جامـــــــعة المســـــــتقبل

كلية التقنيات الصحية والطبية

قـــسم تقنيـــات الاشعـــــة

المرحلـــة الثالثة

تطبيقات الحاســـوب (1)

المحاضرة الخامسة

امن المعلومات (Information Security)

اعداد : م.م حيدر عبد الكريم الجنابي

امن المعلومات (Information Security)

أمان المعلومات يشير إلى الجهود والتدابير التي يتم اتخاذها لحماية المعلومات من التهديدات والمخاطر التي قد تعرضها للخطر. يتضمن أمان المعلومات الحفاظ على سرية وسلامة وتوفرية المعلومات، سواء كانت في صورة إلكترونية أو ورقية، وذلك من خلال تطبيق مجموعة من السياسات والإجراءات والتقنيات.

في سياق أمان المعلومات، تعتبر المعلومات أصولًا قيمة، سواء كانت تتعلق بالأفراد أو المؤسسات، ويهدف أمان المعلومات إلى حمايتها من الوصول غير المصرح به، والتلاعب، والتدمير غير المصرح به.

(اولا) جوانب أمان المعلومات

1. **السرية (Confidentiality):** ضمان عدم الوصول غير المصرح به للمعلومات. يتم ذلك عادةً عن طريق تحديد الوصول إلى المعلومات فقط للأشخاص المخولين.
2. **السلامة (Integrity):** ضمان سلامة المعلومات، معنى ذلك أن يكونوا آمنين من التلاعب أو التغيير غير المصرح به.
3. **التوفرية (Availability):** ضمان توفر المعلومات للأشخاص المخولين في الوقت الذي يحتاجونه إليه.
4. **المصداقية (Authenticity):** التحقق من هوية المستخدمين وتأكيد أن المعلومات لم تتعرض للتزوير.
5. **عدم امكانية الرفض (Non-repudiation):** تقديم دليل على أن شخص ما قام بإرسال رسالة أو إجراء عملية معينة ولا يمكنه نفي ذلك لاحقًا.

أمان المعلومات يتطلب التفكير بشكل شامل، يشمل السياسات والتقنيات والتدابير الإدارية لضمان حماية المعلومات بفعالية وفعالية.

(ثانيا) تصنيف المعلومات (Classification of information)

المعلومات تتنوع بشكل كبير، ويمكن تصنيفها بناءً على طبيعتها والتأثير الذي قد يكون لديها على الأفراد أو المؤسسات. وهذه بعض أنواع المعلومات الشائعة وكيفية تصنيفها حسب درجة سريتها:

1. **البيانات الشخصية:(Personal Data)**

- تشمل معلومات حول الأفراد، مثل الأسماء، وتواريخ الميلاد، وعناوين البريد الإلكتروني، وأرقام الهواتف، ومعلومات الهوية. يُعتبر تصنيف هذه البيانات عالية السرية لأنها تتعلق بخصوصية الأفراد.

2. **المعلومات المالية:(Financial Information)**

- تشمل بيانات حسابات البنوك، وبطاقات الائتمان، والمعلومات المالية الشخصية. تُعتبر عالية السرية بسبب طبيعتها الحساسة والتأثير الكبير على الأفراد.

3. **المعلومات الطبية:(Medical Information)**

- تتضمن سجلات الصحة الشخصية وتفاصيل العلاجات والحالات الطبية. تُصنف عادةً على أنها معلومات حساسة للغاية بسبب الطبيعة الشخصية لهذه المعلومات.

4. **المعلومات التجارية:(Business Information)**

- تشمل معلومات المؤسسات والشركات، مثل الخطط الاستراتيجية، والأسرار التجارية، والمعلومات المالية للشركات. تُصنف على أنها معلومات حساسة تحتاج إلى حماية.

5. **المعلومات الحكومية:(Government Information)**

- تتعلق بالمعلومات التي تخص الحكومات، مثل السجلات الضريبية، والمعلومات الجمركية، والبيانات الحكومية الأخرى. يجب حمايتها بشكل كبير لأسباب أمان وقانونية.

6. **المعلومات الفنية:(Technical Information)**

- تتعلق بالمعلومات التقنية، مثل رموز المصدر، والتصاميم، والبرمجيات. يمكن أن تكون عالية السرية للغاية بما أنها تشكل أصولًا تقنية تعطي للمؤسسات ميزة تنافسية.

تصنيف المعلومات حسب درجة سريتها يعتمد على عدة عوامل، بما في ذلك الطبيعة الحساسة للمعلومات، والتأثير المحتمل لفقدانها أو تسريبها على الأفراد أو المؤسسات. من المهم وضع سياسات أمان تتناسب مع نوعية المعلومات وحساسيتها لضمان حمايتها بشكل فعال

(ثالثا) تهديدات امن المعلومات

هناك بعض التهديدات الشائعة التي يمكن أن تواجهها المعلومات، مع التركيز على الهجمات الإلكترونية والبرمجيات الخبيثة:

1. **الهجمات الإلكترونية:(Cyber Attacks)**

- تتضمن محاولات غير مصرح بها لاختراق الأنظمة الإلكترونية للحصول على المعلومات أو تعطيل الخدمات. من أمثلة الهجمات الشائعة: هجمات التصيد (Phishing) ، والتصيد الهندسي (Social Engineering)، وهجمات نفي الخدمة.(DDoS)

2. **البرمجيات الخبيثة:(Malware)**

- تشمل أنواع مختلفة من البرمجيات الخبيثة مثل الفيروسات، وأحصنة طروادة (Trojans) ، وبرامج التجسس (Spyware) ، وبرمجيات الفدية .(Ransomware) تهدف هذه البرمجيات إلى التسلل إلى الأنظمة والتلاعب بالمعلومات أو طلب فدية.

3. **اختراق الشبكات:(Network Breaches)**

- يتمثل في اختراق الشبكات الحاسوبية للوصول غير المصرح به إلى المعلومات. قد يتم استخدام الثغرات الأمنية في الأنظمة أو هندسة الاجتياح (Intrusion Engineering) لتحقيق ذلك.

4. **تسريب البيانات:(Data Leaks)**

- يشير إلى خروج المعلومات الحساسة خارج النطاق المصرح به، سواء كان ذلك عن طريق الاختراق الإلكتروني أو خطأ بشري.

5. تهديدات البريد الإلكتروني:(Email Threats)

- تشمل الرسائل الاحتيالية (Phishing Emails) والرسائل الإلكترونية المصابة ببرمجيات خبيثة، والتي تهدف إلى خداع المستخدمين للنقر على روابط أو تحميل مرفقات ضارة.

6. الهجمات على البرمجيات:(Software Exploits)

- يستخدم المهاجمون الثغرات في البرمجيات للوصول إلى الأنظمة. قد يتم استغلال هذه الثغرات لتثبيت برمجيات خبيثة أو الحصول على السيطرة على النظام.

7. هجمات التصيد الاجتماعي:(Social Engineering Attacks)

- يتضمن التلاعب بالأفراد للحصول على المعلومات الحساسة، سواء عبر الهاتف أو البريد الإلكتروني، أو حتى شبكات وسائل التواصل الاجتماعي.

لحماية المعلومات من هذه التهديدات، يجب اتباع ممارسات أمان فعالة، مثل تحديث البرمجيات بانتظام، وتعزيز الوعي الأمني لدى المستخدمين، واستخدام تقنيات التشفير والحماية الشبكية.

(رابعا) تقنيات حماية المعلومات

تحمي التقنيات والأساليب المستخدمة لحماية المعلومات الأنظمة والبيانات من التهديدات الإلكترونية والاختراقات. ادناه بعض هذه التقنيات:

1. **التشفير:(Encryption)**

- التشفير هو عملية تحويل المعلومات إلى شكل غير قابل للقراءة دون وجود مفتاح فك التشفير المناسب. يحمي التشفير المعلومات أثناء النقل عبر الشبكات (encryption in transit) ، وأثناء تخزينها على الأجهزة والخوادم .(encryption at rest) يُعتبر استخدام البروتوكولات الآمنة مثل HTTPS للاتصال عبر الإنترنت نموذجًا لتشفير في النقل.

2. **الجدران النارية:(Firewalls)**

- الجدار الناري هو جهاز أو برنامج يقوم بتحديد من يمكن أن يتفاعل مع النظام أو الشبكة ومن يجب أن يتم رفض الوصول إليه. يعمل الجدار الناري على تصفية حركة المرور الواردة والصادرة بناءً على مجموعة من القواعد المحددة مسبقًا.

3. **برامج مكافحة الفيروسات:(Antivirus Software)**

- تعمل برامج مكافحة الفيروسات على الكشف وإزالة البرمجيات الخبيثة مثل الفيروسات وأحصنة الطروادة وبرامج التجسس. تقوم هذه البرامج بفحص الملفات والبرامج بشكل دوري للتأكد من عدم وجود تهديدات.

4. **أمان الشبكات:(Network Security)**

- تشمل تقنيات أمان الشبكات تحديد الوصول بشكل صارم، واستخدام الشهادات الأمانية، وتأمين الشبكات اللاسلكية (Wi-Fi) باستخدام تقنيات مثل WPA3 . Protected Access

5. **نظام اكتشاف التسلل:(Intrusion Detection System - IDS)**

- يراقب نظام اكتشاف التسلل الشبكة للاشتباه في الأنشطة غير المصرح بها أو الهجمات. عند اكتشاف شيء مشتبه فيه، يتم إصدار إنذار أو يتم اتخاذ إجراءات تلقائية.

6. **نظام منع التسلل:(Intrusion Prevention System - IPS)**

- يتمثل دور نظام منع التسلل في منع أو استمرار الهجمات الحية عند اكتشافها. يمكن أن يتم تنفيذ التصحيحات تلقائيًا أو بتوجيه من المسؤول.

7. **إدارة الهوية والوصول:(Identity and Access Management - IAM)**

- تتيح إدارة الهوية والوصول التحكم في من يمكنه الوصول إلى المعلومات. يتضمن ذلك تحديد الهويات، وتفويض الصلاحيات، ومتابعة الأنشطة.

8. **تحليل السلوك:(Behavioral Analysis)**

- يعتمد على رصد أنماط سلوك المستخدمين والأنظمة لتحديد أي نشاط غير عادي يمكن أن يكون علامة على هجوم أمان.

(خامسا) التدابير الامنية

لفهم أفضل لكيفية تطبيق التدابير الأمنية وتجارب حقيقية، يمكننا النظر إلى بعض الحالات العملية والدروس المستفادة:

1. **هجوم الفدية على شركة:**

- **الحالة :** تعرضت شركة لهجوم فدية، حيث تم تشفير بياناتها وطُلب فدية لفك التشفير.
- **الدرس :** أظهرت هذه الحالة أهمية النسخ الاحتياطي الدورية. قامت الشركة بفحص نظام النسخ الاحتياطي واستعادة البيانات بدون دفع فدية. تحفيز الموظفين على عدم فتح روابط أو مرفقات غير معروفة كان أحد التدابير المستفادة.

2. **تسريب بيانات موظفين:**

- **الحالة :** تسربت بيانات موظفين من خلال هجوم احتيال تصيد.
- **الدرس :** تم التأكيد على أهمية تدريب الموظفين على التعرف على هجمات التصيد وتوجيههم بشكل صحيح حول كيفية التحقق من هوية المرسلين قبل الاستجابة للطلبات.

3. **اختراق الشبكة:**

- **الحالة :** تم اختراق شبكة شركة عبر استغلال ثغرة في برنامج قديم لم يتم تحديثه.
- **الدرس :** أظهرت هذه الحالة أهمية تحديث البرمجيات بانتظام لسد الثغرات الأمنية. كما تم التأكيد على ضرورة مراقبة الشبكة بشكل دوري واستخدام أنظمة اكتشاف التسلل.

4. **تسريب بيانات العملاء:**

- **الحالة :** حدث تسريب لبيانات العملاء نتيجة للوصول غير المصرح به إلى قاعدة البيانات.
- **الدرس :** أظهرت هذه الحالة أهمية فحص وتقييم أمان التطبيقات وقواعد البيانات. تبين أيضًا أهمية تطبيق مبدأ الحاجة إلى معلومات الوصول.

5. **هجوم:DDoS**

- **الحالة :** تعرضت خدمة الويب لهجوم DDoS مما أدى إلى توقف الخدمة.
- **الدرس :** تبين أهمية استخدام خدمات مضادة للـ DDoS والتخطيط لمواجهة هجمات الحجب الخدمي للحفاظ على توفرية الخدمات.

من هذه الحالات، يمكن أن تكون الدروس المستفادة هي ضرورة تحديث البرمجيات وتدريب الموظفين بشكل دوري، وتطبيق تدابير الحماية على مختلف المستويات من الأنظمة والشبكات.