
دبلوم الأمن السيبراني
مكونات أنظمة تقنية المعلومات

مقدمة

يشهد العالم اليوم تطورًا متسارعًا في مجال تقنية المعلومات، حيث أصبحت الأنظمة التقنية هي العمود الفقري لمختلف القطاعات الحيوية مثل التعليم، الصحة، البنوك، الصناعة، والخدمات الحكومية. وتكمن أهمية هذه الأنظمة في قدرتها على إدارة البيانات، تسهيل العمليات، وتعزيز كفاءة الأعمال، إلا أن هذا التطور يصاحبه تحديات عديدة خاصة فيما يتعلق بالأمن السيبراني وحماية البنية التحتية الرقمية.

وانطلاقًا من ذلك، تم إعداد هذا البرنامج التدريبي بعنوان "مكونات أنظمة تقنية المعلومات"، والذي يهدف إلى تزويد المشاركين بالمعرفة والمهارات الأساسية لفهم مكونات الأنظمة التقنية من أجهزة وبرمجيات وشبكات، إلى جانب استيعاب أسس الأمن السيبراني، والاطلاع على أحدث التقنيات مثل الحوسبة السحابية، البيئات الافتراضية، وإنترنت الأشياء.

سيمكن هذا البرنامج المتدربين من الإلمام بكيفية حماية الأجهزة والشبكات، إدارة البيانات، التعامل مع التحديات الأمنية، وتبني أفضل الممارسات العالمية لضمان استمرارية الأعمال في بيئة تقنية سريعة التغير.

حماية الأجهزة الطرفية في الشبكات

الوحدة الأولى: حماية الأجهزة الطرفية في الشبكات.

حماية الشبكات وأنواع طرق حماية الشبكات

ما هي حماية الشبكات:

حماية الشبكات هي عملية تأمين شبكات الكمبيوتر من الوصول غير المصرح به، والاستخدام، والكشف، والتعديل، والتدمير، أو تعطيل الأصول الرقمية .تهدف حماية الشبكات إلى الحفاظ على سرية وسلامة وأمن البيانات والأنظمة المتصلة بالشبكة .

هناك العديد من أنواع حماية الشبكات، منها:

1. جدار الحماية :(Firewall) يعمل كحاجز بين الشبكة الداخلية والشبكات الخارجية، ويتحكم في حركة البيانات بناءً على قواعد محددة مسبقًا، ويمنع الوصول غير المصرح به .
2. أنظمة كشف التسلل ومنع التطفل :(IDS/IPS) تراقب حركة البيانات في الشبكة وتحدد التهديدات المحتملة، وتتخذ إجراءات لمنع الهجمات أو التخفيف من آثارها .
3. الشبكات الخاصة الافتراضية :(VPN) توفر اتصالاً آمنًا ومشفرًا بين جهازين أو شبكتين عبر الإنترنت، مما يحمي البيانات من التنصت .
4. أمان البريد الإلكتروني: يتضمن حماية حسابات البريد الإلكتروني ومحتوياتها من التهديدات المختلفة، مثل التصيد الاحتيالي والبرامج الضارة .
5. منع فقدان البيانات :(DLP) يهدف إلى منع تسرب البيانات الحساسة من الشبكة، سواء عن طريق الخطأ أو عن قصد .
6. إدارة الوصول والأذونات: تضمن منح حق الوصول إلى الموارد والبيانات بناءً على أدوار ومستويات صلاحية محددة .

7. التشفير: يستخدم لتحويل البيانات إلى شكل غير مقروء، بحيث لا يمكن فهمها إلا من قبل الأطراف المصرح لها باستخدام مفتاح فك التشفير .

8. التحديثات الأمنية: تتضمن تحديث البرامج وأنظمة التشغيل بانتظام لسد الثغرات الأمنية التي قد يستغلها المهاجمون .

9. المصادقة متعددة العوامل: تتطلب من المستخدمين تقديم أكثر من طريقة للتحقق من هويتهم، مما يزيد من صعوبة الوصول غير المصرح به .

10. تجزئة الشبكة: تقسيم الشبكة إلى شبكات فرعية أصغر، مما يحد من انتشار الهجمات ويقلل من الأضرار المحتملة .

بالإضافة إلى هذه الأنواع، هناك العديد من التقنيات والأساليب الأخرى المستخدمة في حماية الشبكات، مثل:

- **أمن نقاط النهاية:(Endpoint Security)**

حماية الأجهزة المتصلة بالشبكة، مثل أجهزة الكمبيوتر والأجهزة المحمولة، من البرامج الضارة والهجمات .

- **أمن السحابة:(Cloud Security)**

حماية البيانات والأنظمة التي تستضيفها السحابة .

- **إدارة المعلومات الأمنية والأحداث:(SIEM)**

توفير رؤية شاملة لأحداث الأمن السيبراني عبر الشبكة .

تتطلب حماية الشبكات اتباع نهج شامل ومتكامل، يشمل استخدام مجموعة متنوعة من التقنيات والأساليب، بالإضافة إلى توعية المستخدمين بأفضل الممارسات الأمنية .

برامج مكافحة البرامج الضارة

ماهي برامج مكافحة الفيروسات:

برامج مكافحة البرامج الضارة هي أدوات مصممة لحماية أجهزة الكمبيوتر من البرامج الضارة مثل الفيروسات والديدان وأحصنة طروادة وغيرها .تقوم هذه البرامج بفحص الملفات والبرامج بحثًا عن علامات البرامج الضارة، وتمنعها من التثبيت أو التنفيذ، وتزيل أي برامج ضارة موجودة بالفعل .

أمثلة على برامج مكافحة البرامج الضارة:

- **Microsoft Defender:**

يأتي هذا البرنامج مضمنًا مع نظام التشغيل Windows ويقوم بفحص الملفات والبرامج بحثًا عن البرامج الضارة .كما أنه يقوم بتحديث نفسه تلقائيًا ليكون على اطلاع دائم بالتهديدات الجديدة.

- **برامج مكافحة البرامج الضارة الأخرى:**
  - **Avast** يقدم مجموعة متنوعة من خيارات الحماية، بما في ذلك الحماية في الوقت الفعلي والمسح الضوئي العميق.
  - Kasperskyيُعرف بميزاته المتقدمة في اكتشاف البرامج الضارة وإزالتها.
  - Bitdefenderيتميز بأدائه القوي في حماية الكمبيوتر من التهديدات المختلفة.
  - Nortonيوفر حماية قوية ضد البرامج الضارة والتهديدات الأخرى عبر الإنترنت .

أهمية استخدام برامج مكافحة البرامج الضارة:

- **الحماية من التهديدات:**

تساعد في حماية جهازك من البرامج الضارة التي يمكن أن تتسبب في تلف البيانات أو سرقة المعلومات الشخصية.

- **الحفاظ على أداء الجهاز:**

يمكن أن تبطئ البرامج الضارة أداء جهاز الكمبيوتر، لذلك تساعد برامج مكافحة البرامج الضارة في الحفاظ على الأداء السلس .

- **الأمان عبر الإنترنت:**

تساعد في حماية جهازك وبياناتك أثناء تصفح الإنترنت .

نصائح للحماية من البرامج الضارة:

- **تثبيت برنامج مكافحة البرامج الضارة:**

تأكد من تثبيت برنامج مكافحة البرامج الضارة وتحديثه بانتظام .

- **تجنب تنزيل الملفات من مصادر غير موثوقة:**

قم بتنزيل الملفات من المواقع الرسمية والموثوقة فقط .

- **كن حذرًا عند فتح رسائل البريد الإلكتروني:**

لا تفتح رسائل البريد الإلكتروني من مرسلين غير معروفين، وتجنب النقر على الروابط أو تنزيل المرفقات من رسائل البريد الإلكتروني المشبوهة .

- **تحديث نظام التشغيل والتطبيقات:**

حافظ على تحديث نظام التشغيل والتطبيقات الخاصة بك لضمان حصولك على أحدث تصحيحات الأمان .

تأمين الأجهزة الطرفية من الثغرات الأمنية داخل مؤسستك

لتأمين الأجهزة الطرفية من الثغرات الأمنية داخل مؤسستك، يجب عليك تنفيذ استراتيجية شاملة تتضمن عدة خطوات رئيسية، مثل إدارة الثغرات الأمنية، وتحديثات الأمان، والتحكم في الوصول، وتجزئة الشبكة، وتدابير الأمان المادية، والتدريب، ومراقبة الأجهزة .

أولاً: إدارة الثغرات الأمنية

- **تحديد الثغرات:**

قم بإجراء فحوصات منتظمة للثغرات الأمنية على جميع الأجهزة الطرفية لتحديد نقاط الضعف المحتملة .

- **تحديد الأولويات:**

صنف الثغرات بناءً على خطورتها وتأثيرها المحتمل على العمليات التجارية .

- **معالجة الثغرات:**

قم بتطبيق التصحيحات الأمنية والتحديثات اللازمة في أسرع وقت ممكن، ويفضل باستخدام نظام إدارة تصحيحات تلقائي .

- **استخدام أدوات إدارة الثغرات الأمنية:**

استخدم أدوات متخصصة لإدارة الثغرات الأمنية لتسهيل عملية الكشف عن الثغرات وتصحيحها .

ثانياً: تحديثات الأمان

- **تحديثات نظام التشغيل والتطبيقات:**

قم بتحديث أنظمة التشغيل والتطبيقات على جميع الأجهزة الطرفية بانتظام لضمان استخدام أحدث إصدارات البرامج التي تتضمن أحدث تصحيحات الأمان.

- **تحديثات البرامج الثابتة:**

قم بتحديث البرامج الثابتة للأجهزة الطرفية، مثل الطابعات وأجهزة التوجيه، بانتظام لتجنب استغلال الثغرات الأمنية المعروفة .

ثالثاً: التحكم في الوصول وتجزئة الشبكة

- **التحكم في الوصول:**

قم بتنفيذ آليات التحكم في الوصول لتقييد الوصول إلى الأجهزة الطرفية والموارد، وتأكد من أن المستخدمين المصرح لهم فقط هم من يمكنهم الوصول إلى المعلومات الحساسة .

- **تجزئة الشبكة:**

استخدم تجزئة الشبكة لتقسيم الشبكة إلى شبكات فرعية أصغر، مما يحد من انتشار أي هجوم محتمل ويقلل من تأثيره .

رابعاً: الأمان المادي

- **تأمين الأجهزة:**

قم بتأمين الأجهزة المادية، مثل الأجهزة المحمولة وأجهزة الكمبيوتر المكتبية، لمنع العبث بها أو سرقتها.

- **حماية الكابلات:**

قم بتأمين الكابلات والشواحن لتجنب العبث بها واستبدالها بأجهزة أخرى .

خامساً: التدريب والتوعية

- **تدريب الموظفين:**

قم بتدريب الموظفين على أفضل ممارسات الأمان، بما في ذلك كيفية التعرف على رسائل البريد الإلكتروني المخادعة وكيفية التعامل مع الأجهزة الطرفية بشكل آمن .

- **التوعية الأمنية:**

قم بتوعية الموظفين بأحدث التهديدات الأمنية وكيفية حماية أنفسهم والأجهزة الخاصة بهم .

سادساً: المراقبة

- **مراقبة الأجهزة:**

قم بمراقبة الأجهزة الطرفية بانتظام للكشف عن أي نشاط مشبوه أو غير عادي .

- **تحليل السجلات:**

قم بتحليل سجلات الأجهزة للكشف عن أي محاولات اختراق أو انتهاكات أمنية .

سابعاً: استخدام أدوات الأمان

- **جدار الحماية:**

استخدم جدار حماية لتأمين شبكتك والتحكم في حركة المرور الواردة والصادرة .

- **برامج مكافحة الفيروسات:**

قم بتثبيت برنامج مكافحة فيروسات على جميع الأجهزة الطرفية لحمايتها من البرامج الضارة .

- **حلول إدارة الأجهزة المحمولة:(MDM)**

استخدم حلول MDM لإدارة الأجهزة المحمولة وضمان تطبيق سياسات الأمان .

أجهزة التخزين

الوحدة الثانية: أجهزة التخزين

اجهزة تخزين البيانات:

أجهزة تخزين البيانات هي الأجهزة التي تستخدم لحفظ البيانات واسترجاعها .تشمل هذه الأجهزة الأقراص الصلبة(HDD) ، والأقراص الصلبة ذات الحالة الصلبة(SSD) ، ووحدات التخزين السحابية، والأقراص المدمجة(CD) ، وأقراص الفيديو الرقمية(DVD) ، ومحركات أقراص الفلاش، وشرائط البيانات، وبطاقات الذاكرة.

أنواع أجهزة تخزين البيانات:

- **الأقراص الصلبة:(HDD)**

تستخدم أقراصًا مغناطيسية لتدوير البيانات، وهي أقدم تقنية تخزين البيانات.

- **الأقراص الصلبة ذات الحالة الصلبة:(SSD)**

تستخدم ذاكرة فلاش لتخزين البيانات، وتتميز بسرعات قراءة وكتابة أعلى من محركات الأقراص الصلبة.

- **وحدات التخزين السحابية:**

تخزن البيانات على خوادم بعيدة يمكن الوصول إليها عبر الإنترنت.

- **الأقراص المدمجة (CD) والأقراص الفيديو الرقمية:(DVD)**

تستخدم أقراص بصرية لتخزين البيانات.

- **محركات أقراص الفلاش:**

تستخدم ذاكرة فلاش لتخزين البيانات وهي صغيرة الحجم ومحمولة.

- **شرائط البيانات:**

تستخدم لتخزين كميات كبيرة من البيانات، مثل النسخ الاحتياطية.

- **بطاقات الذاكرة:**

تستخدم في الأجهزة المحمولة مثل الهواتف الذكية والكاميرات الرقمية.

أمثلة على أجهزة تخزين البيانات:

- محركات الأقراص الصلبة (HDD) و (SSD) المستخدمة في أجهزة الكمبيوتر.
- محركات الأقراص الصلبة الخارجية.
- محركات أقراص فلاش USB.
- بطاقات الذاكرة المستخدمة في الهواتف والكاميرات.
- وحدات التخزين السحابية مثل OneDrive و Google Drive.
- أقراص Blu-ray.
- محركات أقراص الشريط .

أهمية أجهزة تخزين البيانات:

- حفظ البيانات :تسمح بتخزين البيانات واسترجاعها عند الحاجة.
- النسخ الاحتياطي :توفر وسيلة لعمل نسخ احتياطية للبيانات المهمة.
- نقل البيانات :تتيح نقل البيانات بين الأجهزة المختلفة.
- الأرشفة :تستخدم لحفظ البيانات لفترات طويلة.
- توسيع سعة التخزين :تتيح إضافة مساحة تخزين إضافية للأجهزة .

أنواع وحدات التخزين في الحاسوب

تتضمن وحدات التخزين في الحاسوب ما يأتي:

ذاكرة الوصول العشوائي (RAM)

تعتبر الرام أو ذاكرة الوصول العشوائي بالإنجليزيّة: (Random Access Memory)ذاكرة أساسية ومؤقتة في الحاسوب، حيث تمكن مستخدم الحاسوب من الوصول إلى وحدة المعالجة المركزية، كما يتم تخزين البرامج المفتوحة أو الملفات مباشرةً عليها، لكنها تعد مكانًا غير مناسب لتخزين المعلومات، إذ يمكن أن تضيع عند انقطاع الكهرباء عن الحاسوب، ومن جانبٍ آخر يتم قياس قدرة الرام بالجيجابايت، ويتوفر منه نوعان أساسيان هما DRAM و SRAM

محرك الأقراص الصلبة

يعمل محرك الأقراص الصلبة بالإنجليزيّة: (Solid State Driveأو SSD) على تخزين أكبر قدرٍ ممكن من البيانات، كما أنه يتميز بكونه ثابتاً، وتستخدم الجيجا بايت لتحديد قدرة محرك الأقراص الصلبة، كما يمكن شراؤه وتركيبه داخل الحاسوب أو خارجه ضمن وحدات التخزين الخارجية، ويفضل تركيب قرصين محركات صلبة للحاسوب للحصول على سعة تخزينية كبيرة، لتحسين عمل نظام الحاسوب والبرامج، ومنح مساحة تخزين ملفات الموسيقى أو الوثائق، وسرعة الوصول إليها، ويعتبر وزنه خفيفاً، وصغير الحجم، كما أنه غير قابلة للتلف أو أيٍ من أجزائه، فهو متين ويستهلك القليل من الطاقة.

ذاكرة القراءة فقط ((ROM

تعد ذاكرة القراءة فقط بالإنجليزيّة: (Read-Only Memory)ذاكرة تخزين ثابتة، لا يمكن تعديل أو حذف البيانات المخزنة بداخلها، بمعنى توفير إمكانية القراءة فقط، وتستخدم لبدء تشغيل الحاسوب، ويتوفر نوعان من هذه الذاكرة هما .PROM, EPROM

القرص الصلب

يعتمد القرص الصلب بالإنجليزيّة: (Hard Disk)في مبدأ عمله على استعادة وحفظ البيانات من خلال التخزين الممغنط، بحيث يسمح بتعديل أو حذف البيانات بعدد غير محدد، كما تعتبر سرعته مناسبة.

الأقراص الضوئية

تتوفر الأقراص الضوئية بالإنجليزيّة: (Optical Storage Discs)على شكل قرص مضغوط CD, DVD,Blu Ray، وتختلف سعتها التخزينية من نوع إلى آخر، ويعتبر قرص Blu Ray الأكبر مساحةً، إذ يمكن تخزين الأفلام والبيانات بجودة عالية، بينما يمكن تخزين البيانات بجودة عالية جدًا باستخدام قرص .Blu Ray

ذاكرة الفلاش USB

تعتبر ذاكرة الفلاش USB بالإنجليزيّة: (USB Flash Memory)من أجهزة التخزين غير الثابتة التي تسمح بتخزين كمية كبيرة جدًا من البيانات والملفات، من خلال توصيلها بالحاسوب، وتتميز بكونها صغيرة ومحمولة ووزنها خفيف، إلى جانب قوتها، وسرعتها العالية، وتعتبر منخفضة السعر مقارنةً بغيرها من وحدات التخزين.

التخزين السحابي

تعريف التخزين السحابي

التخزين السحابي هو تقنية مبتكرة تتيح تخزين الملفات عبر الإنترنت بدلاً من الأجهزة المحلية، مما يوفر سهولة الوصول من أي مكان مع اتصال بالإنترنت. يتميز بخيارات مرنة للتوسع، نسخ احتياطي تلقائي، وأدوات مشاركة فعّالة، بينما تشمل تحدياته الخصوصية وتكاليف التخزين الكبيرة. الحلول المختلطة التي تجمع بين السحابة والتخزين المحلي تساعد في تحقيق الأمان والمرونة المطلوبة.

مفهوم التخزين السحابي:

مفهوم التخزين السحابي Cloud storag هو مصطلح يشير إلى خدمة تخزين البيانات عبر الإنترنت، حيث يتم تخزين الملفات والمعلومات على خوادم عبر الإنترنت بدلًا من تخزينها محليًا على أجهزة الكمبيوتر الشخصية أو الأقراص الصلبة. ويتم الوصول إلى هذه البيانات من خلال الاتصال بالإنترنت، ويتم توفير الخدمة عادةً من قبل مزودي خدمات التخزين السحابي.

ولكن من الضروري اتخاذ بعض الاحتياطات عند استخدام التخزين السحابي، مثل تأمين حسابك بكلمات مرور قوية واستخدام خدمات التشفير، وخاصة في حالة تخزين المعلومات الحساسة. لذا يجب التحقق من سياسة الخصوصية وشروط الاستخدام لمزود الخدمة السحابية قبل تخزين الملفات الحساسة.

أنواع التخزين السحابي:

هناك عدة أنواع من خدمات التخزين السحابي المتاحة، حيث تشمل أنواع التخزين السحابي التخزين العام الذي يوفر مرونة وسعة مشتركة، التخزين الخاص للأمان والتحكم الكامل، التخزين الهجين الذي يجمع بينهما، والتخزين المشترك الذي يناسب الشركات الصغيرة بتكلفة أقل.

إليك تفصيل ذلك:

1. التخزين السحابي العام (Public Cloud Storage)

يوفر التخزين السحابي العام سعة تخزين هائلة، وتتيح للمستخدمين تخزين البيانات والملفات والتطبيقات على الخوادم السحابية المشتركة. ويكون الوصول إلى البيانات متاحًا للجميع عبر الإنترنت، ويتم تحمل الشركة المزودة للخدمة مسؤولية الصيانة والتشغيل. وتقدم هذه الخدمة من قبل شركات كبيرة مثل (Amazon Web Services (AWS وMicrosoft Azure و(Google Cloud Platform (GCP.

2. التخزين السحابي الخاص (Private Cloud Storage)

يستخدم التخزين السحابي الخاص من التخزين السحابي بواسطة المؤسسات والشركات الكبيرة التي تفضل الحفاظ على البيانات والملفات داخل بنية تحتية خاصة بها. ويتم بناء البنية التحتية الخاصة بالشركة وتشغيلها داخل الحائط الناري الخاص بها، مما يوفر مستوى عالٍ من الأمان والتحكم في البيانات. وقد تكون هذه الحلول مكلفة وتتطلب صيانة وإدارة مستمرة.

3. التخزين السحابي الهجين (Hybrid Cloud Storage)

يجمع التخزين السحابي الهجين بين التخزين السحابي العام والخاص، حيث يتم استخدام التخزين السحابي للوصول السريع والمرن إلى الملفات والتطبيقات غير الحساسة، في حين يتم استخدام التخزين السحابي الخاص للبيانات الحساسة والتطبيقات التي تتطلب مستوى أعلى من الأمان والتحكم.

4. التخزين السحابي المشترك (Shared Cloud Storage)

يُتيح التخزين السحابي المشترك من التخزين السحابي للمستخدمين المشاركة في تخزين البيانات والملفات على خوادم سحابية مشتركة. ويعتبر التخزين السحابي المشترك خيارًا اقتصاديًا للأفراد والشركات الصغيرة التي تحتاج إلى حجم تخزين محدود وليس لديها متطلبات أمان عالية.

مميزات التخزين السحابي:

تتميز خدمات التخزين السحابي بعدة مميزات، ومن أهم فوائد التخزين السحابي ما يلي:

1. التوافر والوصول السهل

يمكن الوصول إلى البيانات المخزنة في السحابة من أي مكان وفي أي وقت بشرط وجود اتصال بالإنترنت. فلا يوجد حاجة لحمل الأجهزة الفعلية أو الاعتماد على وسائط التخزين المحمولة.

2. التوسع المرن

يمكن لمستخدمي التخزين السحابي زيادة أو تقليل مساحة التخزين حسب حاجتهم بسهولة. ولا يتطلب ذلك شراء أجهزة إضافية أو تجديد الأجهزة الحالية، بل يتم ذلك بسرعة وفعالية عبر واجهة السحابة.

3. الحماية والاحتياطات

يوفر التخزين السحابي نسخًا احتياطية تلقائية للبيانات، مما يضمن سلامتها وتوفرها في حالة حدوث خلل في الأجهزة المحلية أو الكوارث الطبيعية. كما يتم تطبيق إجراءات أمنية متقدمة لحماية البيانات من الوصول غير المصرح به.

4. التكلفة الاقتصادية

يعتبر التخزين السحابي في كثير من الأحيان اقتصاديًا أكثر من شراء وصيانة أجهزة التخزين المحلية. فلا حاجة لدفع تكاليف الأجهزة والبرامج والتحديثات المستمرة. وبدلاً من ذلك، يتم دفع رسوم استخدام قائمة على الاستهلاك الفعلي للمساحة والموارد.

5. التعاون والمشاركة

يوفر التخزين السحابي إمكانية سهلة لمشاركة البيانات والملفات بين المستخدمين المختلفين. ويمكن تعيين أذونات الوصول والتحكم في المشاركة وتحديد من يمكنه الوصول إلى الملفات ومن يمكنه التعديل عليها.

6. الاستدامة البيئية

يمكن أن يكون التخزين السحابي أكثر استدامة من الأنظمة التقليدية، حيث يتم تقليل الحاجة إلى استخدام الأجهزة الفعلية والتشغيل المستمر للخوادم.

عيوب التخزين السحابي

بالرغم من فوائد التخزين السحابي، إلا أن هناك بعض العيوب والتحديات التي يجب أخذها في الاعتبار، ومن أهم سلبيات التخزين السحابي ما يلي:

1. الاتصال بالإنترنت

يتطلب استخدام التخزين السحابي اتصالًا مستمرًا بالإنترنت، وفي حالة عدم توفر اتصال قوي أو انقطاع الاتصال بالإنترنت، وقد يكون الوصول إلى البيانات أو تحميلها بطيئًا أو غير متاح.

2. الخصوصية والأمان

قد تثير قضايا الخصوصية والأمان مخاوف لدى بعض المستخدمين، حيث عندما يتم تخزين البيانات على السحابة، فإنها تكون في عهدة مزود الخدمة وتتعرض لمخاطر الاختراق أو الوصول غير المصرح به. ويجب على المستخدمين اختيار مزود خدمة سحابية موثوق والتحقق من سياسات الأمان المعتمدة.

3. التكلفة

قد تكون خدمات التخزين السحابي مكلفة لبعض المستخدمين، وخاصة عندما يتعلق الأمر بتخزين كميات كبيرة من البيانات. وقد تكون هناك رسوم شهرية أو تكاليف إضافية لزيادة المساحة التخزينية أو استخدام الموارد الإضافية.

4. الاعتمادية

يعتمد التخزين السحابي على خدمات السحابة المقدمة من الشركات. والتي يمكن أن تواجه بعض المشكلات مثل انقطاع الخدمة بسبب أعطال التكنولوجيا أو الصيانة المجدولة.

5. قيود التخزين والمساحة

قد تفرض بعض خدمات التخزين السحابي قيودًا على حجم التخزين أو عدد الملفات المسموح بها. لذا يجب مراعاة هذه القيود عند اختيار خدمة التخزين السحابي والتأكد من أنها تلبي احتياجاتك.

6. قضايا التوافق والانتقالية

في بعض الأحيان، قد تواجه صعوبات في توافق البيانات والتطبيقات مع بعض خدمات التخزين السحابي. يجب التأكد من أن الخدمة المختارة تدعم الأنظمة والتطبيقات التي تستخدمها وتوفر عملية انتقال سلسة للبيانات.

بنى الأنظمة

الوحدة الثالثة: بني الانظمة

المقصود بالبنية التحتية لتكنولوجيا المعلومات :

هي مجموعة المكونات المادية والبرمجية التي تدعم توفير خدمات تكنولوجيا المعلومات في المؤسسات والشركات .تشمل هذه المكونات الأجهزة، والشبكات، والبرمجيات، ومراكز البيانات، وأنظمة التشغيل، وقواعد البيانات، وغيرها من التقنيات التي تمكن الشركات من تشغيل تطبيقاتها وأنظمتها وخدماتها .

ببساطة، هي الأساس الذي تقوم عليه جميع عمليات تكنولوجيا المعلومات في المؤسسة .

أمثلة على مكونات البنية التحتية لتكنولوجيا المعلومات:

- **الأجهزة:**

الخوادم، وأجهزة الكمبيوتر، وأجهزة التخزين، وأجهزة الشبكات، ومعدات الاتصالات .

- **البرمجيات:**

أنظمة التشغيل، وقواعد البيانات، وتطبيقات البرامج، وأدوات الإدارة .

- **الشبكات:**

البنية التحتية للشبكات المحلية(LAN) ، والشبكات واسعة النطاق(WAN) ، والشبكات اللاسلكية، والاتصالات السحابية .

- **مراكز البيانات:**

المباني المجهزة بأنظمة تبريد، وطاقة احتياطية، وأنظمة أمن، لتشغيل الخوادم ومعدات التخزين .

- **التقنيات السحابية:**

توفر خدمات الحوسبة والتخزين عبر الإنترنت، مثل خدمات أمازون ويب سيرفيس(AWS) ومايكروسوفت أزور (Azure) وجوجل كلاود (Google Cloud).

أهمية البنية التحتية لتكنولوجيا المعلومات:

- **دعم العمليات التجارية:**

توفر البنية التحتية الأساس لتشغيل التطبيقات والأنظمة التي تدعم العمليات التجارية المختلفة، مثل إدارة المخزون، وإدارة علاقات العملاء، وإدارة الموارد البشرية .

- **تمكين التحول الرقمي:**
تلعب البنية التحتية دورًا حيويًا في تمكين الشركات من التحول الرقمي، من خلال توفير الأساس لتطبيق التقنيات الجديدة مثل الذكاء الاصطناعي والتعلم الآلي .

- **تحسين الكفاءة:**
تساعد البنية التحتية الجيدة على تحسين كفاءة العمليات، وتقليل التكاليف، وتحسين الأداء العام للشركة .

- **ضمان الأمن:**
تساهم البنية التحتية في حماية البيانات والمعلومات الحساسة من الوصول غير المصرح به والتهديدات السيبرانية .

باختصار، البنية التحتية لتكنولوجيا المعلومات هي العمود الفقري الذي يدعم جميع جوانب العمليات التشغيلية والتجارية للشركة .

أنواع البنية التحتية لتكنولوجيا المعلومات:

تنقسم البنية التحتية لتكنولوجيا المعلومات إلى ثلاثة أنواع رئيسية :البنية التحتية التقليدية (المحلية)، والحوسبة السحابية، والبنية التحتية الهجينة .

1. البنية التحتية التقليدية (المحلية):

- تتكون من الأجهزة والبرامج التي يتم تخزينها محليًا، عادةً في مبنى أو مركز بيانات خاص بالشركة.
- تتضمن هذه البنية مرافق، ومراكز بيانات، وخوادم، وأجهزة شبكات، وأجهزة كمبيوتر، وحلول برمجيات.
- تتطلب عادةً استثمارات كبيرة في الأجهزة والبرامج، بالإضافة إلى المساحات والموارد المالية.
- عادة ما تكون مخصصة للاستخدام الداخلي للشركة .

2. الحوسبة السحابية:

- تعتمد على موارد الحوسبة التي يتم توفيرها عبر الإنترنت من قبل مزودي الخدمات السحابية.
- توفر مرونة وقابلية للتوسع، حيث يمكن للمستخدمين الوصول إلى الموارد حسب الحاجة.
- تتضمن البنية التحتية السحابية الخوادم والتخزين والشبكات والتطبيقات التي يتم تشغيلها على البنية التحتية لمزود الخدمة.
- يمكن للمستخدمين الوصول إلى هذه الموارد عبر الإنترنت دون الحاجة إلى تثبيت أي شيء محليًا.
- تتضمن السحابة العامة (المتاحة للجميع) والسحابة الخاصة (مخصصة لمؤسسة معينة) والسحابة الهجينة (مزيج من الاثنين) .

3. البنية التحتية الهجينة:

- تجمع بين البنية التحتية التقليدية (المحلية) والحوسبة السحابية.
- تسمح للمؤسسات بالاستفادة من مزايا كل من البنية التحتية التقليدية والسحابية.
- يمكن نقل أعباء العمل بين البنية التحتية المحلية والسحابية حسب الحاجة.
- توفر مرونة أكبر في إدارة الموارد والتكاليف .

مكونات البنية التحتية لتكنولوجيا المعلومات:

- **الأجهزة:**
تشمل الخوادم، وأجهزة الكمبيوتر، وأجهزة الشبكات، وأنظمة التخزين، وغيرها من المعدات المادية .

- **البرامج:**
تشمل أنظمة التشغيل، والتطبيقات، وقواعد البيانات، وبرامج إدارة المحتوى، وغيرها .

- **الشبكات:**
تشمل أجهزة الشبكات، وبروتوكولات الاتصال، واتصال الإنترنت، والشبكات اللاسلكية، وتدابير أمن الشبكات .

- **الموارد البشرية:**

الأشخاص الذين يقومون بتصميم وإدارة وتشغيل ودعم البنية التحتية لتكنولوجيا المعلومات .

أمثلة على خدمات البنية التحتية السحابية:

- **الحوسبة:**
مثيلات الحوسبة، والحاويات، والبنية التحتية للحوسبة بلا خادم.
- **الشبكات:**
شبكات آمنة وموثوقة، وخدمات تسليم المحتوى.
- **التخزين:**
تخزين سحابي موثوق، وقابل للتطوير، وآمن .

تعتمد الشركات على هذه الأنواع المختلفة من البنية التحتية لتلبية احتياجاتها التشغيلية والتجارية، حيث توفر البنية التحتية السحابية مرونة وقابلية للتوسع، بينما توفر البنية التحتية التقليدية تحكمًا أكبر على البيانات والتطبيقات .

مراحل البناء التقني

تنقسم مراحل البناء التقني إلى ثلاثة أقسام رئيسية :بناء الإدارة التقنية، بناء البنية التحتية التقنية، وبناء الأنظمة والخدمات .

شرح المراحل:

1. **بناء الإدارة التقنية:(IT Management)**
تتضمن هذه المرحلة وضع استراتيجية تقنية واضحة للمنظمة، وتحديد الأدوار والمسؤوليات، وتحديد الميزانية والجدول الزمني للمشاريع التقنية.
2. **بناء البنية التحتية التقنية:(IT Infrastructure)**
تشمل هذه المرحلة توفير الأجهزة والبرامج والمعدات اللازمة لتشغيل الأنظمة والخدمات التقنية، مثل الخوادم، وأجهزة الشبكات، وقواعد البيانات.
3. **بناء الأنظمة والخدمات:(Systems and Services)**
تتضمن هذه المرحلة تطوير وتنفيذ الأنظمة والبرامج التي تدعم العمليات التجارية للمنظمة، وتقديم الخدمات التقنية للموظفين والعملاء .

دورة البناء التقني في كل مرحلة:

تتضمن كل مرحلة من مراحل البناء التقني دورة متكررة تشمل :

- **تحديد الاحتياج:**
تحديد المتطلبات التقنية اللازمة لتحقيق أهداف المنظمة.
- **معرفة الحلول المتاحة:**
البحث عن التقنيات والحلول المناسبة لتلبية الاحتياجات.
- **المقارنة والاختيار:**
تقييم الخيارات المتاحة واختيار الأفضل من حيث التكلفة والجودة والوقت.
- **التنفيذ:**
تطبيق الحلول التقنية واختبارها.
- **التقييم المستمر:**
متابعة أداء التقنيات والحلول وتعديلها حسب الحاجة.

أمثلة على بناء الأنظمة والخدمات:

تشمل هذه المرحلة بناء أنظمة إدارة علاقات العملاء(CRM) ، وأنظمة تخطيط موارد المؤسسات (ERP)، وأنظمة إدارة المحتوى(CMS) ، وتطبيقات الجوال، وغيرها من الأنظمة والخدمات التقنية .

أهمية مراحل البناء التقني:

تعتبر مراحل البناء التقني أساسية لنجاح أي منظمة في العصر الرقمي، حيث تضمن هذه المراحل :

- **تحقيق الأهداف الاستراتيجية للمنظمة:**
من خلال توفير البنية التحتية التقنية والأنظمة والخدمات المناسبة.
- **تحسين الكفاءة والإنتاجية:**
من خلال أتمتة العمليات التجارية وتوفير أدوات وتقنيات متطورة للموظفين.
- **تقديم خدمات أفضل للعملاء:**
من خلال توفير قنوات اتصال رقمية متنوعة وتجارب مستخدم متميزة.
- **تحقيق النمو والتطور:**
من خلال تبني التقنيات الجديدة والتكيف مع التغيرات في السوق.

البيئات الافتراضية والحوسبة الحسابية

الوحدة الرابعة: البيئات الافتراضية والحوسبة الحسابية

المقصود بالمحاكاة الافتراضية

المحاكاة الافتراضية (Virtualization) هي عملية إنشاء نسخة افتراضية من شيء ما، مثل جهاز كمبيوتر أو نظام تشغيل أو شبكة أو جهاز تخزين، بدلاً من استخدام الأجهزة الفعلية .تتيح المحاكاة الافتراضية تقسيم جهاز فعلي واحد إلى عدة أجهزة افتراضية، أو دمج موارد أجهزة متعددة في جهاز افتراضي واحد .

شرح أكثر تفصيلاً:

- **إنشاء نسخ افتراضية:**
المحاكاة الافتراضية تعني إنشاء تمثيلات رقمية للأشياء المادية، مثل الخوادم أو أجهزة التخزين أو الشبكات، باستخدام البرامج .
- **تشغيل عدة أنظمة على جهاز واحد:**
بدلاً من استخدام جهاز فعلي لكل نظام تشغيل أو تطبيق، تتيح المحاكاة الافتراضية تشغيل عدة أنظمة افتراضية على جهاز مادي واحد .

- **أمثلة على المحاكاة الافتراضية:**
  - **محاكاة سطح المكتب: توفير أجهزة سطح مكتب افتراضية من خادم مركزي .**
  - **محاكاة الشبكة :تقسيم عرض النطاق الترددي للشبكة إلى قنوات افتراضية .**
  - **محاكاة التخزين تجميع موارد تخزين متعددة في جهاز تخزين افتراضي واحد .**
- **فوائد المحاكاة الافتراضية:**
  - **تحسين استخدام الموارد :استخدام الموارد المادية بكفاءة أكبر .**
  - **خفض التكاليف :تقليل عدد الأجهزة الفعلية المطلوبة وتكاليف الصيانة .**
  - **زيادة المرونة :سهولة نقل الأجهزة الافتراضية وإدارتها .**
  - **تمكين الحوسبة السحابية :توفير البنية التحتية الأساسية لخدمات الحوسبة السحابية .**
- **أمثلة على المحاكاة الافتراضية في الحياة العملية:**
  - **الشركات :تستخدم المحاكاة الافتراضية لتقليل تكاليف البنية التحتية وزيادة كفاءة العمليات .**
  - **مقدمو خدمات الحوسبة السحابية :يعتمدون على المحاكاة الافتراضية لتوفير خدماتهم .**
  - **المطورون :يستخدمون المحاكاة الافتراضية لتجربة أنظمة تشغيل مختلفة أو اختبار التطبيقات .**

تقنيات البيئة الافتراضية Virtualization أنواعها وكيفية عملها ومستقبلها:

توفر البيئة الافتراضية (Virtualization) خيارات مميزة منها تمكين مدراء أنظمة المعلومات بتثبيت ترقيات وتحديثات في حيز من الحاسوب بينما يقوم المستخدم بأداء عمله بتطبيقات وبرامج في بيئة أخرى قد تكون نظام تشغيل مختلف على سبيل المثال. وتسرّع هذه التقنية تحميل ملفات نظام التشغيل في حال حدوث خلل في النظام القديم، مع إمكانية التخلي عن النظام ككل واستبداله بنظام آخر بديل موجود مسبقا، ويتم التعامل مع أنظمة التشغيل كالبرامج حيث لم يعد إعادة تحميل نظام تشغيل جديد يتطلب إنشاء صورة للقرص الصلب كما يفعل برنامج غوست (Ghost) على سبيل المثال، وتعتبر ميزة تشغيل عدة أنظمة بنفس الوقت مناسبة لمطوري البرامج أثناء كتابتهم البرامج والأنظمة المختلفة لسهولة التنقل بينها. وتخفف البيئة الافتراضية تكاليف الشركات المتخصصة باستضافة مواقع الشبكة (الانترنت)، فوجود عدد كبير من المستخدمين يتطلب خواديم تكافئ عددهم وهو خيار ناجح أمنياً إلا أنه فاشل اقتصادياً لوجود تكاليف باهظة أهمها الدعم التقني الذي ستوفره الشركة لعملائها. تحل البيئة الافتراضية المعضلة بتقديم كمبيوتر افتراضي مستقل لكل مستخدم يحق له تنزيل البرامج التي يريدها ودون حدوث تضارب مع المستخدمين الآخرين، وفي حال حدوث انهيار في الخادوم سيكون الحل متوفرا بشكل فوري وحتى دون شعور المستخدم بحدوث الخلل.

أنواع البيئة الافتراضية

هناك ثلاثة أنواع للبيئة الافتراضية هي:

- **Paravirtualization**
- **Binary Translation**
- **Emulation.**

تقنية فاندربول Vanderpool الافتراضية من إنتل:

أعلنت إنتل عن هذه التقنية "تقنية فاندربول) بالإنجليزية (Vanderpool :الافتراضية" لأول مرة عام 2003، وعرضتها بتشغيل لعبة الحاسوب وبث فيديو رقمي إلى شاشة الحاسوب بنفس الوقت، تتيح تقنية فاندربول تشغيل أكثر من نظام تشغيل في ذات الوقت، كما تسمح لعدة مستخدمين من تشغيل برامج وتطبيقات مختلفة من نفس الحاسوب ودون حدوث خلل، وستقدم إنتل دعما لهذه التقنية في الشرائح التي ستطرحها منتصف العام الجاري، وعملت إنتل مع شركات برامج لتقديم دعم لها في برامجهم دون الاعتماد على دعم نظام التشغيل مثل شركةVMware ، ويمكن لشركات البرامج تقديم دعم لبرامجهم من خلال تنزيل مواصفات محددة من موقع إنتل.

نظام الإدارة الافتراضي:

تشير توقعات كثيرة إلى انتشار البيئة الافتراضية على نطاق واسع في المستقبل القريب مع انخفاض ملحوظ في تكاليفها، وقد يكون قطاع الخواديم من أقل القطاعات حماسا لثورة التقنية الافتراضية في حين سيشهد قطاع مستخدمي الشركات الكبيرة تغيرات حاسمة أهمها نظام الإدارة الافتراضي للأجهزة والذي يشكل جزءا لا يتجزأ من رزمة برامج الإدارة التي يمكن تنزيلها على الأجهزة وإجراء التعديلات عليها. يمكن نظام الإدارة الافتراضي المستخدم من تتبع البرامج غير المشروعة المستخدمة في الحاسوب مثلا وإيقافها أو تحميل وإلغاء البرامج المخزنة على القرص الصلب وإن حاول أحد المستخدمين العبث بملفات نظام التشغيل مثلا يمكنك إلغاء النظام فورا واستبداله بآخر وبسرعة كبيرة، وكذلك الحال مع الفيروسات والبرامج التخريبية التجسسية. وستزوّد إنتل نظام (Virtual Machine Manager (VMM كميزة معيارية في شرائحها مع تقنية VT في معالجات بنتيوم 4التي أو في معالجات ثنائية تلقب حاليا بـ «سميثفيلد» التي ستطرحها الشركة في النصف الثاني من هذا العام.

كيفية عمل البيئة الافتراضية:

يتطلب إنشاء خادوم افتراضي مستضاف ذاكرة بسعة 4 كيلوبايت واستخدام الأمر VMPTLRD الذي يحول هذه الذاكرة إلى مكان تتوضع فيه جميع البتات عنما يكون نظام التشغيل في حالة سبات وتبقى هذه المنطقة طالما بقي نظام التشغيل بحالة جيدة ولا يواجه أية مشاكل. وللتحكم بالجهاز الافتراضي يمكن استخدام أحد الأمرين VMLaunch و.VMResume.

خيارات واسعة من البيئة الافتراضية:

تعد البيئة الافتراضية ذات طبيعة ديناميكية مرنة تتماشى مع التطور التقني الذي يشهده قطاع تقنية المعلومات وتتنوع خيارات هذه البيئة فمن الممكن مثلا إنشاء بيئة افتراضية جزئية فبدلا من جعل كامل النظام بوضع افتراضي يمكن اختيار أجزاء من هذا النظام وتحويلها للحالة الافتراضية ليعمل كل برنامج على جهاز افتراضي بشكل مستقل عن بقية البرامج ولتوفر على المستخدم تكاليف شراء عدد من الحواسيب يساوي عدد المستخدمين الفعليين.

الحلول الأمنية للبيئة الافتراضية:

توفر البيئة الافتراضية قائمة طويلة من مزايا الحماية أهمها تفحص البرامج غير المناسبة والتعرف عليها ورفض تنزيلها على الجهاز الافتراضي، فعند تصفح مواقع الشابكة (الانترنت) مثلا يقوم النظام بجمع معلومات عن عملية التصفح هذه قبل إغلاق الجهاز الافتراضي وسيتعذر على الفيروسات الانتشار عن تشغيل المتصفح في المرات القادمة نظرا لتحميل النظام لملفات كوكيز المفيدة.

مستقبل البيئة الافتراضية:

تعد تقنية البيئة الافتراضية من التقنيات المتنامية وسيمضي بعض الوقت على تبني الحواسيب المكتبية لهذه البيئة نظرا لتوقف انتشار هذه التقنية على توفر دعم لها في أنظمة التشغيل المختلفة، وعدم ملائمتها للتطبيقات المستخدمة في هذا النوع من الحواسيب، ولكن إنتل حلت هذه المعضلة عن طريق تعاملها مع شركات برامج لتقديم دعم لها في برامجهم دون الاعتماد على دعم أنظمة التشغيل .ويتبنى مطورو البرامج وأنظمة التشغيل غير هذه التقنية إضافة إلى الشركات المتخصصة بإنتاج مكونات الحاسوب الصلبة أمثال آي بي إم وأيه إم دي وقد تعاني البيئة الافتراضية من سلبيات أهمها انخفاض أداء الجهاز الافتراضي (البيئة الافتراضية) مثلا عند تنزيل أكثر من نظام تشغيل على جهاز واحد. إضافة إلى التكاليف الباهظة، إلا أنه يمكن التغاضي عن جميع هذه السلبيات لحساب المزايا الإيجابية التي تقدمها هذه البيئة.

تحليل الحوسبة السحابية والمحاكاة الافتراضية:

أولًا :تعريف المفهومين

1. الحوسبة السحابيةCloud Computing

هي تقديم موارد الحوسبة (مثل الخوادم، والتخزين، وقواعد البيانات، والشبكات، والبرمجيات) عبر الإنترنت، حسب الطلب، ومن خلال نموذج الدفع مقابل الاستخدام.

أنواعها:

- **سحابة عامة (Public Cloud)**: مثلAmazon AWS ، Microsoft Azure.
- **سحابة خاصة (Private Cloud)**: داخل مؤسسة واحدة.
- **سحابة هجينة (Hybrid Cloud)**: مزيج من السحابة العامة والخاصة.

2. المحاكاة الافتراضيةVirtualization

هي تقنية تتيح إنشاء نسخ افتراضية (غير فعلية) من موارد الحوسبة، مثل أنظمة التشغيل، أو الخوادم، أو وحدات التخزين، لتعمل على جهاز مادي واحد.

أنواعها:

- **محاكاة الخوادم(Server Virtualization)**
- **محاكاة أنظمة التشغيل(OS Virtualization)**
- **محاكاة الشبكات(Network Virtualization)**
- **محاكاة التخزين(Storage Virtualization)**

ثانيًا :الفرق بين الحوسبة السحابية والمحاكاة الافتراضية

المقارنة	الحوسبة السحابية	المحاكاة الافتراضية
التقنية الأساسية	تعتمد على الإنترنت	تعتمد على البرامج لتقسيم الموارد
النطاق	أوسع، تشمل خدمات متعددة	محدودة في البنية التحتية فقط
التكلفة	حسب الاستخدام	تعتمد على البنية التحتية
الهدف	توفير موارد عند الطلب	تحسين استخدام الموارد الفعلية
العلاقة	تعتمد على المحاكاة الافتراضية	تُستخدم كأساس لتشغيل السحابة

ثالثًا :الفوائد

1. فوائد الحوسبة السحابية:

- خفض التكاليف التشغيلية.
- التوسع المرن حسب الحاجة.
- الوصول العالمي من أي مكان.
- صيانة وتحديث تلقائي.

2. فوائد المحاكاة الافتراضية:

- تقليل الحاجة للأجهزة الفيزيائية.
- زيادة كفاءة استغلال الموارد.
- تسهيل اختبار الأنظمة.
- تعزيز استمرارية الأعمال.

رابعًا :التحديات

في الحوسبة السحابية:

- القلق من الأمان والخصوصية.
- الاعتماد على الاتصال بالإنترنت.
- مشاكل التوافق مع الأنظمة القديمة.

في المحاكاة الافتراضية:

- إدارة الأعطال أصعب أحيانًا.
- أداء منخفض إذا لم تُدار بشكل جيد.
- تكاليف الترخيص في بعض البرمجيات.

خامسًا :التكامل بين الحوسبة السحابية والمحاكاة الافتراضية

غالبًا ما تُستخدم المحاكاة الافتراضية كأساس للحوسبة السحابية. فعلى سبيل المثال:

- مقدمو الخدمة السحابية يستخدمون المحاكاة الافتراضية لتشغيل مئات الخوادم الافتراضية على عدد قليل من الخوادم الفيزيائية.
- يساعد هذا على تقديم موارد مرنة وآمنة للمستخدمين دون الحاجة لإدارة الأجهزة الفعلية.

ما هو الفرق بين الحوسبة السحابية والمحاكاة الافتراضية ؟

الحوسبة السحابية والمحاكاة الافتراضية هما مفهومان مختلفان، على الرغم من أنهما قد يبدوان متشابهين .المحاكاة الافتراضية هي تقنية تسمح لك بإنشاء بيئات متعددة أو موارد مخصصة من جهاز مادي واحد، بينما الحوسبة السحابية هي نموذج لتوفير خدمات تكنولوجيا المعلومات عبر الإنترنت، والتي قد تتضمن المحاكاة الافتراضية كجزء من بنيتها التحتية .

المحاكاة الافتراضية:

التعريف:

هي تقنية تسمح لك بإنشاء عدة بيئات افتراضية (أجهزة افتراضية) على جهاز مادي واحد .

- **الهدف:**

تحسين استخدام الموارد المادية وتوفير بيئات معزولة لأغراض مختلفة (مثل تطوير واختبار البرمجيات) .

- **مثال:**

يمكنك تشغيل عدة أنظمة تشغيل (مثل ويندوز ولينكس) على جهاز واحد باستخدام المحاكاة الافتراضية .

الحوسبة السحابية:

- **التعريف:**

هي نموذج لتوفير خدمات تكنولوجيا المعلومات عبر الإنترنت (مثل الخوادم والتخزين وقواعد البيانات والتطبيقات) .

- **الهدف:**

توفير مرونة وقابلية للتوسع عند الطلب للمستخدمين، مع إمكانية الوصول إلى الموارد من أي مكان عبر الإنترنت .

- **مثال:**

استخدام خدمات مثل Google Driveأو Amazon Web Services حيث يتم توفير التخزين والحوسبة عبر الإنترنت .

- **العلاقة بينهما:**

يمكن أن تكون المحاكاة الافتراضية جزءًا من الحوسبة السحابية، حيث يتم استخدامها لتشغيل الأجهزة الافتراضية التي تدعم خدمات السحابة.

لكن الحوسبة السحابية أوسع نطاقًا من المحاكاة الافتراضية، فهي تشمل توفير الخدمات عبر الإنترنت وتجعل الموارد متاحة للعديد من المستخدمين.

بمعنى آخر، المحاكاة الافتراضية هي تقنية تستخدمها السحابة، بينما الحوسبة السحابية هي نموذج لتوفير الخدمات .

بيئات التحكم الإشرافي وجمع البيانات scada وبيئات الاستجابة الحظية والبنية التحتية الحساسة

الوحدة الخامسة:

بيئات التحكم الإشرافي وجمع البيانات scada وبيئات الاستجابة الحظية والبنية التحتية الحساسة

ما هو نظام سكادا:

نظام سكادا (SCADA) هو نظام حاسوبي يستخدم لمراقبة وتحكم العمليات الصناعية عن بعد .يجمع هذا النظام البيانات من أجهزة استشعار ومعدات ميدانية، ثم يعالجها ويحللها لعرضها على واجهة مستخدم رسومية (HMI) ليتمكن المشغلون من مراقبة العمليات واتخاذ القرارات المناسبة .

مكونات نظام سكادا الأساسية:

- **وحدات التحكم عن بعد:(RTUs)**

أجهزة كمبيوتر صناعية صغيرة توضع في مواقع ميدانية لجمع البيانات من أجهزة الاستشعار والمعدات .

- **وحدات التحكم الرئيسية:(MTUs)**

أجهزة كمبيوتر مركزية تتلقى البيانات من وحدات التحكم عن بعد (RTUs) وتعالجها .

- **واجهات المستخدم الرسومية:(HMIs)**

شاشات عرض تعرض البيانات والمعلومات للمشغلين، وتتيح لهم التحكم في العمليات .

- **نظام الاتصالات:**

يربط بين جميع مكونات نظام سكادا، سواء كانت شبكات سلكية أو لاسلكية .

- **برامج سكادا:**

توفر وظائف التحكم والمراقبة والتحليل وإعداد التقارير .

أهمية نظام سكادا:

- **زيادة الكفاءة:**

يتيح أتمتة العمليات الصناعية والتحكم فيها عن بعد، مما يقلل من التدخل اليدوي ويزيد من الإنتاجية.

- **المراقبة في الوقت الفعلي:**

يوفر مراقبة مستمرة للعمليات، مما يتيح اكتشاف المشاكل واتخاذ الإجراءات التصحيحية بسرعة.

- **تحسين السلامة:**

يوفر إنذارات عند حدوث مشكلات، مما يساعد على منع وقوع الحوادث والأضرار.

- **إمكانية الوصول عن بعد:**

يتيح للمشغلين مراقبة العمليات والتحكم فيها من أي مكان، مما يسهل إدارة العمليات واسعة النطاق.

مجالات استخدام نظام سكادا:

- **قطاع الطاقة:**

التحكم في محطات توليد الطاقة، وشبكات توزيع الكهرباء، وخطوط أنابيب النفط والغاز.

- **المرافق:**

إدارة شبكات المياه والصرف الصحي، وأنظمة معالجة المياه.

- **النقل:**

التحكم في حركة المرور، وأنظمة النقل العام.

- **الصناعات التحويلية:**

التحكم في عمليات التصنيع، وإدارة خطوط الإنتاج.

- **المباني الذكية:**

التحكم في أنظمة الإضاءة والتدفئة والتكييف وغيرها.

نظام تحصيل البيانات والتحكم:

نظام تحصيل البيانات والتحكم، المعروف أيضًا باسم نظام SCADA (Supervisory Control and Data Acquisition)، هو نظام لجمع ومراقبة البيانات والتحكم في العمليات الصناعية والعمليات الحيوية الأخرى .يتكون نظام SCADA من أجهزة وبرامج تتيح للمنظمات مراقبة العمليات والتحكم بها عن بعد .

شرح نظام :SCADA

- **التحكم الإشرافي:**

يتيح للمشغلين مراقبة العمليات والتحكم فيها من خلال واجهة مستخدم رسومية (.(HMI

- **اكتساب البيانات:**

يقوم بجمع البيانات من أجهزة الاستشعار والمعدات الميدانية ومعالجتها .

- **وحدات التحكم المنطقية القابلة للبرمجة:(PLCs)**

هي وحدات تحكم صغيرة تقوم بتنفيذ منطق التحكم في العمليات .

- **وحدات الطرفية البعيدة:(RTUs)**

تقوم بجمع البيانات من الأجهزة الميدانية وإرسالها إلى نظام .SCADA

- **واجهة الإنسان والآلة:(HMI)**

توفر واجهة رسومية للمشغلين لمراقبة العمليات والتحكم بها .

أمثلة على تطبيقات نظام :SCADA

- **محطات الطاقة :**لمراقبة وتعديل إنتاج الطاقة والتحكم في شبكات توزيع الكهرباء.
- **محطات معالجة المياه :**لمراقبة وضبط تدفق المياه ومعالجة مياه الصرف الصحي.
- **خطوط الأنابيب :**لمراقبة تدفق النفط والغاز والتحكم فيه.
- **المصانع :**لمراقبة العمليات الصناعية والتحكم فيها.
- **النقل :**لمراقبة حركة القطارات والحافلات وتنظيم حركة المرور .

أهمية نظام :SCADA

- **زيادة الكفاءة :**من خلال أتمتة العمليات والتحكم فيها عن بعد.
- **تحسين السلامة :**من خلال توفير مراقبة في الوقت الفعلي وتنبيهات مبكرة.
- **تحسين إدارة البيانات :**من خلال جمع وتخزين كميات كبيرة من البيانات.
- **تحسين الموثوقية :**من خلال توفير قدرات مراقبة وتحكم عن بعد.
- **خفض التكاليف :**من خلال تقليل الحاجة إلى التدخل اليدوي .

أنظمة التحكم الإشرافي وتحصيل البيانات

نظام التحكم الإشرافي وتحصيل البيانات (SCADA) هو نظام حاسوبي يستخدم لمراقبة والتحكم في العمليات الصناعية .يجمع النظام البيانات من أجهزة الاستشعار والمعدات، ويقوم بتحليلها، ثم يعرضها للمشغلين لاتخاذ قرارات بشأن العمليات .

مكونات نظام :SCADA

- **أجهزة جمع البيانات:**

مثل المستشعرات والمحولات، التي تجمع البيانات من العمليات الصناعية.

- **وحدات التحكم:**

مثل وحدات التحكم المنطقية القابلة للبرمجة (PLCs) ووحدات التحكم عن بعد(RTUs) ، التي تعالج البيانات وتتحكم في العمليات.

- **واجهات المستخدم الرسومية:(HMIs)**

التي تعرض البيانات للمشغلين وتسمح لهم بالتحكم في العمليات.

- **شبكة الاتصالات:**

التي تربط بين جميع المكونات .

وظائف نظام :SCADA

- **جمع البيانات:**

جمع البيانات من مجموعة متنوعة من المصادر.

- **معالجة البيانات:**

تحليل البيانات وتحديد المشاكل المحتملة.

- **التحكم في العمليات:**

التحكم في العمليات الصناعية من خلال واجهة المستخدم الرسومية.

- **تسجيل البيانات:**

تسجيل البيانات لاتخاذ القرارات وتحليلها في المستقبل.

- **التنبيه:**

إرسال تنبيهات للمشغلين في حالة وجود مشاكل .

أمثلة على استخدامات :SCADA

- **محطات توليد الطاقة :**لمراقبة وتحكم في توليد الطاقة الكهربائية.
- **محطات معالجة المياه :**لمراقبة وتحكم في معالجة المياه.
- **شبكات توزيع الطاقة :**لمراقبة وتحكم في توزيع الطاقة الكهربائية.
- **خطوط الأنابيب :**لمراقبة وتحكم في نقل السوائل.
- **العمليات الصناعية المختلفة :**في مختلف الصناعات مثل النفط والغاز، والتصنيع، والنقل .

أهمية نظام :SCADA

- **تحسين الكفاءة:**

يسمح نظام SCADA للمشغلين بمراقبة العمليات وتحسينها، مما يؤدي إلى زيادة الكفاءة وتقليل التكاليف.

- **تحسين السلامة:**

يتيح نظام SCADA للمشغلين اكتشاف المشاكل المحتملة والتعامل معها قبل أن تتسبب في أي ضرر، مما يحسن السلامة.

- **زيادة الإنتاجية:**

يسمح نظام SCADA للمشغلين بمراقبة العمليات والتحكم فيها عن بعد، مما يزيد من الإنتاجية.

- **توفير الوقت والجهد:**

يتيح نظام SCADA للمشغلين التحكم في العمليات عن بعد، مما يوفر الوقت والجهد.

- **اتخاذ قرارات أفضل:**

يوفر نظام SCADA بيانات دقيقة وفي الوقت المناسب للمشغلين لاتخاذ قرارات أفضل بشأن العمليات.

الشبكات المحلية والشبكات اللاسلكية والانترنت

الوحدة السادسة

الشبكات المحلية والشبكات اللاسلكية والانترنت

تعريف الشبكة المحلية:

الشبكة المحلية (LAN) هي مجموعة من الأجهزة المتصلة ببعضها البعض ضمن منطقة جغرافية محدودة، مثل مبنى أو مكتب أو منزل .تتيح هذه الشبكة للأجهزة مشاركة الموارد والبيانات، مثل الملفات والطابعات والإنترنت .

شرح تفصيلي:

- **الموقع الجغرافي:**

الشبكات المحلية تقتصر على مساحة صغيرة نسبيًا، مما يميزها عن الشبكات الأوسع نطاقًا مثل) WAN الشبكة الواسعة.

- **الأجهزة المتصلة:**

تشمل الأجهزة المتصلة بالشبكة المحلية أجهزة الكمبيوتر، والطابعات، والخوادم، والأجهزة الذكية، وغيرها.

- **المشاركة:**

تتيح الشبكة المحلية مشاركة الموارد بين الأجهزة المتصلة، مما يعزز التعاون والكفاءة.

- **أمثلة:**
  - شبكة منزلية متصلة بالإنترنت عبر جهاز توجيه (راوتر) .
  - شبكة مكتبية في شركة صغيرة .
  - شبكة في مبنى مدرسة .
- **التحكم والإدارة:**

غالبًا ما يتم التحكم في معدات الشبكة المحلية وإدارتها محليًا، سواء من قبل مالك الشبكة أو من قبل مزود خدمة محلي .

- **أهمية الشبكات المحلية:**
- **الكفاءة :**تمكن الشبكات المحلية من مشاركة الموارد والبيانات بسرعة، مما يزيد من كفاءة العمل .
- **التعاون :**تسهل الشبكات المحلية التعاون بين المستخدمين من خلال مشاركة الملفات والوصول إلى التطبيقات المشتركة .
- **الإنتاجية :**توفر الشبكات المحلية بيئة عمل متصلة، مما يساهم في زيادة الإنتاجية .
- **الأمان :**تتيح الشبكات المحلية التحكم في الوصول إلى البيانات والموارد، مما يعزز الأمان .

ما هي أنواع الشبكات:

هناك عدة أنواع من الشبكات، ويمكن تصنيفها بناءً على عدة معايير، مثل النطاق الجغرافي، والتقنية المستخدمة، والغرض من الشبكة .من بين الأنواع الأكثر شيوعًا:

1. حسب النطاق الجغرافي:

- **الشبكة المحلية (LAN)** تغطي مساحة محدودة، مثل منزل أو مكتب أو مبنى .
- **شبكة المنطقة الحضارية (MAN)** تغطي مساحة أكبر منLAN ، مثل مدينة أو منطقة .
- **شبكة المنطقة الواسعة (WAN)** تغطي مساحة واسعة جدًا، مثل بلد أو قارة .

2. حسب التقنية المستخدمة:

- **الشبكات السلكية :(Wired Networks)** تستخدم الكابلات لنقل البيانات.
- الشبكات اللاسلكية **:(Wireless Networks)** تستخدم موجات الراديو لنقل البيانات.
- **الشبكات السحابية :(Cloud Networks)** تستخدم خدمات الحوسبة السحابية لتقديم موارد الشبكة .

3. حسب الغرض من الشبكة:

- **شبكة شخصية (PAN)**

تربط الأجهزة الشخصية مثل الهواتف الذكية والأجهزة اللوحية .

- **شبكات الشركات (CAN)**

تربط أجهزة الكمبيوتر والأجهزة الأخرى داخل شركة .

- **شبكات الإنترنت (Internet)**

شبكة عالمية تربط شبكات متعددة .

- **شبكات الأجهزة (IoT Networks)**

تربط الأجهزة المتصلة بالإنترنت (مثل أجهزة الاستشعار والأجهزة المنزلية الذكية) .

- **شبكات المنطقة المحلية الافتراضية(VLAN)**

شبكات افتراضية داخل شبكةLAN ، تسمح بتقسيم الشبكة منطقياً .

4. حسب طوبولوجيا الشبكة (الشكل الهندسي):

- **الشبكة النجمية :(Star Topology)** جميع الأجهزة متصلة بجهاز مركزي (مثل الموجه).
- **الشبكة الحلقية :(Ring Topology)** الأجهزة متصلة في حلقة.
- **الشبكة الخطية :(Bus Topology)** الأجهزة متصلة بخط واحد.
- **الشبكة المتداخلة :(Mesh Topology)** الأجهزة متصلة ببعضها البعض بطرق متعددة.
- **الشبكة الشجرية :(Tree Topology)** شبكة هرمية.
- **الشبكة الهجينة :(Hybrid Topology)** مزيج من أنواع مختلفة من الطوبولوجيات .

الشبكات السلكية واللاسلكية والانترنت

الشبكات السلكية واللاسلكية هي طرق لنقل البيانات بين الأجهزة المختلفة، وتستخدم الإنترنت كشبكة واسعة النطاق للاتصال .الشبكات السلكية تعتمد على الكابلات، بينما الشبكات اللاسلكية تستخدم الموجات الراديوية .

الشبكات السلكية:

- **تعتمد على الكابلات:**

لنقل البيانات بين الأجهزة، مثل الأسلاك النحاسية أو الألياف البصرية .

- **استقرار عالي وسرعات مميزة:**

توفر سرعات عالية ومستقرة، مما يجعلها مناسبة للمكاتب والمؤسسات ومراكز البيانات .

- **أكثر أمانًا:**

تُعتبر أكثر أمانًا من الشبكات اللاسلكية، حيث يصعب الوصول إليها من الخارج .

- **أمثلة:**

الشبكات المستخدمة في المنازل والمكاتب والمؤسسات التي تعتمد على الكابلات لتوصيل الأجهزة بالإنترنت أو بشبكة محلية .

الشبكات اللاسلكية:

- **تعتمد على الموجات الراديوية:**

لنقل البيانات دون الحاجة إلى كابلات، مما يوفر حرية التنقل .

- **أكثر مرونة:**

تسمح للأجهزة بالاتصال بالشبكة من أي مكان داخل نطاق الشبكة .

- **أكثر انتشارًا في المنازل والأماكن العامة:**

تستخدم على نطاق واسع في المنازل الذكية والأماكن العامة مثل المقاهي والفنادق .

- **أمثلة:**

شبكات الواي فاي (Wi-Fi) وشبكات الهاتف المحمول .

الإنترنت:

- **شبكة واسعة النطاق:**

شبكة عالمية تربط بين شبكات محلية مختلفة، سواء كانت سلكية أو لاسلكية .

- **أساس الاتصال العالمي:**

يسمح للأجهزة بالاتصال ببعضها البعض من جميع أنحاء العالم .

- **يعتمد على الشبكات السلكية واللاسلكية:**

يستخدم الشبكات السلكية واللاسلكية لتوصيل الأجهزة بالشبكة العالمية .

الاختلافات الرئيسية:

الشبكات اللاسلكية	الشبكات السلكية	الميزة
موجات راديوية	كابلات	وسيلة الاتصال
أقل سرعة وأكثر عرضة للتداخل	أسرع وأكثر استقرارًا	السرعة
أقل أمانًا، خاصةً بدون تشفير	أكثر أمانًا	الأمان
أكثر مرونة وحرية في الحركة	أقل مرونة	المرونة

أهمية الشبكات السلكية واللاسلكية:

- **توفير الاتصال:**

تمكن الأجهزة من الاتصال بالشبكات المحلية والعالمية.

- **تبادل البيانات:**

تسهل تبادل المعلومات والملفات بين الأجهزة.

- **الوصول إلى الموارد:**

تتيح الوصول إلى الإنترنت والخدمات عبر الإنترنت.

- **دعم التطبيقات الحديثة:**

تدعم تطبيقات مثل الاتصالات الصوتية والفيديو والاجتماعات عبر الإنترنت .

ما الفرق بين الشبكة المحلية LAN والشبكة الواسعة WAN

الشبكة المحلية (LAN) والشبكة الواسعة (WAN) هما نوعان من شبكات الكمبيوتر، لكنهما يختلفان في النطاق الجغرافي ونوع الاتصالات المستخدمة .بشكل عام، تربط LAN الأجهزة ضمن منطقة محدودة مثل منزل أو مكتب، بينما تربط WAN الأجهزة عبر مساحة واسعة، مثل مدينة أو حتى دول .

الشبكة المحلية (LAN)

- **النطاق:**

تغطي منطقة جغرافية صغيرة (مثل منزل، مكتب، مبنى).

- **الاتصال:**

تستخدم اتصالات سلكية (مثل كابلات الإيثرنت) أو لاسلكية (مثل Wi-Fi)داخل نفس الموقع.

- **السرعة:**

عادةً ما تكون أسرع وأكثر موثوقية داخل نطاقها.

- **مثال:**

ربط أجهزة الكمبيوتر والطابعات في مكتب واحد بشبكة واحدة .

الشبكة الواسعة (WAN)

- **النطاق:**

تغطي مساحة جغرافية واسعة (مثل مدينة، بلد، أو حتى العالم).

- **الاتصال:**

تستخدم مجموعة متنوعة من الاتصالات، بما في ذلك خطوط الهاتف، الأقمار الصناعية، أو شبكات الإنترنت.

- **السرعة:**

قد تكون أبطأ من LAN بسبب المسافة الطويلة التي يجب أن تقطعها البيانات.

- **مثال:**

ربط شبكات LAN المختلفة في مواقع مختلفة معًا (مثل ربط مكاتب الشركة في مدن مختلفة) .

التعينات الشبكية

الوحدة السابعة

التعينات الشبكية

ما هي تقنية الشبكات

تقنية الشبكات هي مجموعة من التقنيات والأدوات التي تمكن الأجهزة من الاتصال وتبادل البيانات والمعلومات عبر شبكة .تتضمن هذه التقنيات الأجهزة المادية مثل أجهزة التوجيه والمبدلات، والبروتوكولات التي تحدد كيفية نقل البيانات، والبرامج التي تدير الشبكة وتراقبها .تهدف تقنية الشبكات إلى توفير وسائل فعالة وموثوقة للاتصال وتبادل الموارد بين الأجهزة المختلفة.

شرح مفصل:

تشمل تقنية الشبكات عدة جوانب رئيسية:

1. **الأجهزة المادية:**

تشمل أجهزة التوجيه (routers) التي تحدد مسار البيانات، والمبدلات (switches) التي تربط الأجهزة داخل الشبكة المحلية، والكوابل والألياف الضوئية التي تنقل البيانات، بالإضافة إلى بطاقات الشبكة (network interface cards) الموجودة في كل جهاز.

2. **البروتوكولات:**

هي مجموعة من القواعد والتعليمات التي تحدد كيفية تبادل البيانات بين الأجهزة .من أشهر هذه البروتوكولاتTCP/IP ، وهو البروتوكول الأساسي للإنترنت .

3. **الشبكات المحلية:(LAN)**

هي شبكات تربط الأجهزة في منطقة محدودة، مثل مكتب أو منزل .

4. **الشبكات الواسعة:(WAN)**

هي شبكات تربط الأجهزة في مناطق جغرافية واسعة، مثل شبكة الإنترنت .

5. **الشبكات اللاسلكية:(WLAN)**

هي شبكات تستخدم تقنيات لاسلكية مثل Wi-Fi للاتصال وتبادل البيانات .

6. إدارة الشبكة:

تتضمن مراقبة أداء الشبكة، وتحديد المشاكل وإصلاحها، وتأمين الشبكة من التهديدات الأمنية .

أهمية تقنية الشبكات:

تعد تقنية الشبكات أساسية في العصر الحديث، حيث تعتمد عليها العديد من التطبيقات والخدمات، مثل:

- **الاتصالات:**

تتيح الشبكات إجراء المكالمات الهاتفية، وإرسال الرسائل النصية، وإجراء مكالمات الفيديو.

- **تبادل البيانات:**

تمكن الشبكات من مشاركة الملفات، والوصول إلى قواعد البيانات، والتعاون في العمل.

- **الوصول إلى الإنترنت:**

تعتمد جميع الأجهزة المتصلة بالإنترنت على تقنية الشبكات للاتصال بالشبكة العالمية .

- **الخدمات السحابية:**

تعتمد الخدمات السحابية على الشبكات لتخزين البيانات ومعالجتها .

- **إنترنت الأشياء:(IoT)**

تتيح الشبكات ربط الأجهزة المتصلة ببعضها البعض لتبادل البيانات وتنفيذ الأوامر .

الاتصالات والتكنولوجيا في الشبكات الإلكترونية

تكنولوجيا المعلومات والاتصالات (ICT) هي البنية التحتية والمكونات التي تمكن الحوسبة الحديثة، وتهدف إلى تحسين طريقة إنشاء البيانات والمعلومات ومعالجتها ومشاركتها، بالإضافة إلى تطوير القدرات في مختلف المجالات .تشمل تكنولوجيا المعلومات والاتصالات جميع الأجهزة ومكونات الشبكات والتطبيقات التي تساعد الأفراد والمؤسسات على التفاعل في العالم الرقمي .

أهمية تكنولوجيا المعلومات والاتصالات:

- **تحسين التواصل:**

تمكن من التواصل الفعال عبر المسافات والوقت.

- **تسهيل الوصول إلى المعلومات:**

توفر وصولاً سريعًا وسهلاً إلى المعلومات والخدمات.

- **تطوير العمليات التجارية:**

تساعد في تحسين العمليات التجارية وتبسيطها.

- **دعم التعليم والتعلم:**

توفر فرصًا للتعليم عن بعد والتعلم عبر الإنترنت.

- **توفير الترفيه والاستجمام:**

تتيح طرقًا ممتعة للترفيه والتواصل الاجتماعي .

تطبيقات تكنولوجيا المعلومات والاتصالات:

- **شبكات الحاسوب:**

تتضمن شبكاتLAN ، WAN، MAN، وغيرها، وتستخدم لنقل البيانات وتبادل المعلومات .

- **تكنولوجيا الاتصالات:**

تشمل الهواتف المحمولة، والإنترنت، والأقمار الصناعية، وغيرها من وسائل الاتصال .

- **البرمجيات والتطبيقات:**

تستخدم لتطوير البرامج والأجهزة وتلبية احتياجات الاتصالات والأعمال .

- **الشبكات الذكية:**

تستخدم في مجالات مثل الطاقة المتجددة والمركبات الكهربائية، وتحسين كفاءة الشبكات .

- **تقنيات الذكاء الاصطناعي:**

تستخدم في تحليل سلوك الشبكات والتنبؤ بالأعطال .

كيف تعمل شبكات الكمبيوتر مع الإنترنت؟

تعمل شبكات الكمبيوتر مع الإنترنت عن طريق ربط الأجهزة معًا عبر اتصالات سلكية أو لاسلكية .تسمح هذه الاتصالات بنقل البيانات بين الأجهزة، مما يتيح التواصل ومشاركة الموارد مثل الملفات والوصول إلى الإنترنت .

كيف تعمل بالتفصيل:

1. **شبكات الكمبيوتر:**

هي مجموعة من الأجهزة (مثل أجهزة الكمبيوتر، والهواتف الذكية، والأجهزة اللوحية) المتصلة ببعضها البعض، وتسمح بمشاركة الموارد والبيانات .

2. **الإنترنت:**

هو شبكة عالمية تربط شبكات الكمبيوتر المختلفة معًا، مما يتيح للأجهزة المتصلة بها التواصل مع بعضها البعض ومشاركة الموارد عبر مسافات كبيرة .

3. **أجهزة التوجيه:(Routers)**

تلعب أجهزة التوجيه دورًا حاسمًا في توجيه حركة البيانات عبر الإنترنت .فهي تحدد أفضل مسار للبيانات للانتقال من جهاز إلى آخر، مما يضمن وصولها إلى وجهتها الصحيحة .

4. **عناوين:IP**

لكل جهاز متصل بالإنترنت عنوان IP فريد يميزه عن غيره .يتم استخدام هذه العناوين لتحديد وجهة البيانات .

5. **بروتوكولات الإنترنت:**

تستخدم شبكات الكمبيوتر بروتوكولات (مجموعة من القواعد) لإدارة الاتصال وتبادل البيانات .على سبيل المثال، بروتوكول TCP/IP هو البروتوكول الأساسي المستخدم في الإنترنت .

6. **أمثلة على الاستخدام:**

عند تصفح الإنترنت، يقوم جهازك بإرسال طلب إلى خادم الويب الذي يحتوي على الصفحة التي تريدها .ثم يقوم الخادم بإرسال البيانات المكونة للصفحة عبر الإنترنت إلى جهازك، حيث يتم عرضها بواسطة متصفح الويب .

مكونات أمن الشبكات

الوحدة الثامنة
مكونات امن الشبكات

ما هو أمن الشبكات

أمن الشبكات هو مجموعة من التدابير والإجراءات الأمنية التي تهدف إلى حماية شبكات الحاسوب من التهديدات السيبرانية المختلفة، مثل الاختراقات والبرمجيات الخبيثة وهجمات حجب الخدمة .يهدف أمن الشبكات إلى ضمان توفر البيانات وسلامتها وسريتها، بالإضافة إلى الحفاظ على استمرارية عمل الشبكة .

يشمل أمن الشبكات جوانب مختلفة، منها:

- **التحكم في الوصول:**

يهدف إلى تحديد من يمكنه الوصول إلى موارد الشبكة ومنع الوصول غير المصرح به .

- **الحماية من البرمجيات الخبيثة:**

يشمل استخدام برامج مكافحة الفيروسات وجدران الحماية للكشف عن البرامج الضارة ومنعها من الانتشار .

- **تشفير البيانات:**

يستخدم لحماية البيانات الحساسة أثناء نقلها عبر الشبكة .

- **الشبكات الخاصة الافتراضية:(VPN)**

توفر اتصالات آمنة عبر الإنترنت، خاصةً عند استخدام شبكات غير آمنة .

- **مراقبة الشبكة:**

تهدف إلى اكتشاف التهديدات الأمنية المحتملة والتحقيق فيها .

- **تحديثات البرامج:**

ضرورية لسد الثغرات الأمنية في الأنظمة والتطبيقات .

- **بشكل عام، يمثل أمن الشبكات جزءًا أساسيًا من الأمن السيبراني، ويهدف إلى حماية البنية التحتية لتكنولوجيا المعلومات للمؤسسات من الهجمات الإلكترونية .**

كيف يعمل مجال أمن الشبكات

يعمل مجال أمن الشبكات على حماية الشبكات والبيانات من الوصول غير المصرح به، والاستخدام الضار، والتعطيل، والتعديل، والإفشاء .يتم ذلك من خلال تطبيق مجموعة من التدابير الدفاعية، بما في ذلك الأجهزة والبرامج والسياسات والممارسات .تهدف هذه التدابير إلى ضمان سرية وسلامة وتوافر البيانات والمعلومات المتداولة عبر الشبكة .

كيف يعمل أمن الشبكات بالتفصيل:

1. الدفاع المتعمق:

يعتمد أمن الشبكات على مبدأ "الدفاع المتعمق"، وهو عبارة عن إنشاء طبقات متعددة من الدفاعات لتقليل خطر نقطة فشل واحدة .يتضمن ذلك استخدام مجموعة متنوعة من التقنيات والتدابير الأمنية، مثل:

- **جدران الحماية :**تعمل على تصفية حركة مرور الشبكة ومنع الوصول غير المصرح به .
- **أنظمة كشف التسلل :(IDS)** تراقب حركة مرور الشبكة بحثًا عن الأنشطة الضارة وتنبيه المسؤولين .
- **شبكات :VPN** توفر اتصالًا آمنًا ومشفرًا عبر شبكات غير آمنة .
- **برامج مكافحة الفيروسات :**تحمي الأجهزة من البرامج الضارة .
- **المصادقة متعددة العوامل :(MFA)** تتطلب من المستخدمين تقديم أكثر من طريقة للتحقق من هويتهم، مثل كلمة المرور وبصمة الوجه .
- **تشفير البيانات :**يحمي البيانات من خلال تحويلها إلى شكل غير مقروء لا يمكن فك تشفيره إلا بواسطة الأطراف المصرح لها .
- **أنظمة إدارة معلومات الأمن والأحداث :(SIEM)** تجمع وتحلل بيانات الأمان من مصادر مختلفة لتقديم رؤية شاملة لأمان الشبكة .

2. التحكم في الوصول:

يضمن أمن الشبكات وصول المستخدمين المصرح لهم فقط إلى موارد الشبكة .يتم ذلك من خلال:

- **إدارة الهويات :**تحديد المستخدمين والمجموعات المصرح لهم بالوصول إلى موارد الشبكة .
- **إدارة الأذونات :**تحديد مستوى الوصول المسموح به لكل مستخدم أو مجموعة .

3. التدابير الأمنية الوقائية:

تشمل مجموعة من التدابير التي تهدف إلى منع وقوع الحوادث الأمنية، مثل:

- **توعية المستخدمين :**توعية المستخدمين بأفضل الممارسات الأمنية وكيفية تجنب الوقوع ضحية للهجمات .
- **تحديثات البرامج :**تحديث البرامج بانتظام لإصلاح الثغرات الأمنية .
- **إدارة كلمات المرور :**استخدام كلمات مرور قوية وتغييرها بانتظام .

4. التدابير الأمنية الاستباقية:

تشمل مجموعة من التدابير التي تهدف إلى الكشف عن التهديدات والاستجابة لها في الوقت المناسب، مثل:

- **مراقبة الشبكة :**مراقبة حركة مرور الشبكة بحثًا عن أي علامات على نشاط ضار .
- **تحليل السجل :**تحليل سجلات النظام بحثًا عن أي علامات على الاختراقات .
- **الاستجابة للحوادث :**اتخاذ الإجراءات اللازمة لاحتواء الحوادث الأمنية والتخفيف من آثارها .

5. أمن الشبكات السحابية:

- **تتطلب الحوسبة السحابية تدابير أمنية إضافية لحماية البيانات والتطبيقات المخزنة على السحابة .**

6. أمن البريد الإلكتروني:

يهدف إلى حماية حسابات البريد الإلكتروني من الوصول غير المصرح به والتصيد الاحتيالي .

- **باختصار، يعمل أمن الشبكات من خلال مجموعة متكاملة من التدابير الأمنية التي تهدف إلى حماية الشبكات والبيانات من التهديدات المختلفة، مما يضمن سلامة الشبكات واستمراريتها في العمل بشكل آمن .**

أنواع أمن الشبكات

تشمل أنواع أمن الشبكات العديد من التقنيات والتدابير التي تهدف إلى حماية الشبكات من التهديدات المختلفة .من بين هذه الأنواع :جدران الحماية، أنظمة كشف التطفل(IDS) ، أنظمة منع التطفل(IPS) ، الشبكات الخاصة الافتراضية(VPN) ، منع فقدان البيانات (DLP)، التشفير، وإدارة الهوية والوصول .(IAM)

أمثلة على أنواع أمن الشبكات:

- **جدران الحماية:(Firewalls)**

تعمل كحاجز بين الشبكة الداخلية والشبكات الخارجية (مثل الإنترنت)، وتراقب حركة المرور الواردة والصادرة لتحديد ومنع الوصول غير المصرح به .

- **أنظمة كشف التطفل:(IDS)**

تراقب حركة المرور بحثًا عن الأنشطة المشبوهة أو الضارة وتحذر المسؤولين عند اكتشاف تهديد محتمل .

- **أنظمة منع التطفل:(IPS)**

تتجاوز IDS من خلال منع التهديدات واعتراضها بشكل فعال، وليس مجرد اكتشافها .

- **الشبكات الخاصة الافتراضية:(VPN)**

توفر اتصالًا آمنًا ومشفرًا عبر شبكة عامة (مثل الإنترنت)، مما يسمح للمستخدمين بالوصول إلى الموارد الخاصة عن بعد بأمان .

- **منع فقدان البيانات:(DLP)**

تساعد في تحديد واكتشاف ومنع تسرب البيانات الحساسة خارج الشبكة، سواء عن قصد أو غير قصد .

- **التشفير:(Encryption)**

يحول البيانات إلى شكل غير قابل للقراءة (مشفر) بحيث لا يمكن لأي شخص غير مصرح له فك تشفيرها وقراءتها .

- **إدارة الهوية والوصول:(IAM)**

تتيح للمسؤولين التحكم في وصول المستخدمين إلى موارد الشبكة المختلفة وتحديد مستوى الوصول لكل مستخدم بناءً على هويته .

أمثلة إضافية:

- **أمان المتصفح:**

حماية المتصفحات من التهديدات عبر الإنترنت .

- **أمان مراكز البيانات:**

حماية البنية التحتية المادية والافتراضية لمراكز البيانات .

- **أمان التطبيقات:**

حماية التطبيقات من نقاط الضعف والثغرات الأمنية .

- **أمان الشبكات اللاسلكية:**

حماية الشبكات اللاسلكية من الوصول غير المصرح به .

- **برامج مكافحة الفيروسات:**

تكتشف وتحذف البرامج الضارة والفيروسات .

- **إدارة المعلومات الأمنية والأحداث:(SIEM)**

تجمع وتحلل معلومات الأمان من مصادر مختلفة لتقديم رؤية شاملة للأحداث الأمنية .

ملاحظة: تتداخل بعض هذه الأنواع وقد يتم دمجها في حلول أمنية شاملة .على سبيل المثال، غالبًا ما تستخدم جدران الحماية من الجيل التالي (NGFW)قدرات اكتشاف التطفل ومنع التهديدات المتقدمة .

مكونات أمن الشبكات:

تتكون شبكات أمن الشبكات من عدة مكونات أساسية تعمل معًا لتوفير الحماية للشبكة وبياناتها من التهديدات السيبرانية .تشمل هذه المكونات الرئيسية :جدران الحماية، وأنظمة منع التطفل (IPS)، وأنظمة كشف التطفل(IDS) ، والشبكات الخاصة الافتراضية(VPN) ، وإدارة معلومات وأحداث الأمان .(SIEM)

المكونات الرئيسية لأمن الشبكات:

- **جدران الحماية:(Firewall)**

تعمل كحاجز بين شبكة داخلية موثوقة وشبكة خارجية غير موثوقة (مثل الإنترنت)، وتنظم حركة المرور الواردة والصادرة بناءً على قواعد أمنية محددة مسبقًا .

- **أنظمة منع التطفل:(IPS)**

تقوم بمراقبة حركة مرور الشبكة للكشف عن الأنشطة الضارة وحظرها قبل أن تصل إلى الشبكة .

- **أنظمة كشف التطفل:(IDS)**

تراقب حركة مرور الشبكة للكشف عن الأنشطة الضارة، ولكنها لا تحظرها، بل تقوم بتنبيه المسؤولين .

- **الشبكات الخاصة الافتراضية:(VPN)**

توفر اتصالاً آمنًا ومشفرًا بين جهازين أو شبكتين عبر شبكة غير آمنة (مثل الإنترنت) .

- **إدارة معلومات وأحداث الأمان:(SIEM)**

تجمع وتنسق بيانات الأمان من مصادر مختلفة لتوفير رؤية شاملة لتهديدات الشبكة .

مكونات إضافية:

- **البرامج المضادة للفيروسات والبرامج الضارة:**

تحمي الشبكة من الفيروسات وبرامج الفدية والبرامج الضارة الأخرى .

- **أمن التطبيقات والويب والبريد الإلكتروني:**

تأمين التطبيقات والبرامج المستخدمة على الشبكة، بالإضافة إلى تأمين حركة مرور الويب والبريد الإلكتروني .

- **التحكم في الوصول إلى الشبكة:(NAC)**

تحديد المستخدمين والأجهزة المصرح لها بالوصول إلى الشبكة .

- **منع فقدان البيانات:(DLP)**

تساعد في حماية البيانات الحساسة من التسرب أو السرقة .

- **التشفير:**

يحمي البيانات من خلال تحويلها إلى شكل غير مقروء إلا للشخص المصرح له .

أهمية أمن الشبكات:

أمن الشبكات أمر بالغ الأهمية لحماية الشبكات من التهديدات السيبرانية، حيث أن أي اختراق للشبكة يمكن أن يؤدي إلى خسائر كبيرة في البيانات والسمعة، بالإضافة إلى توقف العمل .

أنظمة رصد ومنع التسلل

الوحدة التاسعة
أنظمة رصد ومنع التسلل

نظام منع التسلل:

نظام منع التسلل (IPS) هو نظام أمان شبكة يراقب حركة مرور الشبكة بحثًا عن أي نشاط ضار ويحاول منع هذه الأنشطة .يقوم نظام منع التسلل بذلك عن طريق فحص حركة المرور الواردة، واكتشاف التهديدات المحتملة، واتخاذ إجراءات لمنعها، مثل حظر عناوين IP أو إسقاط الحزم الضارة.

شرح تفصيلي:

- **نظام منع التسلل (IPS) هو تطور لأنظمة كشف التسلل:(IDS)**

بينما تقوم أنظمة كشف التسلل (IDS) بمراقبة حركة مرور الشبكة والإبلاغ عن التهديدات المحتملة، فإن أنظمة منع التسلل (IPS) تتجاوز ذلك وتتخذ إجراءات لمنع التهديدات .

وظائف نظام منع التسلل:

- **مراقبة حركة مرور الشبكة :**يقوم نظام IPS بمراقبة حركة مرور الشبكة باستمرار بحثًا عن أي أنماط أو سلوكيات غير عادية قد تشير إلى وجود هجوم .
- **كشف التهديدات :**يستخدم نظام IPS تقنيات مختلفة، مثل البحث عن التوقيعات المعروفة للتهديدات (signature-based detection)والكشف عن السلوك المشبوه(anomaly-based detection) ، لتحديد التهديدات المحتملة .
- **منع التهديدات :**بمجرد اكتشاف تهديد، يقوم نظام IPS باتخاذ إجراءات لمنعه، مثل حظر عناوين IP الضارة، وإسقاط الحزم الضارة، وتنبيه المسؤولين .

أهمية نظام منع التسلل:

- **حماية الشبكة :**يوفر نظام IPS طبقة إضافية من الحماية للشبكة من خلال منع التهديدات قبل أن تصل إلى الأجهزة أو الأنظمة .
- **تقليل المخاطر :**يساعد في تقليل مخاطر اختراق البيانات والتسلل غير المصرح به .
- **تحسين الاستجابة للحوادث :**من خلال منع التهديدات تلقائيًا، يساعد نظام IPS في تقليل تأثير الهجمات الناجحة وتسهيل الاستجابة للحوادث بشكل أسرع .

أمثلة على أنظمة منع التسلل:

- **جدران الحماية لتطبيقات الويب :**تستخدم لحماية تطبيقات الويب من الهجمات .
- **حلول تصفية حركة المرور :**تستخدم لتصفية حركة المرور غير المرغوب فيها أو الضارة .
- **أنظمة منع التسلل المستقلة :**أجهزة أو برامج مصممة خصيصًا لمنع التهديدات .

- **الدمج مع حلول أمنية أخرى :**يمكن دمج أنظمة IPS في حلول إدارة التهديدات الموحدة (UTM) أو جدران الحماية من الجيل التالي .

سلبيات نظام منع التسلل:

- **إمكانية الحظر الخاطئ :**(False Positives) قد يقوم نظام IPS أحيانًا بحظر حركة مرور شرعية عن طريق الخطأ .
- **الحاجة إلى الضبط الدقيق :**يتطلب نظام IPS إعدادًا وتكوينًا دقيقين لضمان فعاليته ومنع التأثير على أداء الشبكة .
- **استهلاك الموارد :**قد يتطلب نظام IPS قدرًا كبيرًا من الموارد لمعالجة وتحليل حركة المرور.

كيف يعمل معرف الهوية؟

يعمل معرف الهوية، سواء كان رقميًا أو ماديًا، على التحقق من هوية الشخص من خلال مقارنة المعلومات المقدمة بمصدر موثوق .يهدف ذلك إلى التأكد من أن الشخص الذي يدعي هوية معينة هو بالفعل الشخص المعني .تتضمن العملية عادةً استخدام معلومات شخصية، ووثائق رسمية، و/أو بيانات بيومترية لإنشاء هوية رقمية أو التحقق من هوية شخص ما.

شرح تفصيلي:

- **التحقق من الهوية الرقمية:**

يشمل هذا النوع من التحقق استخدام معلومات مثل اسم المستخدم وكلمة المرور، بالإضافة إلى معلومات إضافية مثل رمز التحقق عبر الهاتف أو البريد الإلكتروني، أو المصادقة البيومترية (مثل بصمات الأصابع أو التعرف على الوجه).

- **التحقق من الهوية من خلال وثائق رسمية:**

يتضمن هذا النوع من التحقق تقديم وثائق رسمية مثل جواز السفر أو رخصة القيادة، والتي تحتوي على معلومات شخصية وصورة للشخص، ويتم مقارنة هذه المعلومات مع قواعد البيانات .

- **التحقق من الهوية من خلال البيانات البيومترية:**

يعتمد هذا النوع على خصائص فريدة للشخص مثل بصمات الأصابع أو ملامح الوجه، ويتم مقارنتها مع البيانات المخزنة في قاعدة البيانات .

- **عملية التحقق:**

تتضمن عادةً مقارنة المعلومات المقدمة من قبل الشخص مع مصدر موثوق، مثل قاعدة بيانات حكومية أو سجل ائتماني .

- **أهمية التحقق من الهوية:**

يهدف التحقق من الهوية إلى حماية الأفراد والمنظمات من الاحتيال وسرقة الهوية، وضمان أن المعاملات تتم مع الأشخاص المصرح لهم.

أمثلة على تطبيقات التحقق من الهوية:

- **تسجيل الدخول إلى الخدمات عبر الإنترنت:**

يتم التحقق من هوية المستخدم قبل السماح له بالوصول إلى الخدمات عبر الإنترنت، مثل الخدمات المصرفية أو التسوق عبر الإنترنت .

- **التحقق من الهوية في المعاملات المالية:**

يتم التحقق من هوية العملاء قبل فتح حسابات مصرفية أو إجراء معاملات مالية كبيرة .

- **التحقق من الهوية في التطبيقات الحكومية:**

يتم التحقق من هوية المواطنين قبل الوصول إلى الخدمات الحكومية عبر الإنترنت، مثل تجديد الهوية أو استخراج جواز السفر .

كيف يعمل نظام IPS؟

يعمل نظام منع التطفل ((IPS عن طريق مراقبة حركة مرور الشبكة وتحليلها بحثًا عن الأنشطة الضارة وأنماط الهجوم المعروفة .يستخدم مُحرك IPS قاعدة بيانات للتوقيعات الداخلية لمطابقة حركة مرور الشبكة مع أنماط الهجوم المعروفة .إذا تم اكتشاف هجوم، يمكن لنظام IPS اتخاذ إجراءات لمنع الهجوم، مثل حظر عنوان IP أو منفذ المهاجم، أو إسقاط الحزم الضارة .

شرح تفصيلي:

- **المراقبة والتحليل:**

يقوم نظام IPS بمراقبة حركة مرور الشبكة الواردة والصادرة، وتحليلها بحثًا عن أي نشاط مشبوه .

- **مطابقة التوقيعات:**

يستخدم نظام IPS قاعدة بيانات داخلية تحتوي على توقيعات لأنماط الهجوم المعروفة .يقوم بتحليل حركة المرور ومقارنتها بهذه التوقيعات لتحديد ما إذا كان هناك هجوم محتمل .

- **اكتشاف الشذوذ:**

بالإضافة إلى مطابقة التوقيعات، يمكن لأنظمة IPS استخدام تقنيات الكشف عن الشذوذ لتحديد الأنشطة غير العادية التي قد تشير إلى هجوم .

- **الاستجابة للهجوم:**

إذا تم اكتشاف هجوم، يمكن لنظام IPS اتخاذ إجراءات لمنع الهجوم، مثل :

1. **حظر عنوان IP :**منع حركة المرور من عنوان IP للمهاجم .
2. **إسقاط الحزم الضارة :**منع الحزم التي تحتوي على محتوى ضار من الوصول إلى الشبكة .
3. **إعادة ضبط الاتصالات :**إيقاف الاتصالات المشبوهة .
4. **تنبيه فريق الأمن :**إرسال تنبيه إلى فريق الأمان لتنبيههم بوجود هجوم .

- **التكامل مع حلول الأمان الأخرى:**

غالبًا ما يتم دمج أنظمة IPS مع جدران الحماية وأنظمة كشف التطفل (IDS) لتوفير حماية أمنية شاملة .

أمثلة على تقنيات الكشف المستخدمة في :IPS

- **الكشف المستند إلى التوقيع:**

مطابقة حركة المرور مع توقيعات الهجمات المعروفة.

- **الكشف المستند إلى الشذوذ:**

تحديد الأنشطة غير العادية التي قد تشير إلى هجوم.

مزايا IPS:

نظام منع التطفل (IPS) يوفر العديد من المزايا، أهمها :حماية فورية ضد التهديدات من خلال منع الهجمات بمجرد اكتشافها، مما يقلل من فرص نجاح المخترقين .كما أنه يقلل من الضغط على فرق الأمن السيبراني لأنه يعمل تلقائيًا دون الحاجة لتدخل بشري مستمر .بالإضافة إلى ذلك، يحد من الخسائر المالية من خلال منع الاختراقات التي قد تؤدي إلى سرقة البيانات أو إيقاف الخدمات .

مزايا IPS بالتفصيل:

- **الحماية الفورية:**

يقوم IPS بفحص حركة المرور في الوقت الحقيقي والاستجابة التلقائية للتهديدات المكتشفة، مما يمنع الهجمات قبل أن تتسبب في ضرر .

- **الاستجابة التلقائية:**

يقوم IPS بتنفيذ إجراءات محددة مسبقًا مثل حظر حركة المرور الضارة أو إنهاء الاتصالات أو عزل الأنظمة المصابة .

- **تقليل العبء على فرق الأمن:**

يعمل IPS تلقائيًا، مما يقلل من الحاجة إلى تدخل بشري مستمر في مراقبة الشبكة والاستجابة للتهديدات .

- **تحسين الأداء:**

يمكن لـ IPS تحسين أداء الشبكة من خلال منع حركة المرور غير المرغوب فيها أو الضارة .

- **توفير طبقة أمان إضافية:**

يمكن دمج IPS مع جدران الحماية والأنظمة الأمنية الأخرى لزيادة الحماية .

- **التطور المستمر:**

تستخدم أنظمة IPS الذكاء الاصطناعي والتعلم الآلي لتحسين كفاءتها بمرور الوقت من خلال تحليل التهديدات الجديدة .

- **دقة أعلى في الكشف:**

بالمقارنة مع أنظمة كشف التسلل(IDS) ، يتميز IPS بقدرته على منع التهديدات وليس مجرد اكتشافها .

- **زوايا رؤية واسعة:**

توفر شاشات IPS زوايا رؤية واسعة تصل إلى 178 درجة، مما يضمن جودة صورة ثابتة من أي زاوية .

- **دقة ألوان وتناسق ممتاز:**

تتميز شاشات IPS بدقة ألوان عالية وتناسق ممتاز، مما يجعلها مثالية للتطبيقات التي تتطلب دقة في الألوان .

- **أوقات استجابة أسرع:**

تتميز شاشات IPS بأوقات استجابة أسرع مقارنة ببعض أنواع الشاشات الأخرى، مما يجعلها مناسبة للألعاب والتطبيقات التي تتطلب ردود فعل سريعة .

الاستجابة للحوادث السيبرانية

الوحدة العاشرة
الاستجابة للحوادث السيبرانية

ما هو نموذج خطة استجابة الحوادث السيبرانية ولماذا تحتاج المؤسسة إليه؟

خطة الاستجابة للحوادث السيبرانية هي وثيقة تحدد الخطوات التي يجب على المؤسسة اتخاذها عند وقوع حادث سيبراني تحتاج المؤسسات إلى هذه الخطة لتقليل الأضرار، وتسريع التعافي، والامتثال للمتطلبات التنظيمية.

أهمية خطة الاستجابة للحوادث السيبرانية:

- **تقليل الأضرار:**

تساعد الخطة في احتواء الحادث ومنع انتشاره، مما يقلل من الأضرار التي تلحق بالأنظمة والبيانات

- **تسريع التعافي:**

تحدد الخطة الخطوات اللازمة لاستعادة الأنظمة والبيانات المتضررة، مما يقلل من وقت التوقف عن العمل

- **الامتثال:**

تتطلب العديد من الصناعات وجود خطة استجابة للحوادث كجزء من متطلبات الامتثال التنظيمي

- **الحفاظ على السمعة:**

تساعد الخطة على حماية سمعة المؤسسة من خلال إظهار الاستعداد للتعامل مع الحوادث السيبرانية.

- **تخفيف الخسائر المالية:**

تساعد الخطة على تقليل الخسائر المالية الناتجة عن الحوادث السيبرانية، سواء كانت مباشرة (مثل تكاليف التحقيق) أو غير مباشرة (مثل فقدان ثقة العملاء)

مراحل خطة الاستجابة للحوادث:

عادةً ما تتضمن خطة الاستجابة للحوادث السيبرانية المراحل التالية:

1. **التحضير :**وضع السياسات، وتحديد الأدوار والمسؤوليات، وتجهيز الأدوات والموارد
2. **التعريف** :اكتشاف الحادث وتحديده
3. **الاحتواء** :منع انتشار الحادث
4. **الاستئصال :**إزالة التهديد وإصلاح الأنظمة المتضررة
5. **الاسترداد :**استعادة الأنظمة والبيانات إلى وضعها الطبيعي
6. **الدروس المستفادة :**مراجعة الحادث وتقييم الخطة لتحسينها في المستقبل

عناصر أمن المعلومات الأساسية CIA

ثلاثية وكالة المخابرات المركزية (CIA) في أمن المعلومات هي نموذج يركز على ثلاثة مبادئ أساسية :السرية(Confidentiality) ، والنزاهة(Integrity) ، والتوافر (Availability).هذه المبادئ الثلاثة هي الركائز الأساسية لحماية البيانات والمعلومات، وتعمل كإطار عمل لتطوير وتنفيذ استراتيجيات أمن المعلومات .

شرح عناصر ثلاثية وكالة المخابرات المركزية (CIA):

- **السرية:(Confidentiality)**

تعني حماية المعلومات من الوصول غير المصرح به .يتم تحقيق ذلك من خلال تطبيق تدابير أمنية مثل ضوابط الوصول، والتشفير، وإخفاء البيانات، لضمان وصول الأشخاص المصرح لهم فقط إلى المعلومات الحساسة .

- **النزاهة:(Integrity)**

تعني الحفاظ على دقة واكتمال البيانات، ومنع التعديل أو التغيير غير المصرح به .يتم تحقيق ذلك من خلال استخدام تقنيات مثل التحقق من صحة البيانات(checksums) ، والنسخ الاحتياطي، والتحقق من الأخطاء، لضمان موثوقية البيانات ودقتها .

- **التوافر:(Availability)**

تعني ضمان إمكانية الوصول إلى البيانات والمعلومات عند الحاجة إليها من قبل المستخدمين المصرح لهم .يتم تحقيق ذلك من خلال ضمان استمرارية عمل الأنظمة، وتوفير النسخ الاحتياطية، وتطبيق تدابير الحماية من هجمات الحرمان من الخدمة، لضمان إمكانية الوصول إلى البيانات في الوقت المناسب .

أهمية ثلاثية وكالة المخابرات المركزية (CIA)

إطار عمل شامل:

توفر ثلاثية وكالة المخابرات المركزية إطارًا شاملاً لتحديد وتقييم وتخفيف المخاطر الأمنية .

- **توجيه استراتيجيات الأمن:**

تساعد المؤسسات على تطوير وتنفيذ سياسات وإجراءات أمنية فعالة لمعالجة التهديدات المحتملة .

- **تحسين الأداء:**

من خلال حماية البيانات والأنظمة، تساهم ثلاثية وكالة المخابرات المركزية في تحسين أداء المؤسسات وتقليل المخاطر .

- **بناء الثقة:**

من خلال حماية البيانات والحفاظ على سلامتها وتوافرها، تساهم ثلاثية وكالة المخابرات المركزية في بناء ثقة العملاء والشركاء .

خطة الاستجابة لحوادث الأمن السيبراني

خطة الاستجابة لحوادث الأمن السيبراني هي مجموعة من الإجراءات الموثقة التي تهدف إلى اكتشاف الحوادث الأمنية، والاحتواء، والاستئصال، والتعافي منها .تهدف هذه الخطة إلى الحد من تأثير خروقات الأمن السيبراني وتسرب البيانات وهجمات البرامج الضارة وغيرها من التهديدات المحتملة مع ضمان استمرارية العمليات.

أهمية خطة الاستجابة لحوادث الأمن السيبراني:

- **الحد من الخسائر:**

تساعد الخطة في تقليل الأضرار المالية والسمعية الناتجة عن الحوادث السيبرانية .

- **تسريع الاستجابة:**

توفر إطارًا منظمًا للاستجابة السريعة والفعالة للحوادث، مما يقلل من وقت التعافي .

- **ضمان الامتثال:**

تساعد في تلبية المتطلبات التنظيمية المتعلقة بالأمن السيبراني .

- **تعزيز المرونة:**

تمكن المؤسسات من التعلم من الحوادث وتحسين الإجراءات الأمنية المستقبلية .

عناصر خطة الاستجابة للحوادث:

- **التحضير :**وضع الإجراءات الوقائية وتحديد الأدوار والمسؤوليات وتدريب الموظفين
- **التحديد :**اكتشاف الحوادث الأمنية والتحقيق فيها.
- **الاحتواء :**الحد من انتشار الحادث ومنع المزيد من الضرر.
- **الاستئصال :**إزالة التهديد من الأنظمة والشبكات.
- **التعافي :**استعادة الأنظمة والبيانات إلى وضعها الطبيعي.
- **الدروس المستفادة :**تحليل الحادث ووضع خطط لتحسين الإجراءات الأمنية .

أمثلة على الحوادث التي تتطلب خطة استجابة:

هجمات البرامج الضارة ,اختراقات البيانات ,هجمات رفض الخدمة (DoS), هجمات التصيد ,التهديدات الداخلية .

أفضل الممارسات في وضع خطة الاستجابة:

- **تحديد نطاق الخطة :**تحديد الأصول والأنظمة التي تغطيها الخطة.
- **تحديد الأدوار والمسؤوليات :**تحديد من المسؤول عن كل مرحلة من مراحل الاستجابة.
- **تحديد إجراءات الاستجابة :**وضع إجراءات مفصلة لكل نوع من أنواع الحوادث.
- **اختبار الخطة :**إجراء اختبارات دورية للخطة للتأكد من فعاليتها.
- **التواصل :**إنشاء قنوات اتصال واضحة بين فرق الاستجابة والأطراف المعنية.
- **التوثيق :**توثيق جميع جوانب الخطة والإجراءات .

فريق الاستجابة لحوادث الأمن السيبراني

فريق الاستجابة لحوادث الأمن السيبراني (Cybersecurity Incident Response Team - CSIRT) هو مجموعة متخصصة من الأفراد يهدفون إلى إدارة والاستجابة للحوادث الأمنية التي قد تواجهها المؤسسة .يشمل ذلك الكشف عن التهديدات، وعزلها، والتخلص منها، والتعافي من الحوادث، بالإضافة إلى توثيقها وتحليل الأدلة الجنائية .

مهام فريق الاستجابة للحوادث:

- **الكشف عن التهديدات:**

يتضمن ذلك مراقبة الشبكات والأنظمة للكشف عن أي نشاط مشبوه أو هجمات محتملة .

- **التحقيق في الحوادث:**

تقييم الحوادث لتحديد نطاقها وأثرها، وتحديد الأسباب الجذرية لوقوعها .

- **الاحتواء:**

اتخاذ إجراءات لمنع انتشار الهجوم ومنع المزيد من الضرر .

- **التخلص من التهديدات:**

إزالة التهديدات من الأنظمة والشبكات المتأثرة .

- **الاستعادة:**

إعادة الأنظمة المتضررة إلى حالتها الطبيعية والآمنة .

- **التوثيق:**

تسجيل جميع تفاصيل الحادث، بما في ذلك الإجراءات المتخذة والنتائج التي تم تحقيقها .

- **تحليل الأدلة الجنائية:**

جمع الأدلة الرقمية وتحليلها للتحقيق في الحادث وتقديمها للمحاسبة .

- **دعم الفرق الأخرى:**

تقديم الدعم الفني والتقني للفرق الأمنية الأخرى في المؤسسة .

- **رفع مستوى الوعي:**

توعية الموظفين حول التهديدات السيبرانية وكيفية الاستجابة للحوادث .

- **أهمية فريق الاستجابة للحوادث:**
- **تقليل الأضرار:**

يساعد في تقليل الأضرار الناجمة عن الحوادث السيبرانية.

- **تسريع الاستجابة:**

يضمن استجابة سريعة وفعالة للحوادث.

- **منع التكرار:**

يساعد في تحديد الأسباب الجذرية للحوادث ومنع تكرارها.

- **تحسين الأمن السيبراني:**

يساهم في تحسين مستوى الأمن السيبراني للمؤسسة بشكل عام .

أمثلة على فرق الاستجابة للحوادث:

- **فريق الاستجابة للحوادث السيبرانية الوطني:**

يتولى مسؤولية الاستجابة للحوادث الأمنية التي تؤثر على مستوى الدولة .

- **فرق الاستجابة للحوادث الخاصة بالمؤسسات:**

تتولى مسؤولية الاستجابة للحوادث الأمنية التي تؤثر على مؤسسات محددة .

- **فرق الاستجابة للحوادث المتخصصة:**

تتولى مسؤولية الاستجابة لأنواع معينة من الحوادث، مثل حوادث البرمجيات الخبيثة أو هجمات حجب الخدمة .

الخدمات المدارة

الوحدة الحادية عشر
الخدمات المدارة

الخدمات المدارة

الخدمات المدارة للأمن السيبراني هي خدمات أمنية تقدمها جهات خارجية لمساعدة المؤسسات على حماية أنظمتها وبياناتها من التهديدات السيبرانية تشمل هذه الخدمات مراقبة الشبكات والأنظمة، واكتشاف التهديدات والاستجابة لها، وإدارة الثغرات الأمنية، وتقديم الدعم الفني.

أمثلة على الخدمات المدارة للأمن السيبراني:

- **مراقبة الأمن على مدار الساعة:**

توفير فريق متخصص لمراقبة شبكات وأنظمة المؤسسة على مدار الساعة للكشف عن أي نشاط مشبوه أو تهديدات محتملة.

- **إدارة الثغرات الأمنية:**

تحديد الثغرات الأمنية في الأنظمة والتطبيقات، وتقييم المخاطر، وتنفيذ تصحيحات الأمان المناسبة.

- **الاستجابة للحوادث الأمنية:**

توفير فريق متخصص للتعامل مع حوادث الأمن السيبراني، والتحقيق فيها، واحتوائها، واستعادة العمليات.

- **إدارة الهوية والوصول:**

توفير خدمات لإدارة الهويات والصلاحيات، والتأكد من وصول المستخدمين المصرح لهم فقط إلى الموارد المناسبة .

- **اختبارات الاختراق:**

إجراء اختبارات لمحاكاة الهجمات السيبرانية لتقييم مدى قوة الأنظمة الأمنية .

- **التوعية الأمنية:**

تقديم برامج تدريبية للموظفين لزيادة الوعي بمخاطر الأمن السيبراني وتجنب الوقوع في الفخاخ.

- **خدمات استمرارية الأعمال:**

مساعدة المؤسسات على وضع خطط لاستمرارية الأعمال في حالة وقوع حادث أمني كبير .

فوائد الخدمات المدارة للأمن السيبراني:

- **توفير التكاليف:**

قد تكون الخدمات المدارة أكثر فعالية من حيث التكلفة من بناء فريق أمني داخلي.

- **الوصول إلى الخبرة:**

توفير الوصول إلى فريق من الخبراء في مجال الأمن السيبراني .

- **تحسين الأمان:**

تعزيز مستوى الأمان من خلال المراقبة المستمرة، واكتشاف التهديدات في الوقت المناسب، والاستجابة السريعة للحوادث.

- **التركيز على الأعمال الأساسية:**

يمكن للمؤسسات التركيز على أعمالها الأساسية مع ترك مهمة الأمن السيبراني لمتخصصين.

- **الامتثال للمتطلبات التنظيمية:**

مساعدة المؤسسات على الامتثال للمتطلبات التنظيمية المتعلقة بالأمن السيبراني .

ما هي الخدمات السحابية المدارة:

الخدمات السحابية المدارة هي خدمات تكنولوجيا معلومات تُقدمها جهة خارجية لإدارة موارد البنية التحتية السحابية للعميل، سواء كانت سحابة عامة، خاصة، أو مختلطة .تشمل هذه الخدمات مجموعة واسعة من المهام مثل الترحيل، والتكوين، والتحسين، والأمان، والصيانة، والنسخ الاحتياطي للبيانات .الهدف الرئيسي هو تمكين المؤسسات من الاستفادة القصوى من السحابة مع تقليل التكاليف والوقت والجهد الداخلي .

بمعنى أوسع، الخدمات السحابية المدارة هي:

- **إدارة كاملة أو جزئية لموارد العميل السحابية:**

يتولى مزود الخدمة السحابية المدارة مسؤولية إدارة وتشغيل البنية التحتية السحابية للعميل .

- **خدمات مُخصصة:**

يمكن أن تشمل هذه الخدمات مجموعة متنوعة من المهام، مثل التهيئة، والصيانة، والتحسين، والأمان، والترحيل، ودعم مكتب المساعدة على مدار الساعة طوال أيام الأسبوع، والنسخ الاحتياطي للبيانات، والمراقبة .

- **الاستعانة بمصادر خارجية:**

تتولى شركة خارجية إدارة البنية التحتية السحابية للعميل، مما يوفر على العميل عبء إدارة هذه الموارد بنفسه .

- **التركيز على الأعمال الأساسية:**

من خلال الاستعانة بخدمات سحابية مدارة، يمكن للمؤسسات التركيز على تطوير أعمالها الأساسية وابتكار منتجات وخدمات جديدة .

فوائد الخدمات السحابية المدارة:

- **توفير الوقت والتكاليف:**

تقلل من الوقت والجهد المطلوبين لإدارة البنية التحتية السحابية، مما يؤدي إلى توفير التكاليف.

- **تحسين الأداء:**

تضمن إدارة البنية التحتية بكفاءة عالية، مما يؤدي إلى تحسين أداء التطبيقات والخدمات.

- **زيادة الأمان:**

تقدم حلول أمان متقدمة لحماية البيانات والمعلومات الحساسة.

- **المرونة والقدرة على التوسع:**

توفر مرونة كبيرة وقابلية للتوسع لتلبية احتياجات العمل المتغيرة.

- **الوصول إلى الخبرة:**

يتيح للشركات الاستفادة من خبرة مزودي الخدمات السحابية المدارة في إدارة البنية التحتية السحابية.

- **دعم استباقي:**

توفر الدعم الفني اللازم لحل المشاكل والاستجابة للحوادث الأمنية .

أمثلة على الخدمات السحابية المدارة:

- **إدارة البنية التحتية السحابية:**

تتضمن إدارة الخوادم، والتخزين، والشبكات، وأنظمة التشغيل.

- **إدارة التطبيقات:**

تتضمن إدارة التطبيقات والخدمات التي تعمل على السحابة.

- **إدارة قواعد البيانات:**

تتضمن إدارة قواعد البيانات وتكوينها وصيانتها.

- **أمن السحابة:**

تتضمن حماية البنية التحتية السحابية من التهديدات الأمنية.

- **النسخ الاحتياطي والاسترداد:**

تتضمن النسخ الاحتياطي للبيانات واستعادتها في حالة فقدان البيانات .

ما الفوائد التي تقدمها الخدمات السحابية المدارة؟

خدمات الحوسبة السحابية المدارة هي خدمات يقدمها مزودو الخدمات السحابية (MSPs) للشركات، حيث يتولون إدارة وصيانة البنية التحتية السحابية للعميل بالكامل أو جزء منها .تهدف هذه الخدمات إلى تخفيف عبء إدارة البنية التحتية السحابية عن كاهل الشركات، مما يمكنهم من التركيز على أعمالهم الأساسية .

تشمل خدمات الحوسبة السحابية المدارة جوانب متعددة مثل :

- **إدارة البنية التحتية:**

تشمل إدارة الخوادم، والتخزين، والشبكات، وأنظمة التشغيل.

- **الأمن:**

تتضمن حماية البيانات والبنية التحتية من التهديدات السيبرانية.

- **المراقبة:**

تشمل مراقبة أداء البنية التحتية والتطبيقات، واكتشاف المشكلات وحلها.

- **النسخ الاحتياطي والاستعادة:**

تتضمن ضمان النسخ الاحتياطي للبيانات واستعادتها في حالة فقدان البيانات.

- **الدعم الفني:**

توفير الدعم الفني لحل المشكلات والاستفسارات.

- **التهيئة والصيانة:**

تتضمن إعداد وتكوين البنية التحتية وتحديثها بانتظام.

- **الترحيل:**

مساعدة الشركات في ترحيل تطبيقاتها وبياناتها إلى السحابة.

- **التحسين:**

تحسين أداء البنية التحتية وتكاليفها.

فوائد خدمات الحوسبة السحابية المدارة:

- **توفير التكاليف:**

يمكن أن توفر الخدمات السحابية المدارة تكاليف التشغيل والصيانة مقارنة بإدارة البنية التحتية في الموقع .

- **تحسين الكفاءة:**

يمكن للشركات تحسين كفاءة عملياتها من خلال الاستعانة بخبراء في إدارة السحابة .

- **التركيز على الأعمال الأساسية:**

يمكن للشركات التركيز على تطوير أعمالها الأساسية بدلاً من قضاء الوقت في إدارة البنية التحتية .

- **زيادة المرونة:**

توفر الخدمات السحابية المدارة مرونة أكبر للشركات لتلبية احتياجاتها المتغيرة .

- **تحسين الأمان:**

توفر الخدمات السحابية المدارة مستوى عالٍ من الأمان من خلال خبرة مزودي الخدمات السحابية .

أنواع خدمات الحوسبة السحابية المدارة:

- **خدمات سحابية عامة :**يديرها مزود خدمة سحابي عام.
- **خدمات سحابية خاصة :**يديرها مزود خدمة سحابي خاص.
- **خدمات سحابية هجينة :**مزيج من الخدمات السحابية العامة والخاصة .

أمثلة على مزودي خدمات الحوسبة السحابية المدارة:

Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM, Rackspace.

أمن البرمجيات

الوحدة الثانية عشر
أمن البرمجيات

ما هو أمن البرمجيات؟

أمن البرمجيات هو مجموعة الممارسات والتقنيات التي تهدف إلى حماية البرمجيات من التهديدات والهجمات المختلفة، وضمان سرية وسلامة وتوافر البيانات والمعلومات التي تتعامل معها البرمجيات و يشمل مجموعة واسعة من الإجراءات التي تُنفذ خلال دورة حياة تطوير البرمجيات، بدءًا من مرحلة التصميم وصولًا إلى مرحلة الصيانة .الهدف الرئيسي هو بناء حماية استباقية للبرمجيات بدلاً من مجرد الاستجابة للتهديدات .

تشمل بعض جوانب أمن البرمجيات:

- **نمذجة التهديدات:**

تحديد نقاط الضعف المحتملة في البرمجيات قبل البدء في عملية التطوير .

- **الترميز الآمن:**

كتابة التعليمات البرمجية بطريقة تمنع الثغرات الأمنية الشائعة، مثل الحقن .

- **اختبار الأمان:**

فحص البرمجيات بحثًا عن نقاط الضعف والثغرات الأمنية قبل طرحها في السوق .

- **إدارة الثغرات الأمنية:**

معالجة الثغرات الأمنية التي يتم اكتشافها في البرمجيات وتحديثها بانتظام .

- **المصادقة والتفويض:**

التحقق من هوية المستخدمين وتحديد الصلاحيات المتاحة لهم للوصول إلى موارد النظام

- **التشفير:**

تحويل البيانات إلى صيغة غير مقروءة إلا بواسطة الأشخاص المصرح لهم .

- **جدران الحماية:**

منع الوصول غير المصرح به إلى الأنظمة والشبكات .

- **أنظمة كشف التسلل:**

اكتشاف الأنشطة المشبوهة وتنبيه المسؤولين .

أهمية أمن البرمجيات:

- **حماية البيانات الحساسة:**

منع الوصول غير المصرح به إلى المعلومات الخاصة والبيانات المالية والمعلومات الشخصية.

- **ضمان استمرارية الأعمال:**

الحفاظ على عمل البرمجيات بشكل سليم ومنع تعطيل الخدمات.

- **الحماية من الهجمات الإلكترونية:**

التقليل من خطر التعرض للاختراقات والبرامج الضارة.

- **بناء الثقة:**

توفير بيئة آمنة للمستخدمين وتعزيز ثقتهم في البرمجيات والخدمات .

أحدث التهديدات الإلكترونية

تعتبر التهديدات الإلكترونية في تطور مستمر، وهناك العديد من التهديدات التي يجب على الأفراد والمؤسسات أن يكونوا على دراية بها .من بين أحدث التهديدات الإلكترونية :هجمات البرامج الضارة (مثل برامج الفدية)، وهجمات التصيد الاحتيالي، وهجمات الهندسة الاجتماعية، واستغلال نقاط الضعف في البرامج والأنظمة، والتهديدات الداخلية.

أحدث التهديدات الإلكترونية:

- **هجمات البرامج الضارة:**

تستمر هجمات البرامج الضارة في التطور، مع ظهور أنواع جديدة من برامج الفدية التي تشفر البيانات وتطلب فدية لإلغاء التشفير .بالإضافة إلى ذلك، هناك برامج ضارة تستهدف سرقة المعلومات الشخصية والمالية، أو تعطيل الأنظمة.

- **هجمات التصيد الاحتيالي:**

لا تزال هجمات التصيد الاحتيالي منتشرة وشائعة، حيث يحاول المحتالون خداع الأفراد للكشف عن معلومات حساسة مثل أسماء المستخدمين وكلمات المرور وتفاصيل الحسابات المصرفية .يعتمد التصيد الاحتيالي على الخداع والتلاعب النفسي لخلق شعور زائف بالإلحاح أو الثقة لإغراء الضحايا بالنقر على روابط ضارة أو تنزيل ملفات مصابة.

- **هجمات الهندسة الاجتماعية:**

تعتمد هجمات الهندسة الاجتماعية على التلاعب بالعلاقات الإنسانية لخداع الأفراد للكشف عن معلومات حساسة أو السماح بالوصول غير المصرح به إلى الأنظمة .غالبًا ما تستخدم هذه الهجمات أساليب مثل انتحال هوية شخصية موثوقة أو خلق شعور زائف بالثقة.

- **استغلال نقاط الضعف في البرامج والأنظمة:**

يبحث مجرمو الإنترنت باستمرار عن نقاط ضعف في البرامج والأنظمة لتنفيذ هجماتهم .قد تتضمن هذه الهجمات حقن التعليمات البرمجية، أو استغلال الثغرات الأمنية في بروتوكولات الشبكات، أو استخدام ثغرات في تطبيقات الويب.

- **التهديدات الداخلية:**

قد تحدث التهديدات الإلكترونية من داخل المنظمة نفسها، سواء عن قصد أو غير قصد .يمكن أن يشمل ذلك موظفين غير مدربين أو موظفين لديهم دوافع خبيثة .يجب على المؤسسات اتخاذ إجراءات لتقليل التهديدات الداخلية، مثل تطبيق سياسات أمنية صارمة وتدريب الموظفين على الوعي الأمني.

- **هجمات تعطيل الخدمة:(DDoS)**

تستهدف هجمات DDoS المواقع الإلكترونية والخوادم من خلال إغراقها بحركة مرور غير مرغوب فيها، مما يجعلها غير متاحة للمستخدمين الشرعيين.

- **هجمات انتحال الهوية:**

يحاول مجرمو الإنترنت في هجمات انتحال الهوية انتحال صفة جهة شرعية (مثل شركة أو فرد) لخداع الأفراد للكشف عن معلومات حساسة أو تنفيذ إجراءات معينة.

للتخفيف من هذه التهديدات:

- **التدريب والتوعية:**

يجب على الأفراد والمؤسسات تلقي تدريب مكثف حول الأمن السيبراني والوعي بالتهديدات الشائعة.

- **تحديث البرامج والأنظمة:**

يجب تحديث البرامج والأنظمة بانتظام لتصحيح الثغرات الأمنية.

- **استخدام كلمات مرور قوية:**

يجب استخدام كلمات مرور قوية وفريدة لكل حساب.

- **تفعيل المصادقة متعددة العوامل:**

تساعد المصادقة متعددة العوامل على حماية الحسابات من الاختراق.

- **تشفير البيانات:**

يجب تشفير البيانات الحساسة لحمايتها من الوصول غير المصرح به.

- **مراقبة حركة المرور:**

يجب مراقبة حركة المرور على الشبكة بحثًا عن أي نشاط مشبوه.

- **تطبيق سياسات أمنية قوية:**

يجب على المؤسسات تطبيق سياسات أمنية صارمة لحماية بياناتها وأنظمتها.

حماية المستخدم النهائي

حماية المستخدم النهائي هي مجموعة من الإجراءات والتقنيات التي تهدف إلى تأمين أجهزة المستخدمين وحماية بياناتهم من التهديدات المختلفة .تشمل هذه الحماية أمان نقاط النهاية، واتفاقيات ترخيص المستخدم النهائي (EULA)، وتدابير أمنية أخرى.

- **أمان نقاط النهاية:**

يهدف إلى حماية الأجهزة التي يستخدمها المستخدمون (مثل أجهزة الكمبيوتر المحمولة والهواتف الذكية) من البرامج الضارة والتهديدات الأخرى .يشمل ذلك استخدام برامج مكافحة الفيروسات، وجدران الحماية، وأنظمة الكشف عن التسلل .

- **اتفاقيات ترخيص المستخدم النهائي:(EULA)**

هي عقود قانونية تحدد حقوق المستخدمين ومسؤولياتهم عند استخدام البرامج أو التطبيقات .تهدف إلى حماية حقوق الملكية الفكرية لمطوري البرامج وتحديد استخدام البرنامج بشكل واضح .

- **تدابير أمنية أخرى:**

تشمل تدابير مثل المصادقة القوية، وإدارة كلمات المرور، والتشفير لحماية البيانات الحساسة .كما تشمل توعية المستخدمين حول المخاطر الأمنية المختلفة وكيفية تجنبها .

أهمية حماية المستخدم النهائي:

- **حماية البيانات:**

حماية البيانات الشخصية والمالية والمعلومات الحساسة من السرقة أو الوصول غير المصرح به .

- **الحفاظ على السمعة:**

منع حدوث اختراقات أمنية قد تؤثر سلبًا على سمعة المؤسسة .

- **الامتثال للقوانين:**

العديد من القوانين واللوائح تتطلب حماية بيانات المستخدمين، مثل قانون حماية البيانات .

- **ضمان الاستمرارية:**

تساعد حماية المستخدمين على ضمان استمرارية العمليات التجارية وعدم تعطيلها بسبب هجمات إلكترونية .

أمثلة على حماية المستخدم النهائي:

- **تحديثات البرامج:**

تأمين الأجهزة بتحديثات البرامج بانتظام لإصلاح الثغرات الأمنية .

- **شبكات آمنة:**

استخدام شبكات Wi-Fi آمنة والابتعاد عن الشبكات غير الموثوقة .

- **الحذر من رسائل البريد الإلكتروني:**

تجنب النقر على الروابط أو فتح المرفقات من مصادر غير موثوقة .

- **استخدام كلمات مرور قوية:**

إنشاء كلمات مرور قوية وتجنب استخدام كلمات مرور سهلة التخمين .

طريقة الحماية من البرمجيات الخبيثة

لحماية نفسك من البرمجيات الخبيثة، يمكنك اتباع عدة طرق، منها استخدام برامج مكافحة الفيروسات، وتجنب المواقع والتطبيقات غير الموثوقة، وتحديث نظام التشغيل والتطبيقات بانتظام .

تفصيل طرق الحماية:

1. **استخدام برامج مكافحة الفيروسات:**

- تثبيت برنامج مكافحة فيروسات موثوق به وتحديثه باستمرار، وفقًا لموقع كاسبرسكي، يعتبر هذا الإجراء خطوة أساسية لحماية جهازك من مختلف أنواع البرامج الضارة
- فحص جهاز الكمبيوتر بانتظام باستخدام برنامج مكافحة الفيروسات للكشف المبكر عن البرامج الضارة .
- فحص محركات الأقراص الخارجية والوسائط القابلة للإزالة قبل استخدامها للتأكد من خلوها من البرامج الضارة .

2. **الحذر من المواقع والتطبيقات غير الموثوقة:**

- تجنب تنزيل أي محتوى من مصادر غير موثوق بها، خاصةً البرامج والألعاب المجانية التي قد تحتوي على برامج ضارة .
- تجنب زيارة المواقع المشبوهة أو التي تطلب معلومات شخصية أو مالية دون داعٍ .

3. **تحديث نظام التشغيل والتطبيقات:**

- حافظ على تحديث نظام التشغيل الخاص بك) مثل Windows أو macOS) والتطبيقات التي تستخدمها بشكل منتظم، حيث تتضمن التحديثات غالبًا إصلاحات أمنية لسد الثغرات التي يمكن أن تستغلها البرامج الضارة .

4. **تفعيل جدار الحماية:**

- استخدم جدار الحماية (Firewall)المدمج في نظام التشغيل أو قم بتثبيت جدار حماية خارجي، فهو يساعد في حظر حركة المرور غير المصرح بها وحماية جهازك من الهجمات .

5. **الحذر من رسائل البريد الإلكتروني والروابط المشبوهة:**

- لا تفتح مرفقات البريد الإلكتروني من مرسلين غير معروفين أو روابط مشبوهة في رسائل البريد الإلكتروني، فقد تحتوي على برامج ضارة .
- إذا كنت غير متأكد من مصدر رسالة بريد إلكتروني، فمن الأفضل حذفها بدلاً من فتحها .

6. **استخدام كلمات مرور قوية:**

- استخدم كلمات مرور قوية ومعقدة لكل حساباتك، وتجنب استخدام نفس كلمة المرور لعدة حسابات، حيث يساعد ذلك في حماية حساباتك من الاختراق .

7. لنسخ الاحتياطي للملفات الهامة:

- قم بعمل نسخ احتياطية بانتظام للملفات الهامة الموجودة على جهازك في مكان آمن، مثل قرص صلب خارجي أو خدمة تخزين سحابي، وذلك في حال تعرض جهازك للإصابة بالبرامج الضارة، يمكنك استعادة ملفاتك من النسخة الاحتياطية .

8. التحلي بالوعي الأمني:

- كن على دراية بالتهديدات الأمنية الشائعة وكيفية التعرف عليها، وفقًا لموقع " :EFFفالوعي الأمني هو الخطوة الأولى في الحماية من البرامج الضارة ."

إدارة الإعدادات

الوحدة الثالثة عشر
إدارة الإعدادات

مهارات إدارة التكنولوجيا والابتكار

تعتبر مهارات إدارة التكنولوجيا والابتكار من المهارات الأساسية في العصر الحديث، حيث تشمل القدرة على فهم التكنولوجيا واستخدامها لتحقيق أهداف العمل، بالإضافة إلى تطوير أساليب جديدة ومبتكرة لحل المشاكل وتحسين العمليات .تتضمن هذه المهارات مجموعة واسعة من القدرات، بدءًا من التفكير الإبداعي والتحليلي، وصولًا إلى المهارات التقنية والإدارية.

أهمية مهارات إدارة التكنولوجيا والابتكار:

- **تعزيز القدرة التنافسية:**

تساهم في تطوير منتجات وخدمات جديدة ومبتكرة، مما يعزز مكانة المؤسسة في السوق.

- **تحسين الكفاءة والإنتاجية:**

تمكن من تبني تقنيات حديثة لتحسين العمليات وتقليل التكاليف.

- **مواكبة التطورات السريعة:**

تساعد على التكيف مع التغيرات التكنولوجية المتسارعة وتوظيفها لصالح المؤسسة.

- **تطوير حلول مبتكرة:**

تمكن من إيجاد حلول إبداعية للتحديات التي تواجه المؤسسة والمجتمع.

- **جذب واستقطاب الكفاءات:**

توفر بيئة عمل محفزة وجذابة للموظفين الموهوبين.

مهارات إدارة التكنولوجيا:

- **فهم التكنولوجيا:**

القدرة على فهم التقنيات المختلفة وتطبيقاتها في سياق العمل.

- **إدارة المشاريع التكنولوجية:**

القدرة على تخطيط وتنفيذ وإدارة المشاريع التكنولوجية بنجاح.

- **تحليل البيانات:**

القدرة على تحليل البيانات واستخراج الأنماط والاتجاهات لاتخاذ قرارات أفضل.

- **إدارة المخاطر:**

القدرة على تحديد وتقييم وإدارة المخاطر المرتبطة بالتكنولوجيا.

- **الأمن السيبراني:**

فهم أهمية الأمن السيبراني وحماية البيانات من التهديدات الإلكترونية.

- **إدارة السحابة:**

القدرة على استخدام وإدارة خدمات الحوسبة السحابية .

مهارات الابتكار:

- **التفكير الإبداعي:**

القدرة على توليد أفكار جديدة ومبتكرة.

- **حل المشكلات:**

القدرة على تحديد المشكلات وإيجاد حلول فعالة لها.

- **التفكير النقدي:**

القدرة على تحليل وتقييم المعلومات والأفكار.

- **التواصل والتعاون:**

القدرة على التواصل الفعال مع الآخرين والعمل ضمن فريق.

- **المرونة والتكيف:**

القدرة على التكيف مع التغيير والتعامل مع المواقف غير المتوقعة.

- **إدارة التغيير:**

القدرة على قيادة وتوجيه التغييرات التنظيمية.

- **التفكير الاستراتيجي:**

القدرة على التخطيط للمستقبل وتحديد الأهداف.

كيفية تطوير مهارات إدارة التكنولوجيا والابتكار:

- **التدريب والتعليم:**

حضور الدورات التدريبية وورش العمل التي تركز على إدارة التكنولوجيا والابتكار .

- **التعلم المستمر:**

مواكبة التطورات التكنولوجية من خلال القراءة والبحث والمشاركة في المؤتمرات والفعاليات ذات الصلة .

- **الممارسة العملية:**

تطبيق المهارات المكتسبة في المشاريع العملية والمواقف الحقيقية.

- **التعاون مع الآخرين:**

التعاون مع الزملاء والخبراء في مجال التكنولوجيا والابتكار .

- **بناء ثقافة الابتكار:**

المساهمة في بناء بيئة عمل تشجع على التجربة والابتكار .

ما الفرق بين التنسيق والأتمتة؟

التنسيق والأتمتة مصطلحان مرتبطان ولكنهما ليسا متماثلين .الأتمتة هي عملية جعل مهمة أو سلسلة من المهام تتكرر ذاتيًا باستخدام التكنولوجيا، غالبًا دون تدخل بشري التنسيق هو عملية إدارة وتنظيم مهام متعددة، سواء كانت مؤتمتة أم لا، لتنفيذ عملية أو سير عمل كامل.

- **الأتمتة :**تهدف إلى تبسيط المهام الفردية المتكررة.
- **التنسيق :**يهدف إلى إدارة وربط العديد من المهام، بما في ذلك المهام المؤتمتة، لتنفيذ عملية أكبر وأكثر تعقيدًا .

التوضيح:

- **الأتمتة :**هي جزء من عملية التنسيق .
- يمكن أن تتضمن الأتمتة مهمة واحدة، بينما يتضمن التنسيق عادةً عدة مهام، وقد تتضمن أنظمة متعددة.
- التنسيق يركز على سير العمل الشامل، بينما الأتمتة تركز على المهام الفردية .

مثال:

تخيل بناء منزل .الأتمتة قد تكون استخدام آلة لخلط الخرسانة أو استخدام آلة لقطع الخشب .التنسيق سيكون عملية إدارة وتجميع جميع هذه المهام المختلفة، بالإضافة إلى المهام الأخرى مثل البناء والتشطيب، لإنشاء المنزل بالكامل .

في سياق تكنولوجيا المعلومات:

- **الأتمتة :**يمكن أن تكون أتمتة مهمة مثل نشر الخوادم.
- **التنسيق** :يمكن أن يكون أتمتة سير العمل بأكمله، بدءًا من نشر الخوادم، ثم تثبيت البرامج، ثم التهيئة، ثم الاختبار، ثم النشر.

التحديثات والإصلاحات البرمجية

الوحدة الرابعة عشر
التحديثات والإصلاحات البرمجية

ما هو تحديث البرامج

تحديث البرامج هو عملية استبدال إصدار قديم من برنامج ما بإصدار أحدث .يشمل ذلك تحسينات في الأداء، وإصلاح للأخطاء، وتعزيز للأمان، وإضافة ميزات جديدة .

أهمية تحديث البرامج:

- **تحسين الأداء:**

قد يؤدي تحديث البرنامج إلى تحسين سرعة استجابته وكفاءته.

- **إصلاح الأخطاء:**

يساعد التحديث في معالجة المشكلات البرمجية التي قد تؤثر على أداء الجهاز أو استقراره.

- **تعزيز الأمان:**

يسد التحديث الثغرات الأمنية التي قد تسمح للمتسللين بالوصول إلى بياناتك أو جهازك.

- **إضافة ميزات جديدة:**

غالبًا ما تتضمن التحديثات ميزات جديدة أو محسنة تزيد من فائدة البرنامج وتجربة المستخدم .

أنواع تحديثات البرامج:

- **تحديثات نظام التشغيل:**

تشمل تحديثات نظام التشغيل الخاص بجهازك (مثل نظام التشغيل ويندوز أو أند رويد).

- **تحديثات التطبيقات:**

تشمل تحديثات التطبيقات التي تستخدمها على جهازك (مثل تطبيقات التواصل الاجتماعي أو الألعاب).

- **تحديثات البرامج الثابتة (البرامج المضمنة):**

تشمل تحديثات البرامج التي تعمل على الأجهزة المادية (مثل تحديثات الكاميرا أو الطابعة) .

كيفية تحديث البرامج:

- **تحديثات تلقائية:**

غالبًا ما توفر الأجهزة والتطبيقات خيار التحديث التلقائي، حيث يتم تنزيل وتثبيت التحديثات الجديدة تلقائيًا.

- **تحديثات يدوية:**

يمكنك أيضًا تحديث البرامج يدويًا عن طريق البحث عن التحديثات المتاحة والتحقق منها .

نصائح لتحديث البرامج:

- **تأكد من أن جهازك متصل بشبكة إنترنت موثوقة:**

قبل البدء في تحديث البرامج، تأكد من أن لديك اتصال إنترنت مستقر لتجنب انقطاع التحديث.

- **قم بعمل نسخة احتياطية لبياناتك:**

قبل تحديث نظام التشغيل أو التطبيقات، قم بعمل نسخة احتياطية لبياناتك المهمة لتجنب فقدانها.

- **اتبع التعليمات المرفقة مع التحديث:**

تأكد من قراءة واتباع التعليمات المرفقة مع التحديث لضمان تثبيته بشكل صحيح .

ما المقصود من تحديثات نظام التشغيل ويندوز

تحديثات نظام التشغيل ويندوز (Windows Updates) هي عمليات تقوم بها شركة Microsoftلإصلاح الأخطاء الأمنية، وتحسين أداء النظام، وإضافة ميزات جديدة إلى نظام التشغيل .Windows هذه التحديثات ضرورية للحفاظ على أمان جهاز الكمبيوتر الخاص بك وتأمين معلوماتك الشخصية .

- **تحديثات الأمان:**

هذه التحديثات تعالج الثغرات الأمنية التي قد تسمح للمتسللين بالوصول إلى جهازك أو معلوماتك الشخصية .

- **تحسينات الأداء:**

تساعد هذه التحديثات على تحسين سرعة واستقرار نظام التشغيل، مما يجعل جهازك يعمل بشكل أسرع وأكثر سلاسة .

- **إصلاحات الأخطاء:**

تعمل هذه التحديثات على إصلاح الأخطاء والمشاكل التي قد تواجهها في نظام التشغيل .

- **ميزات جديدة:**

في بعض الأحيان، تتضمن التحديثات ميزات جديدة لتحسين تجربة المستخدم وإضافة وظائف جديدة إلى نظام التشغيل .

للحفاظ على جهازك آمنًا ومحدثًا، من الضروري تمكين تحديثات Windows التلقائية أو التحقق من وجود تحديثات بشكل دوري .يمكنك القيام بذلك عن طريق الانتقال إلى "الإعدادات" ثم "Windows Update" واختيار "التحقق من وجود تحديثات ."

صيانة البرمجيات

تُعرف صيانة البرمجيات بالإنجليزية (software maintenance) :بأنّها العمليّة التي يتم بها تحديث البرامج، وإدراج مهام جديدة، وتصحيح الأخطاء البرمجيّة، وحل مشاكل البرمجة على شكل عقود صيانة تبرمها شركات البرمجة مع عملائها، وتُحسب كرسوم سنويّة على أساس نسبة مئوية من إجمالي تكلُفة البرنامج، أنواع صيانة البرمجيات توجد ثلاثة أنواع لصيانة البرمجيات:

وهي كالآتي:

- **الصيانة التكيّفية:** وتأتي نتيجة تغيُّرات داخليّة لنُظم المؤسّسة البرمجيّة، كنقل البرامج إلى أجهزة جديدة، أو إلى مترجمات ونظم تشغيل أخرى، وذلك لكي تتكيّف مع المُتطلّبات الخارجية، وتُجاري الحداثة، في تلبية احتياجات المُستخدم وقطاعات الأعمال.

الصيانة التصحيحيّة: تُعتبر عمليّة تعديل، وتحسين مشاكل الخلل في الأنظمة والبرامج جوهر عمل الصيانة التصحيحيّة، بحيث يتم تعديل التعليمات البرمجيّة، وهياكل البرامج، وتنبيهات البرامج، وإمّا أن تأتي الحاجة لها من المُستخدم أو من تقارير الخطأ التي تظهر في البرامج، فيكون الإصلاح إما لحالات الفشل الطارئة، أو عمليّة مُجدولة للتعديل، والتصحيح. الصيانة الوقائيّة: وتتم فيها إعادة هيكلة البرامج، لذا تُسمّى إعادة هندسة البرمجيات، بهدف الوقاية من المشاكل البرمجيّة مُستقبلاً، بحيث تصبح البرامج أكثر فهماً، وتتحسّن مزاياها، وبالتالي تسهُل صيانتها. الصيانة المثالية: وهي بمثابة تعديلات إضافيّة على البرامج لتظل قابلةً للاستخدام لأطول مُدّة مُمكنة، ممّا يُخفّض تكاليف استخدامها، وصيانتها، وتزيد من سرعتها، وموثوقيّتها، وتزوّدها بمزايا جديدة.

أسباب صيانة البرمجيات تظهر الحاجة لصيانة البرمجيّات نظراً للظروف والعوامل الآتية: تغيّرات السوق، والسياسات المُتّبعة، إذ يتم إدراج قوانين جديدة على المؤسّسات، مثل تغيير أنظمة الضرائب، والعمليّات المُحاسبيّة، الأمر الذي يستوجب تعديل البرامج. متطلبات العميل، حيث يطلُب العميل دائماً تعديل الإعدادات الخاصّة بعمله، وإضافة ميّزات جديدة لبرامجه. تغيرات البرامج أو الأجهزة المُضيفة، ففي حال تم تغيير أيّ من الأجهزة، أو أنظمة التشغيل، من الطبيعي تغيير بُنية البرامج لتتكيّف معها. تعديلات مُستويات العمل التنظيمي، حيث يتطلّب الأمر أحياناً من المُنظّمات إجراء تغييرات تنظيميّة، ممّا يستدعي تعديل برامجها . خطوات صيانة البرمجيات تتضمّن عمليّة صيانة البرمجيات الخطوات الآتية: تحديد مُتطلبات التغيير في البرامج، من خلال تسجيل المُلاحظات، أو الرسائل الخاطئة التي تصدُر منها. تحليل قابليّة البرمجيّات للتعديل، ويشمل ذلك أمن النظام وسلامته، وفي حال كان التعديل مُكلفاً، يتم البحث عن بديل آخر. تصميم الإجراءات الجديدة التي تحتاج للتعديل، وذلك باختبارها، والتأكُّد من فعاليّتها. تنفيذ الكود الجديد للوحدات التي تم تصميمها في المرحله السابقة، بحيث يُطلب من كل مبرمج اختبار الوحدة المُبرمجة، وبشكل متوازٍ مع الوحدات الأخرى. اختبار تكاملي للوحدات الجديدة مع النظام ككل. تسليم ونشر النظام في جميع أنحاء المؤسسة، ويتم إجراء الاختبار النهائي في الشركة بعد تسليم البرنامج، وإذا لزم الأمر يتم تدريب المستخدمين عليه.

خطوات عملية صيانة البرمجيات

تتضمن عملية صيانة البرمجيات عدة خطوات أساسية لضمان استمرارية عمل البرنامج بكفاءة وفعالية، وتشمل هذه الخطوات :تحديد متطلبات التغيير، تحليل قابلية البرمجية للتعديل، تصميم الإجراءات الجديدة، تنفيذ الكود الجديد، الاختبار، والتسليم والنشر .

خطوات عملية صيانة البرمجيات بالتفصيل:

1. **تحديد متطلبات التغيير:**
   - يتم في هذه المرحلة جمع الملاحظات والشكاوى من المستخدمين حول المشاكل أو الأخطاء التي يواجهونها في البرنامج.
   - يتم تحليل هذه الملاحظات لتحديد نطاق التغييرات المطلوبة.
2. **تحليل قابلية البرمجية للتعديل:**
   - يتم في هذه المرحلة تقييم مدى سهولة أو صعوبة إجراء التغييرات المطلوبة على البرنامج.
   - يتم النظر في جوانب مثل أمن النظام وسلامته، وهل التعديل المقترح سيؤثر على الأداء العام للبرنامج.
   - في حال كانت التعديلات المقترحة معقدة أو مكلفة، قد يتم البحث عن بدائل أخرى.
3. **تصميم الإجراءات الجديدة:**
   - يتم في هذه المرحلة تصميم الإجراءات والوحدات البرمجية الجديدة التي ستقوم بتنفيذ التغييرات المطلوبة.
   - يتم اختبار هذه الإجراءات والوحدات للتأكد من أنها تعمل بشكل صحيح وفعال.
4. **تنفيذ الكود الجديد:**
   - يتم في هذه المرحلة تنفيذ الكود الجديد للوحدات التي تم تصميمها في المرحلة السابقة.
   - يتم اختبار كل وحدة برمجية بشكل فردي للتأكد من أنها تعمل بشكل صحيح قبل دمجها مع النظام ككل.
5. **الاختبار:**
   - يتم إجراء اختبار تكاملي للوحدات الجديدة مع النظام ككل للتأكد من عدم وجود أي مشاكل أو تعارضات.
   - يتم إجراء اختبارات إضافية للتأكد من أن البرنامج يعمل بكفاءة وفعالية بعد التعديل.
6. **التسليم والنشر:**
   - يتم تسليم البرنامج المحدث للمستخدمين ونشره على نطاق المؤسسة.
   - يتم إجراء اختبار نهائي بعد التسليم لضمان عمل البرنامج بشكل صحيح في بيئة الإنتاج.
   - قد يتم توفير التدريب للمستخدمين على البرنامج المحدث .

أنواع صيانة البرمجيات:

بالإضافة إلى الخطوات المذكورة أعلاه، هناك أنواع مختلفة من صيانة البرمجيات، تشمل :

- **الصيانة التصحيحية:**

إصلاح الأخطاء والمشاكل التي تظهر في البرنامج.

- **الصيانة التكيفية:**

تعديل البرنامج ليتوافق مع التغييرات في البيئة التي يعمل فيها (مثل نظام التشغيل أو الأجهزة).

- **الصيانة التحسينية:**

إضافة ميزات جديدة أو تحسين الميزات الموجودة في البرنامج لتحسين أدائه أو تجربة المستخدم.

- **الصيانة الوقائية:**

تحديد المشاكل المحتملة وإصلاحها قبل أن تتسبب في مشاكل أكبر.

فحص الثغرات الأمنية

الوحدة الخامسة عشر
فحص الثغرات الأمنية

ما هي أداة فحص الثغرات الأمنية

أداة فحص الثغرات الأمنية هي برنامج مصمم للكشف عن نقاط الضعف في الأنظمة والتطبيقات والشبكات .تعمل هذه الأدوات على فحص الأجهزة والبرامج بحثًا عن نقاط ضعف معروفة، مثل أخطاء البرمجة، وسوء التكوين، وإصدارات البرامج القديمة، وضعف كلمات المرور .تهدف هذه العملية إلى تحديد المشاكل الأمنية المحتملة قبل أن يتم استغلالها من قبل المهاجمين.

أمثلة على أدوات فحص الثغرات الأمنية:

- **Nessus**

أداة مشهورة لفحص الثغرات الأمنية، توفر فحصًا شاملاً للشبكات والأجهزة .

- **OpenVAS**

بديل مفتوح المصدر لأداةNessus ، يقدم ميزات مماثلة .

- **Qualys**

أداة تجارية لفحص الثغرات الأمنية، تستخدمها العديد من الشركات الكبيرة .

- **AWS Inspector**

أداة فحص أمني من أمازون ويب سيرفيسز، مصممة خصيصًا لبيئات السحابة .

- **GitHub Dependabot**

أداة لفحص تبعيات البرامج في مستودعات جيثب، وتحديد الثغرات في المكتبات المستخدمة .

- **Nmap**

أداة لفحص المنافذ واكتشاف الخدمات المفتوحة على الشبكة .

كيف تعمل أدوات فحص الثغرات الأمنية؟

تعمل أدوات فحص الثغرات الأمنية عن طريق :

1. **اكتشاف المضيفين :**تحديد الأجهزة المتصلة بالشبكة والنشطة.
2. **فحص المنافذ :**تحديد المنافذ المفتوحة على الأجهزة.
3. **تحليل البرامج :**تحديد إصدارات البرامج والتطبيقات المثبتة على الأجهزة.
4. **مطابقة قاعدة البيانات :**مقارنة المعلومات التي تم جمعها بقواعد بيانات الثغرات الأمنية المعروفة (مثل .(CVE
5. **إنشاء تقارير :**إصدار تقارير عن الثغرات الأمنية المكتشفة، مرتبة حسب مستوى الخطورة.

أهمية فحص الثغرات الأمنية:

- **تحديد نقاط الضعف:**

تساعد على اكتشاف الثغرات الأمنية قبل أن يتم استغلالها .

- **تحسين الأمان:**

تمكن المؤسسات من معالجة الثغرات الأمنية واتخاذ الإجراءات اللازمة لتحسين وضعهم الأمني .

- **الامتثال:**

تساعد على تلبية متطلبات الامتثال التنظيمي .

- **توفير الوقت والجهد:**

تؤتمت عملية تحديد الثغرات الأمنية وتحديد أولوياتها .

- **التقليل من المخاطر:**

تقلل من خطر الهجمات الإلكترونية والاختراقات .

بعض بدائل أداة فحص الثغرات الأمنية

- **ماسح المنافذ**

يُستخدم ماسح المنافذ لتحديد المنافذ المفتوحة على النظام. يساعد هذا على تحديد التطبيق ونظام التشغيل المُستخدمين على الشبكة، مما يُسهّل اكتشاف الثغرات الأمنية المُحتملة التي قد يستغلها المُهاجمون.

- **ماسح الثغرات الأمنية**

يقوم ماسح الثغرات بتقييم جهاز الكمبيوتر والتطبيقات والخوادم لتحديد الثغرات الأمنية والثغرات التي يمكن استغلالها. ويتم ذلك عادةً بتحديد إصدار البرنامج قيد التشغيل ومقارنته بقائمة إصدارات البرامج التي تحتوي على ثغرات معروفة.

- **متتبع الشبكة**

تتيح لك أداة اختبار الاختراق هذه مراقبة حركة البيانات عبر الشبكة، بما في ذلك مصدرها ووجهتها والجهاز المتصل بها والبروتوكولات والمنافذ المستخدمة. يساعد هذا في التحقق من تشفير البيانات وتحديد مسارات الاتصال التي يمكن استغلالها أثناء اختبار الاختراق.

- **وكيل الويب**

يستطيع مُختبرو الاختراق اعتراض وتعديل حركة البيانات بين خوادم الويب ومتصفحات مؤسستهم باستخدام وكيل ويب. يُساعد هذا في الكشف عن حقول النماذج المخفية وعناصر HTML الأخرى التي قد تكشف عن ثغرات أمنية مثل XSS و CSRF.

- **استعادة كلمة المرور المتقدمة**

يميل المخترقون عادةً إلى كشف كلمات المرور الضعيفة والشائعة. تتيح لك أدوات فحص كلمات المرور تقييم تجزئة كلمات المرور لتحديد ما إذا كانت كلمة المرور قابلة للاختراق بسهولة أم لا.

كيفية عمل إدارة الثغرات الأمنية

إدارة الثغرات الأمنية هي عملية منهجية لتحديد نقاط الضعف في الأنظمة والتطبيقات، وتقييم المخاطر المرتبطة بها، واتخاذ الإجراءات اللازمة لتخفيف تلك المخاطر أو إزالتها .تتضمن العملية اكتشاف الثغرات الأمنية، وتقييمها، وتحديد أولوياتها، ومعالجتها، والمراقبة المستمرة، والتحسين المستمر.

خطوات إدارة الثغرات الأمنية:

1. **اكتشاف الثغرات الأمنية:**
   - **المسح الضوئي للثغرات :**استخدام أدوات آلية لفحص الأنظمة والتطبيقات عن نقاط الضعف.
   - **التقييم اليدوي :**إجراء تقييم يدوي للثغرات الأمنية المحتملة من قبل خبراء الأمن.
   - **جرد الأصول :**تحديد جميع الأصول (الأنظمة، التطبيقات، البيانات) التي تحتاج إلى حماية .
2. **تقييم المخاطر:**
   - **تحليل تأثير التهديدات :**تحديد حجم الضرر المحتمل الناجم عن استغلال الثغرات الأمنية، مع الأخذ في الاعتبار التأثير المالي والتشغيلي والسمعة .
   - **تحديد الأولويات** :تصنيف الثغرات الأمنية بناءً على مدى خطورتها وتأثيرها المحتمل، وتحديد أولويات المعالجة بناءً على ذلك
3. **المعالجة:**
   - **تطبيق التصحيحات :**تطبيق التحديثات الأمنية التي توفرها الشركات المصنعة لإصلاح الثغرات الأمنية
   - **إعادة التهيئة :**إعادة تكوين الأنظمة والتطبيقات لتجنب استغلال الثغرات الأمنية .
   - **الضوابط الأمنية :**تطبيق ضوابط أمنية إضافية لتخفيف المخاطر المرتبطة بالثغرات الأمنية .
4. **لمراقبة المستمرة:**
   - **مراقبة الأحداث الأمنية :**استخدام أنظمة SIEM لمراقبة الأحداث الأمنية واكتشاف أي نشاط مشبوه.
   - **التحقق من صحة المعالجة :**التأكد من أن الإجراءات المتخذة قد أزالت أو خففت المخاطر بشكل فعال .
5. **التحسين المستمر:**
   - **المراجعة الدورية :**مراجعة وتحديث عمليات إدارة الثغرات الأمنية بانتظام لتحسينها وتكييفها مع التهديدات المتغيرة .
   - **التعلم من الحوادث :**تحليل الحوادث الأمنية لفهم أسبابها واتخاذ الإجراءات اللازمة لمنع تكرارها .

الأدوات المستخدمة في إدارة الثغرات الأمنية:

- **ماسحات الثغرات الأمنية :**للكشف عن الثغرات الأمنية.
- **أنظمة** :SIEM لمراقبة الأحداث الأمنية وتحليلها
- **أدوات إدارة التكوين :**لإدارة إعدادات الأمان وتكوين الأنظمة.
- **أدوات إدارة التصحيح :**لتطبيق التحديثات الأمنية.

- **أدوات اختبار الاختراق :**لاختبار فعالية الإجراءات الأمنية .

أهمية إدارة الثغرات الأمنية:

- **تقليل المخاطر:**
  تمنع استغلال الثغرات الأمنية وتخفف من تأثيرها.
- **الامتثال:**
  تساعد في الامتثال للمتطلبات التنظيمية المتعلقة بالأمن السيبراني.
- **تعزيز الأمن:**
  تحسن بشكل عام الوضع الأمني للمؤسسة.
- **توفير التكاليف:**
  تمنع الخسائر المالية والسمعة الناتجة عن الهجمات الأمنية .

الأشخاص ودورهم الأمني

الوحدة الخامسة عشر

الأشخاص ودورهم الأمني

كيف تؤثر اتجاهات التكنولوجيا على قطاع الأمن في 2024؟

تؤثر اتجاهات التكنولوجيا على قطاع الأمن في عام 2024 بشكل كبير، حيث تتزايد الهجمات السيبرانية وتتطور أساليبها باستمرار، مما يستدعي تعزيز التدابير الأمنية وتطوير استراتيجيات جديدة لمواجهة هذه التهديدات المتزايدة.

أهم اتجاهات التكنولوجيا وتأثيرها على الأمن:

1. **الذكاء الاصطناعي والتعلم الآلي:**
   - يُستخدم الذكاء الاصطناعي في تعزيز قدرات الكشف عن التهديدات والاستجابة لها، وتحليل البيانات بشكل أسرع وأكثر دقة .
   - يستغل مجرمو الإنترنت أيضًا هذه التقنيات في شن هجمات أكثر تطوراً وفاعلية .
2. **أمن الثقة المعدومة:**
   - مع زيادة العمل عن بعد والخدمات السحابية، أصبح أمن الثقة المعدومة ضرورة لحماية الشبكات والتطبيقات والبيانات .
   - يقوم هذا النهج على عدم الثقة بأي شيء داخليًا أو خارجيًا والتحقق من جميع الأجهزة والأشخاص .
3. **إدارة الهوية والوصول:**
   - توسيع نطاق وظائف أنظمة الوصول وتعزيزها أمر بالغ الأهمية، بالإضافة إلى تحسين الكشف عن التهديدات والاستجابة لها .
4. **التقنيات المساعدة للخصوصية:(PETs)**
   - تعتبر PETs مهمة في ظل تزايد المخاوف بشأن خصوصية البيانات، حيث توفر حلولًا مبتكرة لحماية المعلومات الشخصية مع السماح بتحليل البيانات واستخدامها .
5. **الهجمات السيبرانية المتزايدة:**
   - يشهد العالم زيادة في الهجمات السيبرانية، مما يتطلب من الشركات والمؤسسات اتخاذ إجراءات استباقية لحماية نفسها .
6. **الحوسبة الكمومية:**
   - تُعد الحوسبة الكمومية تطورًا تكنولوجيًا واعدًا، لكنها تحمل أيضًا تحديات أمنية محتملة تتطلب دراستها ومواجهتها .
7. **التقنيات الإقناعية:**
   - يمكن استخدام التقنيات الإقناعية في تعزيز الأمن، ولكن يجب أن يتم ذلك بطريقة أخلاقية ومسؤولة، مع احترام خصوصية المستخدمين .

توصيات:

- **تعزيز الوعي الأمني:**
يجب على الأفراد والشركات زيادة الوعي حول التهديدات السيبرانية وكيفية التعامل معها .
- **تطبيق تدابير أمنية قوية:**
يجب على الشركات تطبيق مجموعة من التدابير الأمنية، مثل التشفير والمصادقة متعددة العوامل، وحماية السحابة .
- **تطوير استراتيجيات استباقية:**
يجب على الشركات تطوير استراتيجيات استباقية للكشف عن التهديدات والاستجابة لها، بدلاً من الاعتماد على الاستجابة بعد وقوع الهجوم .
- **التعاون وتبادل المعلومات:**
يجب على الشركات التعاون وتبادل المعلومات حول التهديدات والحلول الأمنية لتعزيز الأمن السيبراني بشكل عام .

أفضل الممارسات لضمان أمن تكنولوجيا المعلومات

لضمان أمن تكنولوجيا المعلومات، هناك عدة ممارسات أساسية يجب اتباعها .تشمل هذه الممارسات تحديث البرامج والأنظمة بانتظام، واستخدام كلمات مرور قوية، وتفعيل المصادقة متعددة العوامل، وتدريب الموظفين على الوعي الأمني، والنسخ الاحتياطي للبيانات بشكل دوري، واستخدام برامج مكافحة الفيروسات، وتشفير البيانات، وتنفيذ جدار حماية، والتحكم في الوصول إلى البيانات، وتطبيق سياسات أمنية واضحة، ومراقبة الشبكة والأنظمة للكشف عن أي نشاط مشبوه، وإجراء تقييمات دورية للمخاطر.

أفضل الممارسات بالتفصيل:

1. **حديث البرامج والأنظمة:**

تحديث البرامج وأنظمة التشغيل بانتظام يضمن تصحيح الثغرات الأمنية التي قد يستغلها المتسللون .

2. **كلمات المرور القوية:**

استخدام كلمات مرور قوية ومعقدة، وتغييرها بشكل دوري، وتجنب استخدام كلمات مرور متكررة على حسابات مختلفة .

3. **المصادقة متعددة العوامل:**

تفعيل المصادقة متعددة العوامل يضيف طبقة إضافية من الحماية تتجاوز مجرد كلمة المرور، مما يجعل من الصعب على المهاجمين الوصول إلى الحسابات .

4. **الوعي الأمني:**

تدريب الموظفين على الوعي الأمني وممارسات الأمان الجيدة، مثل عدم فتح رسائل البريد الإلكتروني المشبوهة أو النقر على الروابط غير الموثوقة، أمر بالغ الأهمية .

5. **النسخ الاحتياطي للبيانات:**

إجراء نسخ احتياطي منتظم للبيانات، وتخزينها في مكان آمن، يضمن استعادة البيانات في حالة وقوع أي حادث أمني أو كارثة .

6. **برامج مكافحة الفيروسات:**

استخدام برامج مكافحة الفيروسات وتحديثها بانتظام للكشف عن البرامج الضارة ومنعها .

7. **تشفير البيانات:**

تشفير البيانات الحساسة أثناء التخزين والنقل يضمن عدم تمكن أي شخص غير مصرح له من قراءتها أو الوصول إليها .

8. **جدار الحماية:**

استخدام جدار الحماية لحماية الشبكة من الوصول غير المصرح به .

9. **التحكم في الوصول:**

تنفيذ سياسات صارمة للتحكم في الوصول إلى البيانات والتطبيقات، وضمان أن المستخدمين لديهم فقط الأذونات اللازمة للوصول إلى الموارد التي يحتاجونها .

10. **سياسات الأمن:**

وضع سياسات أمنية واضحة وموثقة، وتدريب الموظفين عليها، وتطبيقها بانتظام .

11. مراقبة الشبكة:

مراقبة الشبكة والأنظمة للكشف عن أي نشاط مشبوه، مثل محاولات الوصول غير المصرح بها أو حركة مرور غير عادية .

12. تقييم المخاطر:

إجراء تقييمات دورية للمخاطر لتحديد نقاط الضعف في البنية التحتية الأمنية، واتخاذ الإجراءات التصحيحية المناسبة .

الأمن المادي والبيئي

الوحدة السادسة عشر

الأمن المادي والبيئي

ما هو ISO 27002؟

ISO 27002هو معيار دولي يقدم إرشادات للمؤسسات حول كيفية اختيار وتنفيذ وصيانة ضوابط أمن المعلومات يهدف إلى مساعدة المؤسسات على إنشاء نظام إدارة أمن المعلومات (ISMS) الذي يركز على الأمن السيبراني وحماية الأصول المعلوماتية

- **ضوابط أمن المعلومات:**
  يصف ISO 27002 مجموعة من الضوابط التي يمكن للمؤسسات تطبيقها لحماية معلوماتها من التهديدات المختلفة .
- **نظام إدارة أمن المعلومات:(ISMS)**
  يوفر ISO 27002 إطارًا للمؤسسات لتطوير وتنفيذ وصيانة نظام إدارة أمن المعلومات (ISMS) بشكل فعال .
- **التوجيهات:**
  يقدم المعيار إرشادات حول كيفية اختيار وتنفيذ وصيانة الضوابط الأمنية المختلفة .
- **التحديثات:**
  تم تحديث ISO 27002 في عام 2022، مع التركيز على أحدث التهديدات والمخاطر الأمنية .
- **العلاقة بـ:ISO 27001**
  يعتبر ISO 27002 مكملاً لمعيار ISO 27001، حيث يوفر تفاصيل حول الضوابط التي يمكن للمؤسسات تنفيذها لتحقيق متطلبات .ISO 27001

باختصار، ISO 27002هو دليل شامل للمؤسسات التي تسعى إلى حماية معلوماتها من خلال تطبيق ضوابط أمن المعلومات المناسبة .

سياسة الأمن المادي والبيئي

سياسة الأمن المادي والبيئي هي مجموعة من الإجراءات والضوابط التي تهدف إلى حماية الأصول المادية والمعلومات من التهديدات المحتملة، سواء كانت طبيعية أو من صنع الإنسان .تشمل هذه السياسات حماية المباني والمعدات والمخازن والمعلومات من السرقة والتلف والوصول غير المصرح به .

أهمية سياسة الأمن المادي والبيئي:

- **حماية الأصول:**
تضمن حماية الأصول المادية والمعلومات من التلف والسرقة والوصول غير المصرح به .
- **الاستمرارية:**
تساعد في الحفاظ على استمرارية العمليات من خلال حماية البنية التحتية من الكوارث الطبيعية أو الحوادث .
- **الامتثال:**
تضمن الامتثال للمتطلبات القانونية والتنظيمية المتعلقة بالأمن والسلامة .
- **الثقة:**
تعزز الثقة في المنظمة من قبل العملاء والموظفين والشركاء .
- **الحد من المخاطر:**
تقلل من المخاطر المحتملة التي قد تؤثر على سمعة المنظمة أو أرباحها .

عناصر سياسة الأمن المادي والبيئي:

- **التحكم في الوصول:**
تحديد وتقييد الوصول إلى المناطق الحساسة باستخدام بطاقات التعريف أو أنظمة المراقبة .
- **المراقبة:**
استخدام كاميرات المراقبة وأنظمة الإنذار للكشف عن أي تهديدات محتملة .
- **الحماية المادية:**
استخدام الأقفال والأبواب والنوافذ المقاومة للحريق والسرقة لحماية الأصول .
- **إدارة الكوارث:**
وضع خطط للطوارئ للتعامل مع الكوارث الطبيعية أو الحوادث التي قد تؤثر على الأصول .
- **إدارة البيئة:**
الحفاظ على بيئة عمل آمنة وصحية من خلال التحكم في درجة الحرارة والرطوبة والتهوية .
- **التدريب والتوعية:**
تدريب الموظفين على إجراءات الأمن والسلامة ورفع مستوى الوعي لديهم حول المخاطر المحتملة .
- **مراجعة وتحديث السياسات:**
مراجعة وتحديث سياسات الأمن المادي والبيئي بشكل دوري للتأكد من فعاليتها وشمولها .

أمثلة على الإجراءات المادية:

- تحديد مناطق آمنة ووضع حواجز مادية حولها.
- تركيب كاميرات مراقبة في المناطق الحساسة.
- استخدام أقفال متينة للأبواب والنوافذ.
- توفير حراس أمن في المناطق ذات الأهمية .

أمثلة على الإجراءات البيئية:

- الحفاظ على درجة حرارة ورطوبة مناسبة في مراكز البيانات.
- توفير أنظمة تهوية مناسبة.
- تأمين مصادر الطاقة الاحتياطية في حالة انقطاع التيار الكهربائي.
- وضع خطط لإدارة الحرائق والكوارث الطبيعية .

تحديات تنفيذ سياسة الأمن المادي والبيئي

تتضمن تحديات تنفيذ سياسات الأمن المادي والبيئي عدة جوانب، منها: التهديدات السيبرانية المتزايدة، والتحديات المتعلقة بالعمل عن بعد، ونقص الموارد والمهارات الأمنية، وزيادة تعقيد البيئات التقنية، والحاجة إلى التوعية والتدريب الأمني .

التحديات الرئيسية:

- **التهديدات السيبرانية المتزايدة:**
مع تزايد الاعتماد على التقنيات الرقمية، تزداد الهجمات الإلكترونية التي تستهدف البنية التحتية المادية والبيئية، مما يتطلب تعزيز الأمن السيبراني لحماية الأصول المادية والبيئية .
- **التحديات المتعلقة بالعمل عن بعد:**
مع انتشار العمل عن بعد، أصبح دمج الأمن المادي والأمن السيبراني أكثر تعقيدًا، حيث يجب على المؤسسات توسيع نطاق سياساتها الأمنية لتشمل بيئات العمل عن بعد، بما في ذلك الشبكات المنزلية الآمنة وتخزين المستندات المادية .
- **نقص الموارد والمهارات الأمنية:**
يواجه العديد من المؤسسات تحديات في تأمين الموارد المالية والبشرية اللازمة لتنفيذ سياسات الأمن المادي والبيئي، بالإضافة إلى نقص الكفاءات الأمنية المتخصصة .
- **زيادة تعقيد البيئات التقنية:**
مع تطور التكنولوجيا، أصبحت البيئات التقنية أكثر تعقيدًا، مما يزيد من صعوبة تأمينها وحمايتها من التهديدات .
- **التوعية والتدريب الأمني:**
يجب توفير التوعية والتدريب للموظفين حول مخاطر الأمن المادي والبيئي وكيفية التعامل معها بشكل فعال وآمن .
- **التهديدات البيئية:**
يجب الأخذ في الاعتبار التهديدات البيئية مثل درجات الحرارة القصوى، والعفن، والأمراض، والكوارث الطبيعية، والحرائق .
- **الكوارث من صنع الإنسان:**
يجب اختيار مواقع المراكز التي تحتوي على معدات تقنية معلومات بعيدًا عن مصادر الخطر المحتملة مثل المطارات والثكنات العسكرية .
- **البنية التحتية:**
يجب أن تعتمد المراكز على مصادر طاقة موثوقة وأن تكون هناك مصادر مياه متعددة وأنظمة اتصال موثوقة .
- **تفرد الغرض:**
يجب أن تكون مراكز البيانات منفصلة عن المكاتب الأخرى، خاصة إذا كانت تابعة لمؤسسات أخرى .
- **محيط الموقع:**
يجب اختيار مواقع المراكز بعناية لتقليل المخاطر المحتملة .

إنترنت الأشياء

الوحدة السابعة عشر

إنترنت الأشياء

المقصود بإنترنت الأشياء

إنترنت الأشياء (IoT) هو مصطلح يشير إلى شبكة واسعة من الأجهزة والأشياء المادية المتصلة بالإنترنت، والتي تمكنها من جمع البيانات وتبادلها مع أجهزة وأنظمة أخرى1] ، 3 .[هذه "الأشياء" يمكن أن تكون أي شيء، بدءًا من الأجهزة المنزلية الذكية وحتى الآلات الصناعية المعقدة، مما يتيح لها التواصل والتفاعل مع بعضها البعض ومع العالم الخارجي]

- **الأجهزة المتصلة:**
أجهزة مادية مزودة بأجهزة استشعار، برامج، وتقنيات أخرى تمكنها من جمع البيانات وإرسالها عبر الإنترنت
- **الاتصال:**
القدرة على الاتصال بالإنترنت وتبادل البيانات بين الأجهزة المختلفة، سواء كانت أجهزة محمولة، أجهزة منزلية، أو آلات صناعية
- **التحليل واتخاذ القرارات:**
القدرة على تحليل البيانات التي تجمعها الأجهزة واستخدامها لاتخاذ قرارات ذكية، سواء بشكل آلي أو من خلال تدخل بشري.

أمثلة على تطبيقات إنترنت الأشياء:

- **المنازل الذكية:**
التحكم في الإضاءة، درجة الحرارة، الأجهزة المنزلية، وأنظمة الأمان عن بعد .
- **السيارات المتصلة:**
تتبع حالة السيارة، تحسين استهلاك الوقود، وتوفير خدمات السلامة
- **الرعاية الصحية:**
مراقبة صحة المرضى عن بعد، وتوفير رعاية مخصصة .
- **التصنيع الذكي:**
تحسين كفاءة العمليات الصناعية، وتقليل التكاليف، وزيادة الإنتاجية

كيف يستطيع إنترنت الأشياء تحسين حياتنا

يمكن لإنترنت الأشياء (IoT) أن يحسّن حياتنا بعدة طرق، من خلال تحسين الكفاءة، والأتمتة، وتوفير التكاليف، وزيادة الراحة والأمان .تشمل التطبيقات العملية مراقبة الصحة عن بعد، وإدارة الطاقة الذكية، والزراعة الدقيقة، والمدن الذكية، وتحسين سلامة السيارات، وغير ذلك الكثير.

تحسين الكفاءة والأتمتة:

- **الصحة:**
تتيح الأجهزة القابلة للارتداء مثل الساعات الذكية وأجهزة مراقبة الجلوكوز مراقبة صحة الأفراد عن بعد، مما يسمح للأطباء بتقديم رعاية شخصية وتدخل مبكر إذا لزم الأمر .
- **إدارة الطاقة:**
تساعد أنظمة إدارة الطاقة الذكية في تقليل استهلاك الطاقة من خلال التحكم التلقائي في الإضاءة والتدفئة والتبريد بناءً على الاستخدام والظروف البيئية .
- **الزراعة:**
يمكن لأجهزة استشعار التربة والمناخ في المزارع الذكية توفير بيانات دقيقة حول احتياجات النباتات، مما يتيح للمزارعين استخدام الموارد بكفاءة أكبر وتقليل استخدام المياه والأسمدة .
- **المدن الذكية:**
يمكن لأجهزة الاستشعار في المدن الذكية مراقبة جودة الهواء وحركة المرور وأنظمة إدارة النفايات، مما يتيح للمسؤولين اتخاذ قرارات مستنيرة لتحسين جودة الحياة .
- **سلامة السيارات:**
تساعد أنظمة مساعدة السائق المتقدمة (ADAS) وأنظمة الملاحة في السيارات المتصلة على تحسين سلامة القيادة وتجنب الحوادث .

توفير التكاليف:

- **الصناعة:**
يمكن للتصنيع الذكي باستخدام إنترنت الأشياء تحسين الكفاءة وتقليل النفايات وتكاليف الصيانة .
- **إدارة المرافق:**
يمكن لمراقبة استهلاك الطاقة والمياه في المباني الذكية تحديد مجالات الهدر وتحسين الكفاءة، مما يؤدي إلى توفير كبير في التكاليف .
- **النقل:**
يمكن لإنترنت الأشياء تحسين إدارة أساطيل النقل، وتقليل استهلاك الوقود، وتكاليف الصيانة، وتكاليف التأمين .

زيادة الراحة والأمان:

- **المنازل الذكية:**
يمكن لأجهزة إنترنت الأشياء في المنازل الذكية توفير الراحة والأمان من خلال التحكم في الإضاءة والأجهزة عن بعد، وتنبيه السكان في حالة وجود تسرب للغاز أو حريق .

- **المجتمعات الذكية:**

يمكن للمدن الذكية استخدام إنترنت الأشياء لتحسين السلامة العامة، وتوفير خدمات الطوارئ بشكل أسرع، وتسهيل التواصل بين السكان .

- **خدمات العملاء:**

يمكن للشركات التي تستخدم إنترنت الأشياء تحسين خدمات العملاء من خلال توفير دعم مخصص، وتوقع احتياجات العملاء، وتوفير تجارب مخصصة .

ما المقصود بـ AWS IoT وما فائدته؟

AWS IoT، أوAmazon Web Services IoT ، هي مجموعة من الخدمات السحابية التي تمكّن الأجهزة المتصلة (مثل أجهزة الاستشعار والأجهزة الذكية) من الاتصال بـ AWS، ومعالجة البيانات، والتفاعل مع الخدمات السحابية الأخرى فائدتها تكمن في تمكين الشركات من بناء وتوسيع نطاق تطبيقات إنترنت الأشياء ((IoTبسهولة وأمان، مع الاستفادة من قدرات التحليلات والذكاء الاصطناعي المتاحة في سحابة AWS

شرح مفصل:

- **ما هوAWS IoT ؟**

AWS IoT هو مجموعة من الخدمات السحابية المُدارة بالكامل من Amazon، مصممة خصيصًا لتمكين الاتصال الآمن وإدارة الأجهزة المتصلة (IoT)

- **كيف يعمل؟**

يقوم AWS IoT بتوفير أدوات لربط الأجهزة بـAWS ، وإرسال واستقبال البيانات، وإدارة الأجهزة، وتحليل البيانات، وتنفيذ إجراءات بناءً على تلك البيانات

ما هي الفوائد؟

- **سهولة الاستخدام AWS IoT :**يوفر واجهات سهلة الاستخدام لإدارة الأجهزة المتصلة وتطوير تطبيقات إنترنت الأشياء
- **قابلية التوسع :**يتيح AWS IoT للشركات توسيع نطاق تطبيقاتها لتشمل عدد كبير من الأجهزة والبيانات دون الحاجة إلى إدارة البنية التحتية الخاصة بها
- **الأمان :**يوفر AWS IoT ميزات أمان متقدمة لحماية بيانات الأجهزة والاتصالات، مثل التشفير والتحكم في الوصول
- **التحليلات والذكاء الاصطناعي :**يتكامل AWS IoT مع خدمات تحليل البيانات والذكاء الاصطناعي فيAWS ، مما يتيح للشركات استخلاص رؤى قيمة من بيانات الأجهزة
- **التكامل :**يتكامل AWS IoT مع خدمات AWS الأخرى، مما يتيح للشركات بناء حلول إنترنت الأشياء متكاملة ومتطورة

أمثلة على الاستخدام:

- **المنازل الذكية :**تمكين الأجهزة المنزلية المتصلة (مثل الإضاءة، والأجهزة، وأنظمة الأمان) من التفاعل مع بعضها البعض وتحسين تجربة المستخدم
- **الصناعة :**مراقبة وتحليل بيانات المعدات الصناعية في الوقت الفعلي لتحسين الكفاءة وتقليل وقت التوقف عن العمل
- **الرعاية الصحية :**مراقبة صحة المرضى عن بعد وتقديم رعاية شخصية بناءً على البيانات.
- **الخدمات اللوجستية :**تتبع الأصول في الوقت الفعلي وتحسين إدارة سلسلة التوريد

تطبيقات إنترنت الأشياء

تطبيقات إنترنت الأشياء (IoT) متعددة ومتنوعة، وتشمل مجالات مختلفة مثل المنازل الذكية، والمدن الذكية، والصحة، والزراعة، والصناعة، والنقل.

أمثلة على تطبيقات إنترنت الأشياء:

- **المنازل الذكية:**

التحكم في الإضاءة، والتدفئة، والأجهزة المنزلية عن بعد، وأنظمة الأمان

- **المدن الذكية:**

إدارة حركة المرور، وأنظمة الإضاءة العامة، وإدارة النفايات، ومراقبة جودة الهواء والمياه، وتوفير الطاقة

- **الصحة:**

الأجهزة القابلة للارتداء لتتبع اللياقة البدنية والصحة، والأجهزة الطبية المتصلة لمراقبة المرضى عن بعد

- **الزراعة الذكية:**

رصد البيئة الزراعية، وإدارة الموارد مثل المياه والتربة، وتحسين إنتاجية المحاصيل

- **الصناعة:**

مراقبة العمليات الصناعية، وتحسين الكفاءة، والصيانة التنبؤية، والتحكم في الإنتاج عن بعد

- **النقل:**

تتبع حركة المرور، وتحسين إدارة حركة المرور، وتطوير خدمات النقل العام، وتمكين السيارات المتصلة

فوائد تطبيقات إنترنت الأشياء:

- **تحسين الكفاءة:**

أتمتة العمليات، وتحسين استخدام الموارد، وتقليل التكاليف

- **تحسين السلامة:**

مراقبة البيئة، والتحذير من المخاطر المحتملة، وتحسين السلامة في المنازل والصناعة والنقل

- **تحسين جودة الحياة:**

توفير الراحة، وتحسين الخدمات، وتحسين إدارة الموارد

- **توفير الطاقة:**

تحسين استخدام الطاقة في المنازل والمدن والمصانع

- **تطوير المدن الذكية:**

توفير خدمات أفضل للسكان، وتحسين إدارة الموارد، وتحسين البيئة