الأمن والشبكات: ما هي الشبكة؟ أنواع الشبكات. مكونات الشبكة الأساسية:

شبكة الحاسوب هو الاندماج بين تكنولوجيا الاتصالات وتكنولوجيا الحاسبات باستخدام مجموعة من الحاسبات والاجهزة الاخرى المتصلة مع بعضها البعض حيث يكون لها القدرة على مشاركة عدد كبير من المستخدمين للبيانات Data والبرمجيات Software والاجهزة Hardware كما تعتبر الشبكة وسيلة اتصال الكتروني بين الافراد والتي تمكنهم من:

1- ارسال رسالة مكونة من عدة صفحات وصور وأصوات ورسومات متحركة الى مجموعة اشخاص في اي مكان دفعة واحدة وفي دقائق معدودة.
2- يتصل من حاسوب المنزل او العمل ببنوك المعلومات والشركات والمكتبات العالمية للحصول على المعلومات التي تهمه
3- عقد المؤتمرات والندوات التفاعلية لأطراف متباعدة عبر شبكة الانترنيت
4- التعليم عن بعد والتجارة الالكترونية والحكومة الألكترونية.

انواع شبكات الحاسوب

اولا : تصنيف الشبكات من حيث الحجم size

1- الشبكة المحلية **L**ocal **A**rea **N**etwork – **LAN**
2- الشبكة الواسعة **W**ide **A**rea **N**etwork – **WAN**
3- شبكة الانترانت
4- شبكة الإكسترانت
5- شبكة الانترنت
6- الإكسترانت
7- شبكة الانترنيت

ثانيا : تصنيف الشبكات من حيث طريقة التوصيلTopology:

1- شبكة المسار الخطي Bus Network
2- الشبكة الحلقية Token Ring Network

3- الشبكة النجمية Star Network

مكونات الشبكة:

تتكون شبكة الحاسوب من عدة أجزاء لكل جزء وظيفته الخاصة في النظام الشبكي وهذه الأجزاء:

1- **الحاسوب الرئيسي – الخادم Server**
2- **محطات العمل Work Stations**
3- خطوط الاتصال **Communication Lines**
4- بطاقات الشبكة **Network Interface Card**
5- المودم Modem
6- الأجهزة الملحقة
7- محولات الشبكة **Communication Switches**
8- **برامج الشبكة**

فوائد الشبكات:

1- المشاركة في استخدام الأجهزة Hardware اي استفادة أي مستخدم للشبكة من إمكانيات الحاسوب الرئيسي بدل من اقتناء حاسوب مستقل، كذلك الاستفادة من جميع الاجهزة الملحقة بالشبكة مثل الطابعات>
2- المشاركة في البرمجيات Software اي استفادة أي مستخدم للشبكة من البرمجيات المخزنة في الحاسوب الرئيسي أو أي حاسوب آخر متصل بالشبكة مثل مشاركة الملفات واستخدام البريد الالكتروني .
3- المشاركة في البيانات Data ونعني استخدام قاعدة بيانات واحدة تحتوي على جميع المعلومات يستخدمها جميع المتصلين بالشبكة كما هو متبع في البنوك وعند حجز تذاكر السفر وفي منافذ الحدود.
4- سهولة تحديث (تطويرUpdate) البرامج والبيانات نظرا لاجراء عملية التطوير مرة واحدة على الحاسوب الرئيسي وليس على كل محطة عمل.
5- شراء نسخة واحدة من البرامج وتحميلها على الحاسوب الرئيسي بالشبكة يكون أرخص ثمناً من شراء عدة نسخ فردية User-Single وتحميل كل منها على محطة عمل .

6- استخدام الانترنت Internet في البحث عن المعلومات واستخدام البريد الالكتورني Electronic Mail-E Mailوتبادل المعلومات والملفات بين المشاركين.
7- إمداد متخذي القرار من الإدارة العليا بالبيانات والمعلومات الحديثة بسرعة وبصورة شاملة.
8- إمكانية شراء وبيع السلع والخدمات والتسويق والقيام بالاعمال التجارية من خلال الشبكة e-commerce .
9- تقديم الخدمات للمواطنين بسرعة وسهولة وبأقل تكلفة كما هو متبع عند دفع فاتورة الهاتف وتجديد البطاقة المدنية وظهور ما يسمى بالحكومة االلكترونية.. .government-e
10- اعتماد العديد من الشركات على الشبكات في عملها بشكل أساسي كشركات الطيران والبنوك وغيرها.

امن الشبكات:

هي مجموعة من الإجراءات التي يمكن خلالها توفير الحماية القصوى للمعلومات والبيانات في الشبكات من كافة المخاطر التي تهددها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية.

تصنيف جرائم المعلومات:

1. جرائم تهدف لنشر معلومات: يتم نشر معلومات سرية تم الحصول عليها بطرق غير مشروعة عن طريق الاختراقات لشبكات المعلومات ونشر هذه المعلومات
2. جرائم تهدف لترويج الإشاعات. وهنا يتم نشر معلومات مغلوطة وغير صحيحة تتعلق بالأشخاص أو المعتقدات أو الدول بهدف تكدير السلم العام في البلدان، وكذلك نشر الإشاعات عن بعض الأشياء وإحداث البلبلة في المجتمعات.
3. جرائم التزوير الإلكترونية. وهنا يتم استخدام وسائل التكنولوجيا في عمليات التزوير بغرض تحقيق هدف معين، وكذلك يندرج تحتها عمليات التحويل المصرفي الوهمية من حسابات إلى أخرى عن طريق اختراق شبكات المصارف.
4. جرائم تقنية المعلومات. وأهم مثال لها هو عمليات القرصنة التي تحدث للبرامج الحاسوبية الأصلية والتي يتم عمل نسخ منها لتباع في الأسواق بدلاً من النسخ الأصلية.

مكونات أمن شبكات المعلومات:

ولاً: سرية المعلومات

[عدل]

(بالإنجليزية Data Confidentiality) : وهذا الجانب يشتمل على الإجراءات والتدابير اللازمة لمنع اطلاع غير المصرح لهم على المعلومات التي يطبق عليها بند السرية أو المعلومات الحساسة، وهذا هو المقصود بأمن وسرية المعلومات، وطبعاً درجة هذه السرية ونوع المعلومات يختلف من مكان لآخر وفق السياسة المتبعة في المكان نفسه، ومن أمثلة هذه المعلومات التي يجب سريتها: المعلومات الشخصية للأفراد.

ثانياً: سلامة المعلومات

[عدل]

(بالإنجليزية Data Integrity) : في هذا الجانب لا يكون الهم الأكبر هو الحفاظ على سرية المعلومات وإنما يكون الحفاظ على سلامة هذه المعلومات من التزوير والتغيير بعد إعلانها على الملأ، فقد تقوم هيئة ما بالإعلان عن معلومات مالية أو غيرها تخص الهيئة وهنا يأتي دور الحفاظ على السلامة بأن تكون هذه المعلومات محمية من التغيير أو التزوير، ومن أمثلة ذلك مثلاً: إعلان الوزارات أو الجامعات عن أسماء المقبولين للعمل بها، تتمثل حماية هذه القوائم في أن تكون مؤمنة ضد التغيير والتزوير فيها بحذف أسماء ووضع أسماء غيرها مما يسبب الحرج والمشكلات القانونية للمؤسسات، وأيضاً بالنسبة للمعلومات المالية بتغيير مبلغ مالي من 100 إلى 1000000 وهذا هام جداً لما يترتب عليه من خسائر فادحة في الأموال.

ثالثاً: ضمان الوصول إلى المعلومات

[عدل]

(بالإنجليزية Availability) : لعله من المنطقي أن نعرف أن كل إجراءات وصناعة المعلومات في الأساس تهدف إلى هدف واحد وهو إيصال المعلومات والبيانات إلى الأشخاص المناسبين في الوقت المناسب، وبالتالي فإن الحفاظ على سرية المعلومات وضمان سلامتها وعدم التغيير فيها لا يعني شيئاً إذا لم يستطع الأشخاص المخولين أو المصرح لهم الوصول إليها، وهنا تأتي أهمية الجانب الثالث من جوانب أو مكونات أمن المعلومات وهو ضمان وصول المعلومات إلى الأشخاص المصرح لهم بالوصول إليها من خلال توفير القنوات والوسائل الآمنة والسريعة للحصول على تلك المعلومات، وفي هذا الجانب يعمل المخربون بوسائل شتى لحرمان ومنع المستفيدين من الوصول إلى المعلومات مثل حذف المعلومات قبل الوصول إليها أو حتى مهاجمة أجهزة تخزين المعلومات وتدميرها أو على الأقل تخريبها.

دوافع الهجوم على شبكات المعلومات

[عدل]

يمكن أن يتبادر إلى الذهن سؤال وهو لماذا يقوم المخربون أو المخترقون بعمليات مثل اختراق شبكات المعلومات وتهديد أمن المعلومات؟ وما هي الدوافع التي يمكن أن تكون لديهم لكي يقوموا بمثل هذه الأعمال؟ فلابد لكل شخص من دوافع للقيام بعمل ما، وهنا سنتعرف على بعض الدوافع التي رصدها المختصون بمراقبة عمليات الاختراق وجرائم المعلومات لدى القائمون بهذه الهجمات.