الأكاديمية العربية الدولية
Arab International Academy

إسم المادة: أمن معلومات البيانات

إسم المحاضِر: م. خليل المحمد

الأكاديمية العربية الدولية – منصة أعد

1- تعريف أمن المعلومات وأهميته

تعريف أمن المعلومات:

أمن المعلومات (Information Security)هو مجموعة من الممارسات والسياسات المصممة لحماية المعلومات من الوصول غير المصرح به، الاستخدام، الإفصاح، التعديل، أو الإتلاف. يتعامل أمن المعلومات مع حماية البيانات والمعلومات بغض النظر عن شكلها سواء كانت بيانات رقمية مخزنة على أجهزة الحاسوب أو أوراقًا مادية. يُعرف أمن المعلومات بأنه التزام بحماية "الثالوث الأمني" الذي يتكون من ثلاث مبادئ رئيسية:

- **السرية :(Confidentiality)** ضمان عدم كشف المعلومات إلا للأشخاص المصرح لهم بالوصول إليها.
- **السلامة :(Integrity)** التأكد من أن المعلومات لم تُعدل أو تُفسد بطرق غير مصرح بها أو غير مقصودة.
- **التوفر :(Availability)** ضمان أن المعلومات والنظم التي تعتمد عليها متاحة في أي وقت عند الحاجة إليها.

أهمية أمن المعلومات:

- **حماية البيانات الحساسة :**سواء كانت معلومات شخصية أو بيانات مالية أو بيانات أعمال، يعد الحفاظ على سريتها وسلامتها أمرًا حاسمًا.
- **الامتثال للتشريعات :**تفرض العديد من القوانين والتشريعات حول العالم على المؤسسات ضرورة حماية بيانات عملائها، مثل قانون GDPR في الاتحاد الأوروبي.
- **منع الخسائر المالية :**يمكن أن تؤدي الهجمات الإلكترونية إلى خسائر مالية كبيرة للمؤسسات، سواء من خلال الابتزاز أو فقدان البيانات أو توقف الأعمال.

تطور أمن المعلومات عبر التاريخ

- **المرحلة البدائية :**كان التشفير البسيط مثل شيفرة قيصر (Caesar Cipher) هو الأسلوب السائد لحماية المعلومات الحساسة في العصور القديمة.
- **الشيفرات اليدوية :**كانت الحكومات والجيوش تستخدم أساليب تشفير لتبادل الرسائل السرية. لكن هذه الأساليب كانت بدائية ومحدودة، وتستند غالبًا إلى تغييرات بسيطة في النصوص.
- **العصور الوسطى: الشيفرات المعقدة :**في العصور الوسطى، بدأ استخدام شيفرات أكثر تعقيدًا مع تطور العمليات العسكرية والسياسية. كانت الوثائق السرية تُحفظ في صناديق مقفلة وتُرسل باستخدام رسل موثوقين. ومع ذلك، كان هناك دائمًا مخاطر فقدان الرسائل أو سرقتها.
- **القرن العشرين :**مع تطور الحوسبة وظهور الشبكات، ازدادت الحاجة إلى تقنيات أكثر تقدمًا لحماية المعلومات. خلال الحرب العالمية الثانية، تم تطوير آلات التشفير المعقدة مثل "إنجما" لحماية المعلومات العسكرية.
- **العصر الرقمي :**مع انتشار الإنترنت، زادت الهجمات الإلكترونية بشكل كبير، مما دفع الشركات والحكومات إلى تطوير أنظمة أمان متقدمة. ظهرت بروتوكولات الأمان مثل SSL وتشفير المفتاح العام لتأمين البيانات المرسلة عبر الإنترنت.
- **الأمن السيبراني الحديث :**في العقود الأخيرة، زادت الهجمات الإلكترونية تطورًا وخطورة. ومع ظهور الحوسبة السحابية والذكاء الاصطناعي، أصبح من الضروري تطوير تقنيات أمنية متقدمة مثل التعلم الآلي للكشف عن التهديدات وتشفير البيانات بشكل أكثر تعقيدًا.

المفاهيم الأساسية: الخصوصية Confidentiality

الخصوصية(Confidentiality) : هي حماية المعلومات من الوصول غير المصرح به. الهدف من الخصوصية هو التأكد من أن المعلومات متاحة فقط للأفراد أو الأنظمة المخولين بالوصول إليها.

- **أهمية الخصوصية:**
  - في العالم الرقمي، تُعتبر حماية الخصوصية أمرًا بالغ الأهمية، خاصة مع تزايد البيانات الحساسة مثل المعلومات الشخصية (PII) والمعلومات المالية والصحية. المؤسسات تُلزم قانونيًا بضمان حماية هذه المعلومات.
  - الحفاظ على الخصوصية يمنع **التجسس الصناعي** أو **سرقة الهوية**، حيث يمكن للمهاجمين استخدام هذه البيانات لأغراض غير مشروعة.
- **أساليب حماية الخصوصية:**
  - **التشفير :**تقنية تُستخدم لترميز المعلومات بحيث لا يمكن قراءتها إلا من قبل الأطراف المخولين.
  - **التحكم في الوصول :**يسمح فقط للمستخدمين المصرح لهم بالوصول إلى المعلومات. ويشمل ذلك استخدام كلمات المرور، نظم المصادقة الثنائية، والبطاقات الذكية.
  - **التقسيم الأمني :**يتم تقسيم الأنظمة والشبكات إلى مناطق مختلفة، بحيث لا يمكن الوصول إلى المناطق الأكثر حساسية إلا للمستخدمين المصرح لهم.

المفاهيم الأساسية: السلامة Integrity

السلامة(Integrity) : تعني التأكد من أن المعلومات لم تتعرض للتعديل أو التلف بطريقة غير مصرح بها. وهي تضمن أن البيانات تظل دقيقة وكاملة ولا يتم تغييرها أثناء النقل أو التخزين إلا من قبل الأشخاص المخولين.

- **أهمية السلامة:**
  - الحفاظ على السلامة يضمن موثوقية وصحة المعلومات. هذا مهم في البيئات المالية والطبية، حيث يمكن أن يؤدي أي تعديل غير مصرح به إلى نتائج خطيرة.
  - الهجمات التي تستهدف سلامة البيانات، مثل **التلاعب بالبيانات** أو **هجمات الإنسان في المنتصف(Man-in-the-Middle)** ، يمكن أن تكون مدمرة إذا لم يتم اكتشافها.
- **أساليب حماية السلامة:**
  - **التوقيع الرقمي :** هو رمز يتم إرفاقه بالبيانات لضمان أن هذه البيانات لم تتغير منذ أن تم توقيعها.
  - **تجزئة البيانات :(Hashing)** يتم استخدام خوارزميات تجزئة لتوليد قيمة فريدة لكل مجموعة بيانات. إذا تم تعديل البيانات، تتغير قيمة التجزئة، مما يسهل اكتشاف التلاعب.
  - **أنظمة التحكم في النسخ :** تُستخدم لضمان وجود نسخ احتياطية من البيانات في حال تعرضت للتلف أو التعديل.

المفاهيم الأساسية: التوفر Availability

التوفر(Availability) : يعني ضمان أن المعلومات والخدمات المتعلقة بها متاحة بشكل مستمر للمستخدمين المصرح لهم عند الحاجة إليها. الهدف من التوفر هو تقليل الأعطال والتأكد من استمرارية الوصول إلى البيانات والأنظمة حتى في حال وقوع كوارث أو هجمات.

- **أهمية التوفر:**
  - توفر الأنظمة هو جزء حيوي من العمليات اليومية للأفراد والمؤسسات. تعطيل الأنظمة يمكن أن يؤدي إلى توقف العمليات أو فقدان الإيرادات.
  - الهجمات التي تستهدف التوفر، مثل **هجمات حجب الخدمة الموزعة(DDoS)** ، يمكن أن تسبب خسائر كبيرة وتؤدي إلى انقطاع الخدمات.
- **أساليب ضمان التوفر:**
  - **النسخ الاحتياطي والاستعادة :**يتم الاحتفاظ بنسخ احتياطية من البيانات على فترات زمنية منتظمة للتأكد من أنه يمكن استعادتها في حالة الفقد أو التلف.
  - **التكرار :(Redundancy)** يتم استخدام معدات أو أنظمة احتياطية للتأكد من استمرار الخدمة في حالة حدوث فشل في النظام الرئيسي.
  - **التخطيط للطوارئ :**يشمل إعداد خطط استمرارية العمل (BCP) وخطط التعافي من الكوارث (DRP) لضمان استمرارية العمليات حتى في ظل الكوارث أو الهجمات السيبرانية.

2- التهديدات والمخاطر الأمنية

1. **الفيروسات(Viruses) :** هي نوع من البرمجيات الضارة التي تقوم بإصابة الملفات والبرامج وتكرار نفسها داخل النظام, وتنتشر من خلال:
   - **البريد الإلكتروني :**حيث يتم إرفاق الفيروس برسائل البريد الإلكتروني الخبيثة.
   - **التنزيلات غير الآمنة :**مثل البرامج غير الموثوقة أو الملفات المحملة من الإنترنت.
   - **الأجهزة القابلة للإزالة :**كالأقراص الصلبة أو مفاتيح USB المصابة.
2. **هجمات القرصنة(Hacking Attacks) :** هي محاولة الوصول غير المصرح به إلى الأنظمة والبيانات، وغالبًا ما يتم تنفيذها من خلال:
   - **استغلال الثغرات الأمنية :**في البرمجيات أو الشبكات، حيث يستغل القراصنة نقاط الضعف في النظام.
   - **الهجمات المستهدفة :**مثل هجمات **Man-in-the-Middle**أو **SQL Injection** التي تهدف إلى اختراق النظام والحصول على البيانات.
3. **برامج الفدية(Ransomware) :** هي نوع من البرمجيات الضارة التي تقوم بتشفير بيانات المستخدم أو النظام وتطالب بفدية مالية مقابل فك التشفير.
   - **تشفير البيانات الحساسة :**حيث يتم إغلاق الوصول إلى الملفات أو الأنظمة المصابة.
   - **طلب فدية :**يتم إبلاغ الضحية بمطالبة مالية عبر رسالة تظهر على الشاشة، ويُطلب الدفع عبر وسائل غير قابلة للتتبع مثل العملات الرقمية.

التصيد الاحتيالي

التصيد الاحتيالي (Phishing) : هو نوع من الهجمات الإلكترونية التي تهدف إلى سرقة المعلومات الحساسة من الأفراد، مثل بيانات تسجيل الدخول أو المعلومات المالية، من خلال تقنيات احتيالية تخدع المستخدمين للكشف عن معلوماتهم. يتم ذلك عادة عبر رسائل مزيفة تبدو وكأنها من مصادر موثوقة، مثل البنوك أو مواقع التواصل الاجتماعي.

أنواع التصيد الاحتيالي:

- **التصيد عبر البريد الإلكتروني :**يتم إرسال رسائل بريد إلكتروني تبدو شرعية وتطلب من الضحية النقر على رابط يقود إلى موقع وهمي يطلب إدخال المعلومات الشخصية.
- **التصيد الاحتيالي المتقدم :(Spear Phishing)** يستهدف أفرادًا أو مؤسسات محددة باستخدام معلومات شخصية لجعل الهجوم يبدو أكثر واقعية. غالبًا ما يكون هدف هذا النوع من الهجمات هو كبار الموظفين أو الأشخاص الذين يملكون صلاحيات حساسة.
- **التصيد عبر الرسائل النصية :(Smishing)** يتم عبر الرسائل النصية القصيرة، حيث تحتوي الرسالة على رابط خبيث أو طلب للحصول على معلومات حساسة.

كيفية الحماية من التصيد الاحتيالي:

- **تجنب النقر على الروابط المشبوهة :**يجب الحذر من الروابط الموجودة في الرسائل غير المتوقعة أو غير الموثوقة.
- **استخدام المصادقة الثنائية :(2FA)** تساعد هذه الطبقة الإضافية من الأمان على حماية الحسابات حتى لو سُرقت كلمة المرور

هجمات الهندسة الاجتماعية

هجمات الهندسة الاجتماعية (Social Engineering) : هي استراتيجية هجوم تعتمد على استغلال العوامل النفسية والمشاعر الإنسانية، مثل الثقة أو الاستعجال، للحصول على معلومات سرية أو الوصول إلى أنظمة مؤمنة. يهدف المهاجمون إلى خداع الأفراد للكشف عن بيانات حساسة أو تقديم معلومات قد تساعد في تنفيذ هجوم أكبر.

أنواع هجمات الهندسة الاجتماعية:

- **الهجمات الهاتفية (Pretexting):** يتصل المهاجم بالضحية مدعيًا أنه شخص موثوق (مثل موظف دعم فني أو مسؤول في الشركة) ويطلب منهم الكشف عن معلومات حساسة.
- **هجمات الطعم (Baiting):** يستخدم المهاجمون أجهزة مثل أقراص USB المصابة بالبرمجيات الضارة ويتركونها في أماكن عامة، على أمل أن يلتقطها أحدهم ويقوم بتوصيلها إلى جهازه.
- **التنكر (Impersonation):** يتظاهر المهاجم بأنه موظف داخلي أو عميل خارجي للحصول على معلومات سرية أو الوصول إلى النظام.

كيفية الحماية من هجمات الهندسة الاجتماعية:

- **التدريب على الوعي الأمني:** يجب تعليم الموظفين كيف يميزون الهجمات الخادعة وعدم الثقة بأي طلبات غير معتادة للكشف عن معلومات.
- **التأكد من هوية المتصل:** يجب التحقق من هوية الشخص الذي يطلب معلومات حساسة عبر القنوات الرسمية قبل تزويده بأي معلومات.

التهديدات الداخلية: الموظفون

التهديدات الداخلية(Insider Threats) :

التهديدات الداخلية هي الهجمات أو التسريبات الأمنية التي تحدث من داخل المؤسسة، على يد الموظفين أو المتعاقدين أو أي شخص لديه وصول مشروع إلى نظم المعلومات. غالبًا ما يكون الموظفون على دراية جيدة بالبنية التحتية الداخلية للشركة وبياناتها الحساسة، ما يجعل هذه الهجمات أكثر خطورة وصعوبة في الكشف عنها مقارنة بالهجمات الخارجية.

أنواع التهديدات الداخلية:

- **الموظفون الخبيثون :(Malicious Insiders)** هؤلاء هم الأفراد الذين يستغلون صلاحياتهم في الوصول إلى الأنظمة لسرقة بيانات حساسة أو إلحاق الضرر بالشركة. قد يكون هذا التصرف نتيجة للسخط، أو لأغراض مالية أو انتقامية.
- **الموظفون غير المقصودين :(Unintentional Insiders)** هؤلاء الموظفون لا يسعون عمدًا إلى إلحاق الضرر بالشركة، ولكنهم قد يتسببون في تسريبات أو تهديدات بسبب قلة المعرفة أو الإهمال، مثل النقر على روابط تصيد احتيالي أو إرسال معلومات حساسة عبر قنوات غير آمنة.

التهديدات الداخلية: التسريبات

التسريبات(Data Leaks) : تحدث عندما يتم الكشف عن بيانات حساسة أو نقلها بطريقة غير مصرح بها خارج المؤسسة. قد تحدث التسريبات نتيجة للخطأ البشري أو البرمجيات الخبيثة أو حتى بسبب الإجراءات غير الملائمة للموظفين.

أنواع التسريبات:

- **التسريبات العرضية :(Accidental Leaks)** مثل إرسال بريد إلكتروني يحتوي على بيانات حساسة إلى المستلم الخطأ أو تحميل الملفات إلى خوادم غير مؤمنة.
- **التسريبات المقصودة :(Intentional Leaks)** وهي تسريبات متعمدة، حيث يقوم شخص من داخل المؤسسة بنقل أو بيع البيانات الحساسة لمصالحه الشخصية أو لشركات منافسة.

أمثلة على التسريبات:

- **تسريب مستندات سرية :**يمكن أن يؤدي نقل الملفات إلى خدمات تخزين سحابية غير آمنة أو نسخ المستندات إلى أجهزة خارجية إلى فقدان البيانات.
- **مشاركة كلمات المرور :**أحد أكثر الطرق الشائعة للتسريب هو مشاركة كلمات المرور أو تركها في أماكن يسهل الوصول إليها، مما يسمح للآخرين بالوصول غير المصرح به إلى الأنظمة.

3- تقنيات التشفير

التشفير هو أحد أهم الأساليب المستخدمة لحماية البيانات والمعلومات من الوصول غير المصرح به.

أنواع التشفير:

- **التشفير المتماثل (Symmetric Encryption):** في هذا النوع من التشفير، يتم استخدام نفس المفتاح لتشفير وفك تشفير البيانات. يُعتبر التشفير المتماثل أسرع من غيره، ولكنه يتطلب أن يتم تأمين المفتاح المستخدم بعناية لأنه يتم تبادله بين الأطراف.

  أشهر خوارزميات التشفير المتماثل:

  - **AES (Advanced Encryption Standard)** يُستخدم على نطاق واسع ويُعد من أكثر الخوارزميات أمانًا.
  - **DES (Data Encryption Standard)** كان يستخدم في الماضي، لكنه الآن يعتبر غير آمن نظرًا لقصر طوله النسبي للمفتاح (56 بت).
- **التشفير غير المتماثل (Asymmetric Encryption):** يُعرف أيضًا بتشفير المفتاح العام، وفيه يتم استخدام مفتاحين مختلفين: مفتاح عام للتشفير ومفتاح خاص لفك التشفير. **أشهر خوارزميات التشفير غير المتماثل:**

  - **RSA (Rivest-Shamir-Adleman)** إحدى أقدم الخوارزميات المستخدمة في التشفير غير المتماثل وتُعتبر من أقوى الأنظمة.
  - **ECC (Elliptic Curve Cryptography)** تستخدم معادلات رياضية تعتمد على المنحنيات البيضاوية وتوفر أمانًا عاليًا مع مفاتيح أصغر مقارنة بـ RSA.

خوارزميات التشفير

خوارزميات التشفير هي مجموعات من القواعد الرياضية والإجراءات التي تُستخدم لتحويل البيانات من نص صريح إلى نص مشفر، والعكس. تنقسم خوارزميات التشفير إلى نوعين رئيسيين: تشفير المفتاح العام (Asymmetric Encryption) وتشفير المفتاح الخاص Symmetric Encryption

تشفير المفتاح العام والمفتاح الخاص:

1- تشفير المفتاح العام (Asymmetric Encryption)

تعريف :تشفير المفتاح العام، المعروف أيضًا بتشفير المفتاح غير المتماثل، يستخدم زوجًا من المفاتيح: مفتاح عام للتشفير ومفتاح خاص لفك التشفير. يمكن لأي شخص استخدام المفتاح العام لتشفير البيانات، ولكن فقط المالك للمفتاح الخاص يمكنه فك التشفير.

2- تشفير المفتاح الخاص(Symmetric Encryption)

تعريف :تشفير المفتاح الخاص هو نظام يستخدم مفتاحًا واحدًا للتشفير وفك التشفير. هذا يعني أن نفس المفتاح الذي يُستخدم لتشفير البيانات هو المفتاح الذي يُستخدم لفك تشفيرها.

التطبيقات العملية لخوارزميات التشفير:

- تأمين الاتصالات: تُستخدم في تأمين بروتوكولات الإنترنت مثل HTTPS.
- توقيع رقمي: يستخدم التشفير غير المتماثل لإنشاء توقيع رقمي يُثبت هوية المرسل.
- حماية البيانات المخزنة: يُستخدم التشفير المتماثل لحماية البيانات المخزنة على الأجهزة.

التوقيعات الرقمية

التوقيعات رقمية : هو تقنية تستخدم لتأكيد هوية المرسل ولضمان سلامة البيانات المرسلة. يعمل التوقيع الرقمي على تطبيق خوارزميات التشفير غير المتماثلة، مما يضمن أن البيانات لم تتعرض للتلاعب أثناء نقلها.

كيفية العمل:

1. **إنشاء المفتاح :**يتم إنشاء زوج من المفاتيح، مفتاح خاص ومفتاح عام. يحتفظ المرسل بالمفتاح الخاص بينما يمكن توزيع المفتاح العام بحرية.
2. **توقيع الرسالة :**عندما يقوم المرسل بتوقيع رسالة، يتم تطبيق خوارزمية هاش (Hash Algorithm) على محتوى الرسالة لإنتاج ملخص (hash) للبيانات. ثم يتم تشفير هذا الملخص باستخدام المفتاح الخاص للمرسل، مما ينتج عنه التوقيع الرقمي.
3. **إرسال الرسالة :**يتم إرسال الرسالة مع التوقيع الرقمي.
4. **التحقق :**يمكن للمستلم استخدام المفتاح العام للمرسل لفك تشفير التوقيع والتحقق من أن الملخص الذي تم إنشاؤه يتطابق مع الملخص الذي تم إنشاؤه من الرسالة المستلمة.

استخدامات التوقيع الرقمي:

- **التحقق من الهوية :**تستخدم في توقيع المستندات القانونية والعقود.
- **تأمين الاتصالات :**تستخدم في تأمين البريد الإلكتروني والتطبيقات التي تتطلب تبادل بيانات حساسة.

شهادات SSL

شهادة (Secure Sockets Layer) SSL هي مستند رقمي يُستخدم لتأكيد هوية موقع ويب وتأمين الاتصالات بين المتصفح والخادم.

كيفية العمل:

1. **إصدار الشهادة :**يتم إصدار شهادة SSL من قبل جهة موثوقة تُعرف بمركز التصديق .(Certificate Authority - CA) يقوم مركز التصديق بالتحقق من هوية الموقع قبل إصدار الشهادة.
2. **تثبيت الشهادة :**بعد الحصول على الشهادة، يتم تثبيتها على الخادم.
3. **تأمين الاتصالات :**عندما يحاول المستخدم الاتصال بالموقع، يقوم المتصفح بإجراء اتصال آمن باستخدام بروتوكول .HTTPS يتم تبادل الشهادة بين المتصفح والخادم، مما يتيح للمستخدم التحقق من هوية الموقع.
4. **تشفير البيانات :**يتم تشفير البيانات المتبادلة بين المتصفح والخادم باستخدام خوارزميات التشفير، مما يمنع أي طرف ثالث من الوصول إلى المعلومات الحساسة.

أنواع شهادات:SSL

- **شهادات :DV (Domain Validation)** للتحقق من ملكية النطاق فقط.
- **شهادات :OV (Organization Validation)** للتحقق من هوية المنظمة.
- **شهادات :EV (Extended Validation)** تقدم أعلى مستوى من التحقق، مما يوفر مستوى عالٍ من الثقة للمستخدمين.

4- نظم التحكم في الوصول

تعريف نظم التحكم في الوصول: (Access Control Systems هي مجموعة من السياسات والإجراءات التي تُستخدم للتحكم في الوصول إلى الموارد والبيانات في الأنظمة المعلوماتية. تهدف هذه النظم إلى حماية المعلومات والموارد الحساسة من الوصول غير المصرح به.

أنواع نظم التحكم في الوصول

1- التحكم القائم على الهوية (Identity-Based Access Control) : هذا النوع يعتمد على هوية المستخدم. يُمنح كل مستخدم حق الوصول بناءً على معلومات تعريفه، مثل اسم المستخدم وكلمة المرور. يتم تنفيذ التحكم من خلال:

- **إجراءات التحقق :**مثل إدخال اسم المستخدم وكلمة المرور.
- **تحديد الأذونات :**يمكن لكل مستخدم أن يمتلك مجموعة محددة من الأذونات بناءً على دوره في المؤسسة.

2- التحكم القائم على الدور (Role-Based Access Control - RBAC) : نظام التحكم هذا يعتمد على الأدوار التي يشغلها الأفراد في المؤسسة. يتم تحديد الأذونات بناءً على الدور وليس على مستوى المستخدم الفردي. يُعد هذا النظام مثاليًا للمؤسسات الكبيرة، حيث يسهل إدارة الأذونات. تشمل مميزاته:

- **تسهيل إدارة الأذونات :**من السهل إضافة أو إزالة أذونات بناءً على تغييرات في الأدوار.
- **تقليل الأخطاء :**يقلل من احتمال منح أذونات غير صحيحة للمستخدمين.

.

أهمية نظم التحكم في الوصول

3- التحكم القائم على الخصائص(Attribute-Based Access Control - ABAC)

يعتمد هذا النوع من نظم التحكم على مجموعة من الخصائص أو السمات. يتم تحديد الأذونات بناءً على معايير محددة، مثل الموقع الجغرافي، الوقت، أو نوع الجهاز. تتضمن مميزاته:

- **مرونة عالية :**يسمح بتطبيق سياسات معقدة وفقًا للمتطلبات المختلفة.
- **تخصيص الوصول :**يمكن تخصيص الوصول بشكل دقيق جدًا بناءً على مجموعة متنوعة من الخصائص.

<u>أهمية نظم التحكم في الوصول</u>

- **حماية المعلومات الحساسة :**تساعد في حماية البيانات الحساسة مثل المعلومات المالية والشخصية من الوصول غير المصرح به.
- **تقليل المخاطر :**تساهم في تقليل مخاطر التهديدات الداخلية والخارجية من خلال التحكم الدقيق في من يمكنه الوصول إلى الموارد.
- **الامتثال للمعايير :**تُساعد المؤسسات في الامتثال للمعايير والقوانين المتعلقة بحماية البيانات.
- **تعزيز الثقة :**تُعزز نظم التحكم في الوصول الثقة بين العملاء والمستخدمين، حيث يشعرون بأن بياناتهم محمية بشكل جيد.

تحديد الهوية والمصادقة

تحديد الهوية Identity: هو عملية التعرف على هوية المستخدم. يُعتبر أول خطوة في تأمين أي نظام معلوماتي، حيث يتم خلالها إدخال المستخدم لمعلومات تعريفية.

العناصر الأساسية لتحديد الهوية:

معلومات تعريفية: تشمل اسم المستخدم، البريد الإلكتروني، أو رقم الهوية. **أنظمة إدارة الهوية:** تُستخدم لتخزين معلومات الهوية وتنظيمها، مثلActive Directory

المصادقة Authentication: هي العملية التي يتم من خلالها التحقق من صحة هوية المستخدم الذي تم تحديده. تُستخدم المصادقة لتأكيد أن الشخص الذي يدعي أنه هو، هو في الواقع هو، ويُعتبر جزءًا أساسيًا من حماية البيانات. **طرق المصادقة:** توجد عدة طرق شائعة للمصادقة، تشمل:

1- **المصادقة الأحادية (Single-Factor Authentication) :** تعتمد على طريقة واحدة للتحقق من الهوية، مثل كلمة المرور. تعتبر هذه الطريقة بسيطة وسهلة الاستخدام، لكنها ليست الأكثر أمانًا.

2- **المصادقة الثنائية (Two-Factor Authentication - 2FA) :** تتطلب المصادقة الثنائية تقديم عاملين للتحقق من الهوية. يمكن أن يكون العامل الثاني شيئًا تعرفه (كلمة مرور) وشيء تملكه (مثل رمز يتم إرساله إلى هاتفك المحمول).

3- **المصادقة المتعددة (Multi-Factor Authentication - MFA) :** تشبه المصادقة الثنائية، لكنها تتطلب أكثر من عاملين للتحقق من الهوية.

4- **المصادقة البيومترية:** تعتمد على القياسات البيولوجية للمستخدم، مثل بصمات الأصابع، التعرف على الوجه، أو قزحية العين.

إدارة الحقوق والصلاحيات ABAC

1- **نموذج التحكم القائم على السمات (ABAC) :** ABAC (Attribute-Based Access Control) يعتمد على مجموعة من السمات أو الخصائص لتحديد الأذونات. يتيح هذا النموذج التحكم في الوصول بشكل أكثر دقة ومرونة، مما يجعله مناسبًا للبيئات الديناميكية.

كيفية العمل:

1. **تحديد السمات :** يتم تحديد مجموعة من السمات التي قد تشمل الخصائص الشخصية للمستخدم (مثل الموقع أو القسم)، وسمات الموارد (مثل نوع البيانات أو حساسية المعلومات)، وسياقات الوصول (مثل الوقت أو طريقة الاتصال).
2. **تحديد السياسات :** يتم إنشاء سياسات تحدد كيفية استخدام هذه السمات لتحديد ما إذا كان يجب السماح بالوصول أم لا.
3. **تقييم الأذونات :** عند محاولة المستخدم الوصول إلى مورد، يتم تقييم السياسات بناءً على السمات المحددة.

مزايا:ABAC

- **مرونة عالية :** يتيح تخصيص الوصول بناءً على مجموعة متنوعة من السمات.
- **دقة:** يمكن أن تكون السياسات معقدة، مما يسمح بتحديد دقيق جدًا للأذونات.
- **ملاءمة للبيئات الديناميكية :** يتناسب بشكل جيد مع البيئات التي تتغير فيها الأذونات بشكل متكرر.

إدارة الحقوق والصلاحيات RBAC

2- **نموذج التحكم القائم على الدور(RBAC) :** RBAC (Role-Based Access Control) يعتمد على توزيع الأذونات بناءً على الأدوار التي يشغلها المستخدمون داخل المؤسسة. يُعتبر هذا النموذج من أكثر النماذج شيوعًا وفعالية في إدارة الحقوق والصلاحيات.

كيفية العمل:

1. **تحديد الأدوار :**يتم تحديد مجموعة من الأدوار داخل المؤسسة، مثل المدير، الموظف، أو المحاسب.
2. **تعيين الأذونات :**يتم تعيين الأذونات لكل دور، مما يحدد ما يمكن للمستخدمين القيام به بناءً على دورهم.
3. **تعيين المستخدمين للأدوار :**يتم تعيين كل مستخدم لدور محدد، مما يضمن أن لديهم الأذونات المناسبة.

مزايا:RBAC

- **إدارة مبسطة :**يسهل إدارة الأذونات، خاصة في المؤسسات الكبيرة.
- **تقليل الأخطاء :**يقلل من إمكانية منح أذونات غير صحيحة، حيث يتم تحديد الأذونات مسبقًا لكل دور.
- **زيادة الأمان :**يساهم في تعزيز الأمان من خلال تقييد الوصول بناءً على الأدوار المحددة.

أنظمة الكشف عن التسلل IDS

أنظمة الكشف عن التسلل (Intrusion Detection Systems) هي أدوات مصممة لمراقبة الشبكات أو الأنظمة لاكتشاف الأنشطة غير الطبيعية أو الهجمات المحتملة. تعمل هذه الأنظمة على تحليل حركة المرور وتسجيل الأحداث في بيئة المعلومات.

أنواع:IDS

1. **أنظمة الكشف على الشبكة:(NIDS) :** تراقب حركة المرور عبر الشبكة بالكامل. تحلل البيانات في الوقت الحقيقي وتكتشف الأنشطة المشبوهة.
2. **أنظمة الكشف على المضيف:(HIDS) :** تراقب أنشطة المضيف الفردي (مثل الخوادم أو أجهزة الكمبيوتر). تركز على ملفات السجل وسلوك النظام لتحليل الأنشطة.

كيفية العمل: تعمل أنظمة IDS على تحليل البيانات بناءً على قواعد معرفية مسبقة أو عن طريق اكتشاف الأنماط. عند اكتشاف نشاط مشبوه، يتم تسجيل الحادث وتنبيه المسؤولين.

مزايا:IDS

- **الكشف المبكر :**توفر إنذار مبكر عن التهديدات المحتملة. **تحليل دقيق :**تسمح بتحليل دقيق لحركة المرور ونشاط النظام.
- **توفير سجلات للأحداث :**تتيح للمسؤولين مراجعة الأحداث وتحليل الهجمات.

أنظمة منع التسلل IPS

أنظمة منع التسلل (IPS) : أنظمة منع التسلل (Intrusion Prevention Systems) هي تقنيات تستخدم لرصد وتحليل حركة المرور الشبكية، ولكنها تختلف عن IDS في قدرتها على اتخاذ إجراءات فورية لمنع الهجمات.

كيفية العمل: تعمل أنظمة IPS على مراقبة البيانات بنفس طريقةIDS ، ولكنها تقوم أيضًا بتحليل حركة المرور وتطبيق السياسات الأمنية. عند اكتشاف هجوم، يمكنها إيقاف حركة المرور الضارة، منع الوصول إلى الموارد، أو إجراء عمليات أخرى للحماية.

أنواع:IPS

1. **IPS على الشبكة:(NIPS) :** يتواجد في نقاط معينة داخل الشبكة لتحليل حركة المرور ومنع الهجمات.
2. **IPS على المضيف:(HIPS) :** تعمل على مستوى النظام الفردي لحماية الخوادم أو الأجهزة من الهجمات.

مزايا:IPS : **استجابة سريعة :**توفر ردود فعل فورية على التهديدات. **تقليل الضرر :**تساعد في تقليل الأضرار الناتجة عن الهجمات عبر منعها في الوقت الحقيقي. **تحسين الأمان العام :**تعزز الأمان من خلال الكشف والرد السريع.

عيوب:IPS : **إمكانية الخطأ :**قد تتسبب في حظر حركة مرور شرعية عن طريق الخطأ (الإنذارات الكاذبة). **التعقيد :**تتطلب تكوينًا وإدارة دقيقة لضمان فعاليتها.

5- أمن الشبكات

أمن الشبكات هو فرع من فروع أمن المعلومات يركز على حماية الشبكات والبيانات المنقولة عبرها من التهديدات والهجمات.

أهداف أمن الشبكات:

- **حماية البيانات :**ضمان سلامة وسرية البيانات المرسلة والمستقبلة عبر الشبكة. **التوفر :**التأكد من أن الشبكة متاحة للاستخدام من قبل المستخدمين المصرح لهم.
- **التكامل :**حماية البيانات من التعديل غير المصرح به. **المراقبة :**تتبع الأنشطة داخل الشبكة لرصد التهديدات والاستجابة لها بشكل سريع.

مكونات أمن الشبكات:

أ .**الجدران النارية:(Firewalls) :** تعمل كحاجز أمني بين الشبكة الداخلية والخارجية، حيث تقوم بتصفية حركة المرور استنادًا إلى قواعد محددة. يمكن أن تكون الجدران النارية على مستوى الشبكة أو المضيف.

ب .**أنظمة الكشف ومنع التسلل:(IDS/IPS) :** كما تم ذكرها سابقًا، تساعد في مراقبة وتحليل حركة المرور واكتشاف ومنع التهديدات.

ج .**التشفير:** استخدام تقنيات التشفير لحماية البيانات المرسلة عبر الشبكات. يعتبر التشفير أحد أهم أدوات حماية البيانات الحساسة.

د) **VPN** .**الشبكة الافتراضية الخاصة :** تسمح بتأمين الاتصالات عبر الإنترنت، حيث تقوم بإنشاء نفق مشفر لنقل البيانات، مما يحمي البيانات من التجسس.

هـ .**التوثيق والمصادقة:** التأكد من أن المستخدمين الذين يحاولون الوصول إلى الشبكة هم فعلاً من يُفترض بهم الوصول. تشمل هذه العملية استخدام كلمات المرور، وبطاقات الهوية، وأنظمة المصادقة متعددة العوامل.

جدران الحماية

تُعتبر جدران الحماية (Firewalls) من العناصر الأساسية في أمان الشبكات، حيث تلعب دورًا محوريًا في حماية الأنظمة والشبكات من التهديدات السيبرانية.

أنواع جدران الحماية

أ. **جدران الحماية المادية:** هي أجهزة مخصصة توضع بين الشبكة الداخلية والاتصال الخارجي. تعمل على فحص البيانات وتصفية حركة المرور بناءً على القواعد المحددة.

ب. **جدران الحماية البرمجية:** هي تطبيقات تُثبت على أجهزة الكمبيوتر أو الخوادم، وتعمل على مراقبة حركة المرور الداخلية والخارجية.

آلية عمل جدران الحماية: تعمل جدران الحماية على تحليل حركة المرور باستخدام مجموعة من القواعد المسبقة التي تحدد ما إذا كان يجب السماح بالبيانات أو حظرها. تشمل بعض الأساليب الشائعة المستخدمة في جدران الحماية:

- **تصفية الحزم (Packet Filtering):** تقوم بفحص كل حزمة بيانات تمر عبر جدار الحماية، وتحدد ما إذا كانت تستوفي الشروط المحددة في القواعد أم لا.
- **التفتيش المتعمق للحزم (Deep Packet Inspection):** تفحص محتوى الحزم في عمق أكبر، مما يسمح بالكشف عن التهديدات المتطورة.
- **تصفية الحالة (Stateful Filtering):** تتعقب حالة الاتصال وتسمح فقط بحركة المرور التي تُظهر سلوكًا متسقًا ومصرحًا به.

تقنيات الشبكات الافتراضية الخاصة VPN

تعريف الشبكة الافتراضية الخاصة(VPN) : هي تقنية تتيح للمستخدمين إنشاء اتصال آمن ومشفر عبر شبكة غير آمنة، مثل الإنترنت.

آلية عمل الشبكة الافتراضية الخاصة : تعمل VPN على نقل البيانات من جهاز المستخدم إلى خادمVPN ، حيث يتم تشفير البيانات أثناء العملية. تشمل مراحل العمل الأساسية ما يلي:

- **التشفير :**تُشفر البيانات باستخدام بروتوكولات التشفير، مما يحمي المعلومات من الاعتراض.
- **النفق :**يتم إنشاء نفق افتراضي يربط بين المستخدم وخادمVPN ، مما يمنع أي طرف ثالث من رؤية البيانات المرسلة.
- **إعادة التوجيه :**يتم توجيه حركة المرور من خادم VPN إلى الإنترنت، مما يجعل من الصعب على المهاجمين معرفة موقع المستخدم الفعلي.

أنواع الشبكات الافتراضية الخاصة

أ **VPNمن نوع الموقع إلى الموقع:(Site-to-Site VPN) :** تُستخدم لربط شبكتين مختلفتين عبر الإنترنت، مما يسمح لمستخدمي الشبكتين بالتواصل بشكل آمن.

ب **VPNمن نوع المستخدم إلى الموقع:(Remote Access VPN) :** تُستخدم للسماح للمستخدمين بالاتصال بشبكة الشركة من مواقع بعيدة، مما يوفر لهم الوصول إلى الموارد الداخلية.

حماية نقاط الوصول اللاسلكية

نقطة الوصول اللاسلكية هي جهاز يتيح الاتصال بين الأجهزة المختلفة وشبكة الكمبيوتر عبر تكنولوجيا الواي فاي. تُستخدم بشكل شائع في البيئات السكنية والتجارية لتوفير الاتصال اللاسلكي للأجهزة مثل الهواتف الذكية، وأجهزة الكمبيوتر المحمولة، والأجهزة اللوحية.

المخاطر المرتبطة بنقاط الوصول اللاسلكية:

أ. **التدخلات غير المرغوب فيها:** يمكن أن تتعرض نقاط الوصول للاختراق من قبل المهاجمين الذين يحاولون الوصول إلى الشبكة المحلية.

ب. **هجمات "المهاجم داخل الشبكة (Man-in-the-Middle Attacks):** " يحدث هذا عندما يتمكن المهاجم من التنصت على البيانات المتداولة بين الأجهزة ونقطة الوصول.

ج. **نقاط الوصول غير الآمنة:** تُعتبر نقاط الوصول العامة أو التي لم يتم تكوينها بشكل صحيح عرضة للاختراق.

استراتيجيات حماية نقاط الوصول اللاسلكية

أ. **تشفير الشبكة:** يجب استخدام بروتوكولات التشفير القوية مثل WPA3 لحماية البيانات المتداولة عبر الشبكة اللاسلكية. يُعتبر WPA3 أكثر أمانًا من WPA2 ويزيد من مستوى الحماية ضد الهجمات.

ب. **تغيير اسم الشبكة الافتراضية (SSID):** يجب تجنب استخدام الأسماء الافتراضية المعروفة، كما ينبغي جعل SSID غير قابل للتخمين لتقليل فرص الهجمات.

ج. **تفعيل جدار الحماية:** يجب تفعيل جدار الحماية الموجود في نقطة الوصول لمنع الاتصالات غير المرغوب فيها.

د. **تحديث البرامج الثابتة:** ينبغي تحديث البرنامج الثابت لنقاط الوصول بشكل دوري لسد الثغرات الأمنية وتحسين الأداء.

6- حماية البيانات في البيئة السحابية

الحوسبة السحابية هي نموذج لتوفير خدمات الحوسبة عبر الإنترنت، حيث يمكن للمستخدمين الوصول إلى موارد الحوسبة مثل الخوادم والتخزين وقواعد البيانات والتطبيقات من خلال الإنترنت. تشمل أنواع الحوسبة السحابية:

- **البنية التحتية كخدمة(IaaS)** **المنصة كخدمة(PaaS)** **البرمجيات كخدمة(SaaS)**

المخاطر المرتبطة بالبيانات في البيئة السحابية

أ. **فقدان البيانات:** قد تتعرض البيانات للفقدان بسبب أعطال في الخوادم أو الأخطاء البشرية أو هجمات القرصنة.

ب. **التسريبات:** يمكن أن تحدث التسريبات نتيجة الوصول غير المصرح به أو ضعف أمان البيانات.

ج. **التحكم في الوصول:** قد يكون هناك صعوبة في التحكم في من لديه الوصول إلى البيانات، مما يزيد من مخاطر الاختراق.

استراتيجيات حماية البيانات في البيئة السحابية

أ. **التشفير:** يجب تشفير البيانات أثناء النقل والتخزين. يستخدم التشفير تقنيات مثل AES (Advanced Encryption Standard) لحماية البيانات من الوصول غير المصرح به.

ب. **إدارة الهوية والوصول:** ينبغي استخدام أنظمة إدارة الهوية والوصول (IAM) لضمان أن المستخدمين المصرح لهم فقط هم من يمكنهم الوصول إلى البيانات الحساسة.

ج. **مراقبة النشاط:** يجب استخدام أدوات لمراقبة الأنشطة والعمليات التي تتم على البيانات، مما يسمح بالكشف عن أي سلوك غير طبيعي أو محاولات اختراق.

د. **النسخ الاحتياطي للبيانات:** يجب تنفيذ استراتيجيات النسخ الاحتياطي الدورية لضمان استعادة البيانات في حال حدوث فقدان. ينبغي الاحتفاظ بنسخ احتياطية في مواقع متعددة لضمان الأمان.

التحديات الأمنية في الحوسبة السحابية

تحديات أمن البيانات

أ. **فقدان السيطرة على البيانات:** عندما يتم تخزين البيانات في السحابة، تفقد المؤسسات السيطرة المباشرة على كيفية تخزينها ومعالجتها. تعتمد الحماية على تدابير الأمان التي يطبقها مزود الخدمة، مما قد يؤدي إلى قلق بشأن سلامة البيانات.

ب. **التسريبات والاختراقات:** يمكن أن تتعرض البيانات للتسريب نتيجة الهجمات الإلكترونية أو الوصول غير المصرح به. تتعرض البيانات الشخصية والحساسة لمخاطر عالية إذا لم يتم تأمين نقاط الوصول بشكل كافٍ.

التهديدات الخارجية

أ. **الهجمات الإلكترونية:** تزداد وتيرة الهجمات الإلكترونية مثل هجمات DDoS (Denial of Service) التي تستهدف مزودي الخدمة السحابية. تتيح هذه الهجمات للمهاجمين إغراق الخوادم بحركة مرور غير شرعية، مما يؤدي إلى تعطيل الخدمة.

ب. **القرصنة:** يمكن أن يتعرض نظام السحابة للاختراق من قبل المهاجمين الذين يستغلون ثغرات الأمان للوصول إلى البيانات الحساسة. تتطلب هذه الهجمات تحديثات دورية للأنظمة والتطبيقات لضمان عدم وجود ثغرات يمكن استغلالها.

التحديات الأمنية في الحوسبة السحابية

التهديدات الداخلية

أ. **الهجمات الداخلية:** قد تأتي التهديدات من داخل المؤسسة نفسها، حيث يمكن للموظفين ذوي الوصول المصرح به استغلال صلاحياتهم للوصول إلى بيانات حساسة أو تنفيذ هجمات.

ب. **الأخطاء البشرية:** يمكن أن يؤدي السلوك غير الآمن من قبل الموظفين، مثل استخدام كلمات مرور ضعيفة أو عدم اتباع سياسات الأمان، إلى زيادة مخاطر الأمان.

تحديات الامتثال

أ. **متطلبات الامتثال:** تتطلب العديد من المؤسسات الامتثال لمجموعة من اللوائح القانونية والمعايير الصناعية. يمكن أن تكون هذه المتطلبات معقدة ومتغيرة، مما يمثل تحديًا للمؤسسات التي تعمل في بيئات سحابية.

ب. **المسؤولية المشتركة:** في بيئة السحابة، غالبًا ما تكون هناك تقسيمات غير واضحة للمسؤولية بين مزود الخدمة والمستخدم النهائي. يجب على المؤسسات أن تفهم ما هي مسؤولياتهم وما هي مسؤوليات مزود الخدمة لضمان الامتثال.

التحديات المتعلقة بالأداء

أ. **تأثير الأداء:** قد تؤثر مشكلات الأمان على أداء النظام. على سبيل المثال، التشفير الزائد أو الفحص الأمني يمكن أن يؤدي إلى بطء في أداء التطبيقات.

ب. **زيادة التعقيد:** تؤدي إضافة طبقات أمان جديدة إلى زيادة تعقيد النظام، مما قد يخلق مشكلات في الأداء ويدفع المؤسسات إلى البحث عن حلول معقدة.

خاتمة

آمل ان تكونوا قد حققتم الفائدة