).

الانتشار: زادت بنسبة 200% في 2023، حسب Cloudflare.

3. هجمات التصيد الاحتيالي (Phishing Attacks):

الوصف: خداع المستخدمين لكشف معلومات حساسة عبر رسائل مزيفة تبدو شرعية (مثل بريد إلكتروني يدعي أنه من بنك).

- الأنواع الفرعية:

1- التصيد العام (Phishing): رسائل جماعية.

2- التصيد المستهدف (Spear Phishing): موجه لشخص معين (مثل مدير تنفيذي).

3- التصيد عبر الهاتف (Vishing) أو الرسائل (Smishing).

<u>آلية العمل:</u> رابط يؤدي إلى موقع مزيف يسرق البيانات.

أمثلة: حملات تصيد تستهدف موظفي شركات للوصول إلى الشبكات الداخلية.

التأثيرات: سرقة بيانات تسجيل الدخول، مما يؤدي إلى اختراقات أكبر (95% من الهجمات تبدأ بتصيد، حسب Proofpoint).

4. هجمات الرجل في الوسط (Man-in-the-Middle - MitM):

الوصف: المهاجم يتدخل بين جهازين متصلين (مثل مستخدم وخادم) للتجسس أو تعديل البيانات.

آلية العمل: استغلال شبكات Wi-Fi عامة غير مشفرة، أو ARP Spoofing لإعادة توجيه الحزم.

أمثلة: سرقة بيانات بطاقات الائتمان في مقاهي الإنترنت.

التأثيرات: سرقة كلمات مرور أو بيانات مالية، مما يؤدي إلى احتيال أو تسريب معلومات سرية.

5. التهديدات الداخلية (Insider Threats):

الوصف: تهديدات من أشخاص داخل المنظمة، سواء متعمدة (مثل موظف غاضب) أو غير متعمدة (مثل مشاركة كلمة مرور).

آلية العمل: استخدام صلاحيات داخلية للوصول إلى بيانات أو تثبيت برمجيات ضارة.

أمثلة: موظف يبيع بيانات الشركة، أو خطأ في التحديث يفتح ثغرة.

التأثيرات: 34% من الانتهاكات داخلية، حسب Verizon، وغالباً ما تكون أصعب كشفًا لأنها لا تثير الإنذارات الخارجية.

6. التهديدات الفيزيائية (Physical Threats):

الوصف: تهديدات تؤثر على الأجهزة المادية للشبكة، مثل الكوارث الطبيعية أو التخريب.

الأنواع: حرائق، فيضانات، سرقة أجهزة، أو انقطاع كهرباء.

آلية العمل: تلف الكابلات أو الخوادم، مما يقطع الاتصال.

أمثلة: إعصار يدمر مراكز البيانات، أو تخريب فيزيائي للكابلات.

التأثيرات: فقدان بيانات دائم أو تعطيل طويل الأمد، خاصة إذا لم يكن هناك نسخ احتياطي.

7. هجمات الحقن (Injection Attacks):

الوصف: إدخال رموز ضارة في الشبكة عبر نماذج الإدخال (مثل SQL Injection في قواعد البيانات).

آلية العمل: استغلال عدم التحقق من الإدخال لتنفيذ أوامر غير مصرحة.

أمثلة: سرقة بيانات من مواقع التجارة الإلكترونية.

التأثيرات: تسريب قواعد بيانات كاملة أو السيطرة على الخادم.

8. هجمات التشفير غير المصرح به (Ransomware):

الوصف: نوع من Malware يشفر البيانات ويطالب بفدية لفك التشفير.

آلية العمل: ينتشر عبر البريد أو الثغرات، ثم يقفل الملفات.

أمثلة: هجوم Colonial Pipeline في 2021 الذي أوقف إمدادات الوقود في الولايات المتحدة.

التأثيرات: دفع ملايين الدولارات، وفقدان بيانات إذا لم يُدفع.

الخلاصة:

التهديدات الشبكية تتطور بسرعة مع تقنيات مثل الذكاء الاصطناعي، مما يتطلب أمنًا متعدد الطبقات (Defense in Depth). للوقاية، يُنصح بتحديث البرمجيات، استخدام التشفير، والتدريب المستمر.