# المحاضرة ١٥

(أنواع شبكات الحاسب الآلي و امن المعلومات)

**أنواع شبكات الحاسب الآلي من حيث المساحة الجغرافية :**

**تنقسم شبكات الحاسب الآلي من حيث المساحة الجغرافية التي تغطيها إلى نوعين رئيسيين هما:**

١. شبكات الحاسب الآلي المحلية ((Local Area Network (LAN)
- وهي منظومة من الحاسبات الآلية وأجهزة الربط الأخرى التي يجمعها مكان محدود كشركة أو مؤسسة.

٢. شبكات الحاسب الآلي الواسعة ((Wide Area Network (WAN)
- وهي منظومة من الحاسبات الآلية وأجهزة الربط الأخرى التي تتوزع على نطاق واسع (على مستوى المدينة أو الدولة أو العالم).

**أنواع شبكات الحاسب الآلي من حيث المركزية :**

١. شبكة الخادم والعميل (Client/Server)
- تتكون من جهاز مركزي (Server) يقدم مجموعة من الخدمات عبر الشبكة لحواسيب - عملاء - اخرى (Clients) .

٢. شبكات الحاسب الآلي الواسعة (Peer-to-Peer)
- تتكون الأجهزة في هذا النوع من الشبكات متكافئة، وبإمكان أي جهاز أن يكون خادم وعميل في نفس الوقت.

**ما هو مفهوم INTERNET ، INTRANET و EXTRANET :**

- **INTERNET :** هو وسيلة اتصال محوسبة ذات إقبال جماهيري مصنفة اليوم كرابع وسيلة اتصال من حيث عدد مستخدميها في العالم.
- **INTRANET :** هي شبكة اتصال خاصة تستخدم الموارد المتاحة للإنترنت (INTERNET) من اجل توزيع معلومات وتطبيقات يمكن لمجموعات خاصة فقط من الوصول إليها.
- **EXTRANET :** هو امتداد للشبكة الداخلية بحيث تسمح لمجموعات خارجية كالموردين والزبائن وأطراف أخرى بالاطلاع على المعلومات التي يتم عرضها بواسطة INTRANET

**INTRANET الحل للحاجات المعلوماتية داخل بيئة المنشأة**

- INTRANET هو عبارة عن نظام وثيق الصلة بالإنترنت، يتكون من شبكة تعتمد على معايير وإجراءات مفتوحة معدة أصلا للإنترنت تسمح بتوفير خدمات عديدة
- **مثل :** البريد الإلكتروني ومجموعات العمل وخدمات إدارية وأمن في الوصول إلى قواعد المعلومات والمشاركة في المعلومات و إدارة النظم

**المزايا الأساسية لاستخدام INTRANET**

١. تجانس نظم المعلومات المستخدمة في جميع الشبكة وتمتعها بنفس الخصائص، الأمر الذي يسهل من الوصول للمعلومات والبحث عنها.
٢. تسهيل عملية تبادل المعلومات داخل المنشأة.
٣. الحصول على المعلومات في الوقت الحقيقي (Real Time) او فور حدوث الحدث المتعلق بها.
٤. رفع كفاءة عمليات الاتصال واتخاذ القرارات.
٥. المساهمة في زيادة تلقائية العمليات الأمر الذي يسهم في تسريع عمليات التشغيل.
٦. تسهل نظام العمل في مجموعات وجعله اكثر سرعة وكفاءة وذلك من خلال تسهيل وتسريع عملية الحصول على المعلومات وتحليلها.

## نظام EXTRANET

نظام EXTRANET ؛ هو عبارة عن شبكة أعمال خاصة مكونة من عدة أطراف أو منشآت (زبائن أو موردين أو شركاء .. الخ) ذات علاقة مباشرة مع عمليات إحدى المنشآت ولكن هذه الأطراف تقع خارج حدود نظام الحماية أو بالأحرى خارج حدودINTRANET .

بعبارة أخرى يمكن اعتباره مكونا من مجموعة من الأطراف أو الشركات التي تتبادل فيما بينها معلومات معينة، من اجل تسهيل عمل منظم بما يؤدي إلى توفير الوقت والتكلفة. و يعتبر نظام EXTRANET من الأدوات الحديثة التي سوف تسمح بحدوث ثورات و طفرات تجارية و اقتصادية ليس فقط على مستوى منشآت الأعمال بل سيمتد ذلك ليشمل

المنظمات الحكومية.

**يمكن تلخيص مزايا استخدام نظام EXTRANET فيما لي :**

١. أداة قادرة على زيادة فاعلية العمليات التشغيلية والصفقات.
٢. عامل مهم في تخفيض التكاليف من خلال ضمان تدفق المعلومات وسرعة نقلها و المقدرة على توفير المرونة والعمق في عملية التزويد.
٣. يمكن من تخفيض تكاليف العمليات التجارية الدورية (الاعتيادية) بما يحتويه من إمكانات كبيرة سواء على المستوى التشغيلي او على المستوى الاستراتيجي.
٤. يساهم في تحقيق نتائج مالية افضل للمنشآت عن طريق تخفيض دورة الطلب و التوريد وما يؤدي إليه ذلك من تخفيض تكاليف التخزين.
٥. تخفيض تكاليف توصيل المعلومات الخاصة بالعمليات التجارية وذلك على اعتبار ان هذا النظام ارخص من وسائل اتصال اخرى ذات طابع تقليدي.
٦. تخفيض مدة التحصيل وذلك اعتمادا على السرعة في الإدارة ومتابعة شئون الفواتير.
٧. تخصيص وقت الموظفين الإداريين في أشغال ومهمات ذات قيمة مضافة.

# أمن المعلومات

❖ **مقدمة :** حدد بعض المؤلفين ثلاث ركائز أساسية لأمن المعلومات هي :

- السرية (Confidentiality)، وتكامل وسلامة المعلومة (Integrity) ، والتوفر (Availability) وأطلق على ذلك مثلث (CIA)
- إلا أن الاتحاد العالمي للاتصالات في توصيته قد حدد عناصر أساسية لأمن المعلومات يمكن حصرها في ستة عناصر رئيسية هي: التحقق من الهوية، التحكم بالوصول، السرية، سلامة وتكامل المعلومة، عدم الإنكار، توفر أو ديمومة المعلومة

**تعريف أمن المعلومات**

❖ " المفاهيم والتقنيات والتدابير التقنية والإدارية المستخدمة لحماية أصول المعلومات من الوصول غير المأذون به عمداً أو سهواً أو حيازتها أو الإضرار بها، أو كشفها، أو التلاعب بها، أو تعديلها، أو فقدها أو إساءة استخدامها"

❖ وتعرّف لجنة أنظمة الأمن القومي الأمريكية (CNSS) أمن المعلومات بأنها "حماية المعلومات وعناصرها الهامة (الحرجة) بما في ذلك الأنظمة والأجهزة التي تَستخدِم وتخزن وترسل هذه المعلومات".

❖ ويعتبر هذا التعريف هو التعريف الأنسب نظراً لشموليته للمعلومات بكافة أشكالها وعناصرها والتي من أهمها الأجهزة والأنظمة (البرامج) التي تخزن وتعالج وترسل هذه المعلومات.

**ماهية عناصر أمن المعلومات :**

- يمكن تعريف أمن المعلومات بأنها "مجموعة العناصر الواجب توافرها لحماية المعلومات الثابتة والمنقولة بحيث يغطي كل عنصر من هذه العناصر جانبا من جوانب الحماية المطلوبة".
- ومعنى ذلك هو أن تتكامل هذه العناصر حتى توفر الحماية المطلوبة، وعند فقد أي منها فسيكون هناك خلل أمني في الجانب الذي يغطي هذا العنصر.

**العناصر الأساسية لأمن المعلومات**

١. **التحقق من الهوية (Authentication)**

- تعني الخدمة التي يمكن من خلالها التحقق من هوية الشخص (أو الجهة) من أنه الشخص المعني لا غيره.
- عند اتصال شخصين (أو جهتين) مع بعضهما البعض، فلا بد من أن يتعرّف كل منهما على الآخر لضمان أن كل منهما يتخاطب مع الشخص أو الجهة المعنية وليس غيرها. وبعبارة أخرى التحقق من الهوية هو التحقق من أن المستخدم لنظام ما هو بالفعل من ادعى أنه ذلك المستخدم.

❖ ويمكن استخدام معيار أو أكثر للتحقق من الهوية حسب درجة قوة التحقق المطلوبة، فيمكن التحقق باستخدام معيار واحد أو معيارين أو ثلاثة معايير معا كما يلي:

١. **التحقق باستخدام معيار واحد. هذا المعيار هو "ماذا تعرف؟"**
   - كاستخدام كلمات المرور أو أرقام التعريف الشخصية (PIN)
٢. **التحقق باستخدام معيارين. ويتم ذلك باستخدام معيار "ماذا تعرف؟" بالإضافة لمعيار آخر هو "ماذا تملك؟".**

- من الأمثلة على ذلك استخدام بطاقات الصرف الإلكتروني (ATM) حيث يتم التحقق من هوية الشخص من خلال رقم بطاقة الصراف التي لا يملكها إلا هو ثم إدخال الرقم السري الذي لا يعرفه إلا هو كذلك، ولا يمكن أن يغني أحدهما عن الآخر.

**٣. التحقق باستخدام ثلاثة معايير. ويتم ذلك باستخدام معيار "ماذا تعرف؟" ومعيار "ماذا تملك؟" بالإضافة إلى معيار ثالث هو "من أنت".**

- وتعتمد هذه الطريقة في التحقق من الهوية على طلب (إدخال) معلومة لا يعرفها إلى الشخص المعني فقط، ومعلومة أخرى لا يملكها إلا نفس الشخص، ومعلومة ثالثة من واحدة أو أكثر من خصائص الشخص التي تميزه عن غيره كبصمات الأصابع.
- توفر هذا الطريقة أعلى درجات التحقق من الهوية وتعتبر أكثر تعقيداً من سابقاتها.

### ٢. التحكم بالوصول (Access Control)

- ويقصد به القدرة على التحكم بالوصول إلى الموارد المتاحة كالأجهزة الرئيسية والبيانات المركزية.
- يأتي عنصر التحكم بالوصول بعد عنصر التحقق من الهوية فعندما يتم التحقق من هوية الشخص والسماح له بالدخول إلى شبكة الحاسب الآلي مثلاً، فإنه يتم التحكم باستخدامه لموارد محددة من الشبكة وليس جميع الموارد عن طريق التحكم بالوصول.
- يمكن أن يكون هناك أشخاص لهم صلاحية الاطلاع (القراءة) فقط، وآخرين لهم صلاحية الطباعة، وآخرين لهم صلاحية الحذف وهكذا.

❖ ومن الأمثلة على الخروقات الممكنة لأمن المعلومات التي يمكن أن تتم في حال عدم توفر عنصر " التحكم بالوصول" :

- هي إمكانية قيام بعض المستخدمين (ممن لديه صلاحية الاطلاع على المعلومات الهامة والحساسة) بعد دخوله النظامي إلى شبكة المنشأة بطباعة وثائق هامة وحساسة على ورق وبالتالي يمكن إطلاع أي شخص على محتويات هذه الأوراق حيث أنها أصبحت خارج السيطرة.

### ٣. السرية (Confidentiality)

- يطلق على هذا العنصر أيضا الخصوصية (Privacy) وتعني الحفاظ على المعلومات من أن يطلع عليها (يقرأها و يفهمها) غير الأشخاص المصرح لهم فقط، أو بعبارة أخرى منع الكشف الغير مصرح به. عندما يتم إرسال رسالة "سرية"، فإن ذلك يتطلب أن لا يراها إلا المرسل والمرسل إليه فقط.
- هناك العديد من الطرق لتوفير السرية تتراوح بين حجب المعلومة يدويا وعدم تسليمها إلا للأشخاص المصرح لهم فقط إلى طرق التشفير الحديثة التي تعتمد على خوارزميات رياضية معقدة يصعب فكها إن لم يكن مستحيلا .
- قد يتبادر إلى ذهن البعض بأنه عندما يتوفر عنصر "السرية" للمعلومة، فإنها بذلك تصبح معلومة آمنة. أو بعبارة أخرى أن التشفير (وهو وسيلة لتحقيق عنصر السرية) يضمن أمن المعلومة بشكل كامل، وهذا مفهوم خاطئ. والصحيح أن السرية ما هي إلا عنصر واحد من عدة عناصر رئيسية يجب توافرها جميعا لتصبح المعلومة آمنة.