الأصناف الكبرى للشبكات
Les Grandes Catégories de Réseaux

الشبكات موجودة منذ زمن طويل، وكانت تخصص لنقل المعلومة. ولكن يمكننا أن نصنف هذه الشبكات إلى:

1- شبكات هاتفية
2- شبكات معلوماتية أنشأت من الحاجة لإقامة الاتصال بين الحواسيب.
3- شبكات البث أو النشر للبرامج

- كل واحدة من هذه الأصناف لها خواص ومميزات تتعلق بالتطبيقات المطلوبة منها "الهاتفية - معلوماتية - تلفزيونية وفيديوية"

* ثورة الشبكات La Révolution des Réseaux

وُلدت الشبكات من الحاجة لنقل المعلومة من شخص لآخر، هذا الاتصال ظل لوقت طويل يُنشأ مباشرة بواسطة الإنسان مثل شبكة البريد - رسائل صوتية أو مرئية"

• إن أول ثورة في الشبكات كانت منذ أكثر من قرن وذلك بأتمتة نقل المعلومات أو المعطيات.

في البداية تم الاستعانة بالخطوط الأرضية للاتصالات المكونة بشكل أساسي من الأسلاك النحاسية، ومن ثم نُشرت المعلومة بالأمواج الهرتزية، ومن بعدها تم النقل بواسطة الليف البصري.

ويكون مناسبًا الإشارة لهذه الخطوط ما يعرف بشبكة المنفذ Réseaux d'accès وهذا ما يعرف بالحلقة المحلية Boucle locale وهي عبارة عن القسم الطرفي للشبكة مثلاً الخط التلفوني الذي يذهب من هاتف المشترك حتى المقسم.

واليوم يمكننا القول أن الشبكة هي عبارة عن مجموعة المنفذات ووصلات الاتصالات اللازمة لنقل المعلومة مهما تكن من نقطة لأخرى وأينما كانت.

• الثورة الثانية للشبكات كانت باستخدام المفهوم الرقمي، حيث أن الشبكات الحديثة هي عبارة عن شبكات رقمية.
هذه الشبكات تقوم بنقل المعلومة التي تكون مترجمة إلى لغة الأصفار "0" و الواحدات "1" وذلك مهما كانت طبيعة هذه المعلومة "صوت - فيديو - معطيات معلوماتية ..."
هنا فترة حديثة، الشبكات كانت محددة بالمعلومة التي تنقلها فهناك كما لاحظنا الثلاثة:
- شبكات الاتصالات
- شبكات المعلوماتية لربط الحواسيب ببعض
- شبكات النشر لفيديو مثل التلفزيون
• الثورة الثالثة:
اليوم وبواسطة التقنيات الحديثة أصبح بالإمكان أن تكون كل هذه الأصناف من الشبكات متحدة بآن واحد، وهذا ما يجعلنا نحصل على ما يعرف بشبكات الملتي ميديا MultiMédias.
وبالتالي الثورة الثالثة في الشبكات هي عبارة عن الملتي ميديا، هذه الشبكات نجحت في تمرير مختلف الأنواع "نص - صوت - صورة متحركة أو ثابتة ----" بنفس الوقت وبنفس الشبكة.
في الشبكات الخاصة، فإن السؤال الذي نطرح: ماهي التغيرات أو التعديلات التي يجب أن نطرأ على الشبكات الخاصة لتتحول لشبكات ملتي ميديا؟
طبعًا الجواب أو الأجوبة على هذا السؤال تكون مختلف وذلك تبعًا للتقنية المستخدمة: - بالنسبة لشبكات المعلوماتية فإنه لم يتغير شيئًا في نقل المعلومة، كنا فقط قمنا بإضافة خواص جديدة على البروتوكولات المستخدم طبعاً.
- أما في مجال الاتصالات فإنه على العكس يجب البحث عن تقنية جديدة لنقل المعلومة.
من جراء ذلك فإن عالم المعلوماتية عرف تحولاً أو تغيراً بسيطاً أما عالم الاتصالات فقد خضع لتحول هائل في تقنية الشبكات

Scanned by CamScanner

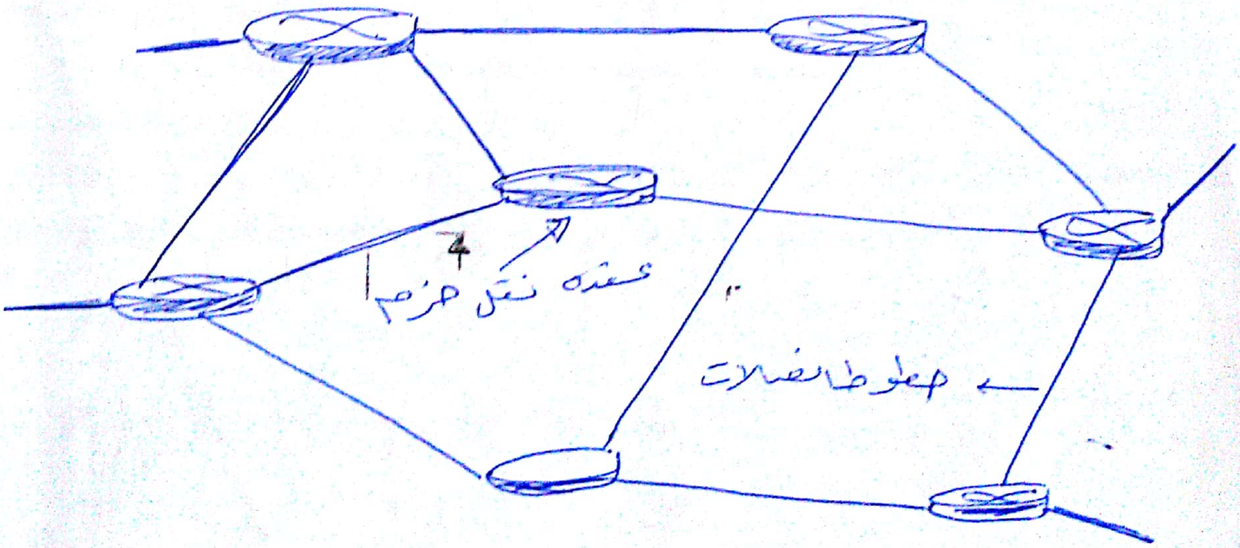
* نقل المعطيات Le Transport des Données

يوجد العديد من التقنيات لنقل المعطيات :

أ- تقنية تبديل الدارات : تاريخياً كانت الاولى حيث أنه يتم ارتباط العناصر الثنائية على دارة ، مثلاً الشبكة الهاتفية تستخدم تبديل الدارات "

ب- تقنية النقل بالحزم : إن أغلبية الشبكات الكبيرة تستخدم تقنية الحزم ((تجميع المعلومة)) ، وهذا يعني : تجميع البيانات المراد نقلها في حزم ، وحيث يكون لدينا سلسلة تحكم مضافة من أجل كونها لم تفقد هذه المعلومة ولم تتشوه .

وعندما تكون الحزم جاهزة فإنه يتم إرسالها بدءاً من الحلقة الأولى باتجاه العقدة الأولى ، وهذه العقدة تسمح للحزم بالدخول للشبكة ، ومن ثم تمرر من عقدة لعقدة حتى الوصول للمرسل إليه . كما هو مبين بالشكل



شكل : شبكة مكونة بالعقد لنقل الحزم

حيث أن سرعة الخطوط الخارجية للعقد يعبر عنها بـ bit/s وبما أنه بالوقت الحالي العقد تسمح بمعالجة عدد كبير من الحزم بالثانية ، وبالتالي فإن سعات الخطوط يعبر عنها بـ Kbit/s أو Mbit/s أو Gbit/s

+ أهم تقنيات نقل الحزم

إن من أهم التقنيات المستخدمة لنقل الحزم هي :

أ- تقنية Asynchronus Transfer Mode: ATM

وهي عبارة عن تقنية لنقل الحزم وحيث أن الحزم ذات طول ثابتة 53 octs وهذه الحزم صغيرة جداً .

ب- تقنية شبكة الانترنت : IP : Internet Protocol

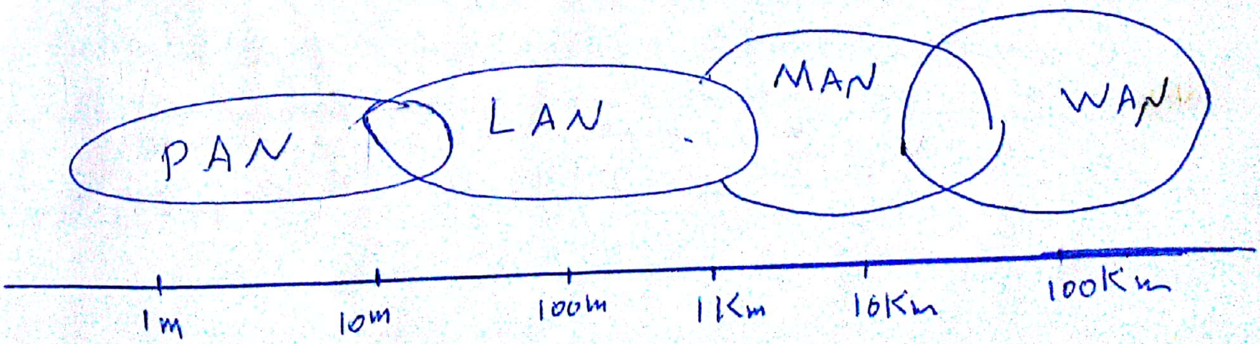
هنا الحزم تكون متغيرة الحجم والطول .

ج- تقنية النقل Ethernet

هذه التقنية تستخدم الحزم بأطوال متغيرة ، ولكنه تختلف عن تلك المستخدمة في التقنيات الاخرى .

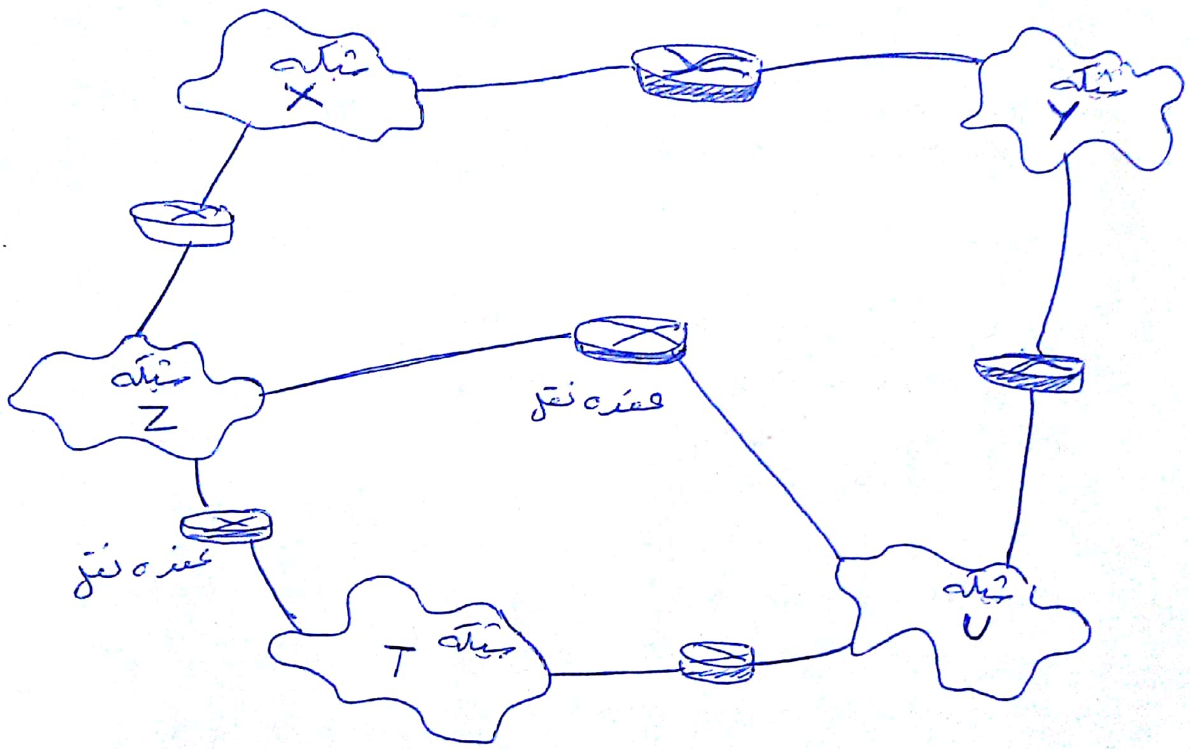
مع العلم أن IP و Ethernet ولدت من الحاجة للحواسيب لربطها لاتصالهم ببعض ، من أجل نقل ملفات المعلومات ، أما البروتوكول ATM فجاء من الاتصالات والصناعة .

هذه التقنيات تطبق على مختلف أصناف الشبكات ابتداءً من الشبكات واسعة الامتداد المسماة WAN : Wide Area Network ، وهي الشبكات المنزلية المسماة PAN : Personal Area Network ، مروراً بالشبكة المتوسطة MAN : Medium Area Network أو الشبكة المحلية LAN : Local Area Network



* الانترنيت Internet

جاءت كلمة انترنيت من كلمة Internetwork ، وهذا يعني وبشكل ترجمته بأنه الوصل الداخلي للشبكات ، وبالفرنسية Inter Connexion de Réseaux .
وبالتالي فإن الانترنيت هي عبارة عن شبكة الشبكات كما هو موضح بالشكل :

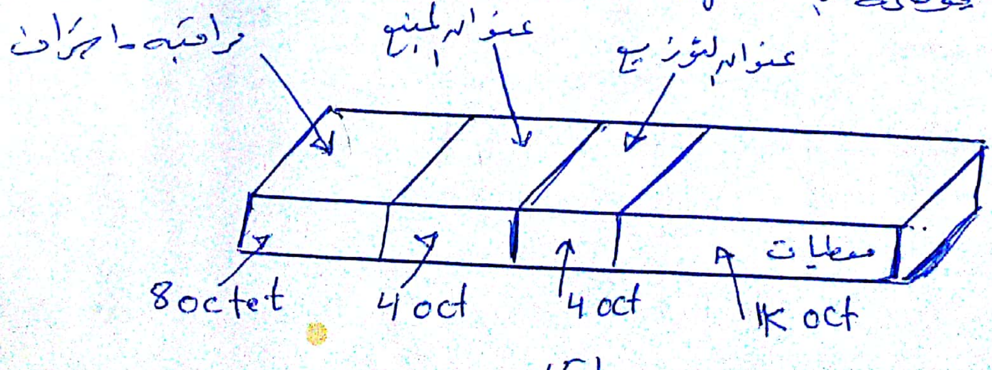


شكل : بنية لشبكة الانترنيت

في بداية السبعينات فإن العديد من الشبكات التي بدأت بالظهور كانت لها بنية حزم مختلفة ، وهذا ما جعل الوصل الداخلي معقد ؛
إن فكرة الانترنيت هي الطلب من شبكاتها بإدخال الحزم حزمة ذات بنية واحدة متماثلة ، وهي تسمى بالحزمة المشتركة .

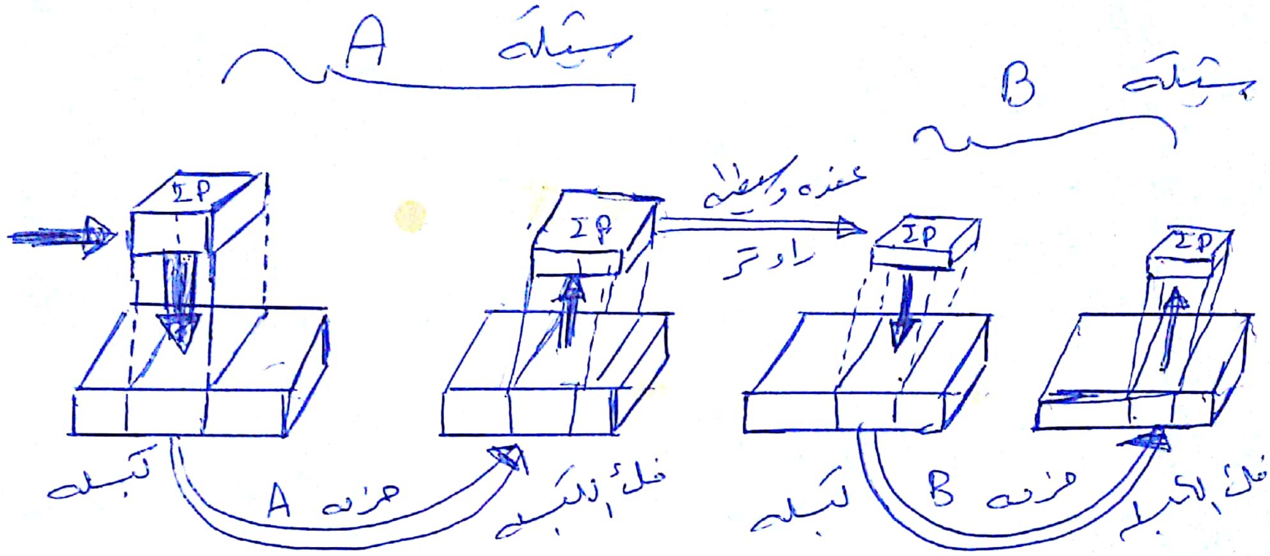
* الحزمة IP

إذ أن كل حزمة من كل شبكة تنقل وتحمل الحزمة المشتركة IP Internet Protocol
بنية هذه الحزمة موضحة بالشكل :



شكل : بنية IP

إن ادخال الحزمه المشتركه وانتقالها من شبكه لأخرى تسمى بالكبسله وفك الكبسله كما هو موضح بالشكل التالي :



حيث أن عمليه الكبسله تشتمل على ادخال حزمه IP ضمن بلوك ذو بنيه نوعيه بشكل شبكة Ethernet ، ....

هذا النظام يلائم شكل TCP مع تطبيقات المعلوماتيه ، ولكن النوعيه الجوده الضروريه لتوجيه وارسال الحديث الهاتفي أو الفيديو غالباً مشكله .

من أسباب ذلك هو عمليه معالجة ال IP في عقد النقل ((الحزمات التي تصل أولاً تعالج أولاً)) وبالتالي إذا أتت لدينا حزمة صغيره مستعجله ولكنها تتواجد خلف حزمه كبيره وغير مستعجله ، وبالتالي الحزمه الصغيره مضطره للانتظار .

وبالاضافه لذلك بأن الانترنت هي عباره عن شبكة الشبكات ، وبالتالي فإنها لا تملك مدير أو مرشد عام يمتلك نظرة الكوليه ولا تملك ولا أي وسيله معرفه كامله عن الشبكه قادر على اداره الشبكه من طرف نهايه الى نهايه كما تحتاج لعدد المستخدمين .

هنالك حلول من أجل تصميم شبكة انترنت متحكم بها ، ومن هذه الحلول والتي تعتمد على استخدام بروتوكول IP ضمن وسطها هي مثل شبكة Intranet في الاجيال الحديثه ل IP فإنه يتم ادخال التحكم بالشبكه وهذا ما يسمح بدعم نوعيه الخدمه

« مفاهيم أساسية لأمن الشبكات »

نظرة عامة :

يبدو أنه كل يومين تطالعنا الصحف بأخبار عن شبكة الاتصالات « حواسيب الاتصالات الهاتفية ... » تعرضت للخطر من قبل قراصنة ،

في الواقع منذ وقت ليس ببعيد وقعت وزارة الدفاع الامريكية ضحية لهجوم قراصنة ناجح ، تمكن من خلاله القراصنة على اختراق شبكة حواسيب الوزارة لمدة اسبوعين كاملين قبل اكتشافهم ، ولحسن الحظ كانت الاجهزة تحتوي فقط على معلومات غير سرية « معلومات تتعلق بالموظفين والرواتب » وبناءاً عليه لم يتعرض الأمن القومي للتهديد . وأمثلة كثيرة أخرى لعمليات اختراق في أماكن تختلف من العالم :

- في الآونة الأخيرة تم استهداف موقع ياهو « Yahoo » وأمازون دوت كوم « Amazon.com » وإي باي « Ebay » ، وبعض المواقع المشهورة الأخرى في شبكة الشبكات العالمية لما يبدو أنه هجوم منسق يعرف بـ « الحرمان من الخدمة » حيث تعرضت هذه المواقع خلال فترة ثلاثة أو أربعة أيام لزحمة من قصف الكتروني كاذب من عدة مواقع الكترونية ، توقفت على أثره هذه المواقع لساعات ولمرات متكررة .

هذه الهجمات توضح مدى خطورة تهديد القراصنة الخارجي على الشركات والهيئات .

- في نفس الوقت ، كل منشأة تستخدم أجهزة حاسوب تواجه التعرض من أفراد داخل المنشأة « الموظفين الحاليين والموظفين السابقين » ذوي النوايا السيئة الذين يرغبون في الحصول على معلومات مثل رواتب الموظفين أو الاطلاع على ملفات الموظفين الآخرين ، هؤلاء هم أيضاً يمثلون تهديداً لشبكة اتصالات المنشأة وحواسيبها حيث أنه مثلاً :

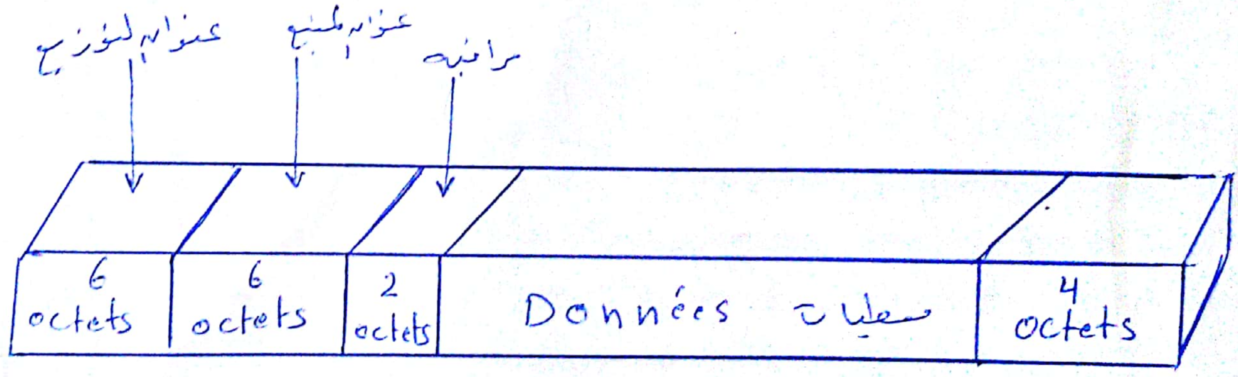
- في الآونة الأخيرة تدور في عالم الحواسيب والشبكات قصة موظف يعمل كمبرمج لدى إحدى الشركات شن هجوم الحرمان من الخدمة ضد شركته التي تقدم خدمات تداول الاسهم عبر شبكة الانترنت ، على ما يبدو أن هذا الموظف الذي يعمل كمبرمج كان في مفاوضات مع ادارة شركته لزيادة راتبه ،

* شبكة ATM

إن تقنية النقل Asynchronous Transfer Mode: ATM وضعت بالسنوات الأخيرة كهدف تشبيه نوعي لخدمة. وهي عبارة عن تقنية لنقل الحزم الصغيرة بطول ثابت تسمى خلية.
إذاً إن أول خاصية أساسية لهذه التقنية هو أن الخلية ذات طول ثابت 53 octets، وهذا ما يسمح لمعالج سريع داخل العقدة.

* شبكة Ethernet

إن شبكات Ethernet تقدم هيكلية مختلفة، وبشكل خاص أنها تحدد أو تعرف مسبقاً شكل أطر للرزمة، التي ستكون معروضة من قبل وسيط الشبكات المحلية LAN، ولكن هذا غير ملائم للشبكات الممتدة.
إن شكل حزمة Ethernet مبينة بالشكل التالي



شكل حزمة Ethernet

حيث أن العناوين الدائمة لل Ethernet تكون مجزأة لحقلين 3octets لكل واحد:
- الأول يدل على رقم المنشئ، والثاني يدل على رقم التسلسل أو السلسلة.
إن استخدام هذا النوع من الشبكات يكون ملائماً فقط في المجال المحلي وذلك بسبب أنه يجب تحديد مكان أو موضع الـ PC المستخدم من قبل الشبكة
ولاستخدام هذه الشبكة في الشبكات الممتدة فإنه يجب:
1- إما إيجاد طريقة تفسير أخرى للعناوين 6octets
2- أو إضافة عنوان إضافي

Scanned by CamScanner

لقد أصبح هذا المبرمج من طلائع المفاوضات مقتدراً أن يثبت للشركة إمكانية تعرضها لخطر القرصنة، فقام بشن هجوم على أنظمتها عبر شبكة الانترنت، وبما أنه كان على دراية دقيقة بأنظمة وبرمجيات الشركة، مكنته تلك المعرفة الداخلية للشركة من ضربها بطريقة أدت إلى إغلاقها.

في الحقيقة أدى الهجوم إلى تعطيل خدمات تداول الأسهم في الشركة لمدة ثلاثة أيام، في النهاية تمت الاستعانة بجهاز الخدمة السرية الأمريكي، وتم تتبع الهجوم الذي قادهم إلى هذا الموظف (المبرمج) وتم القاء القبض عليه.

لذلك على كل مؤسسة مراقبة أنظمتها ضد الاقتحام عن طريق الأشخاص غير المصرح لهم وغيرهم من الجهات، وهذا النشاط يجب أن يكون جزءاً من الروتين اليومي لوحدة تكنولوجيا المعلومات في كل وحدة، حيث أنه ضروري لحماية أصول الشركة من المعلومات.

الطريقة الأكثر وثوقاً لضمان سلامة أجهزة الحواسيب وغيرها للمنشأة هي عدم وضعها على الشبكة والاحتفاظ بها وراء أبواب مغلقة، لسوء الحظ هذا ليس حلاً عملياً، حيث أن اليوم تصبح أجهزة الحواسيب أكثر فائدة إذا تم ربطها مع بعض في شبكة ليتم تبادل المعلومات وتقاسم الموارد.

وعلى الشركات التي تضع أجهزتها الخاصة بها في شبكة أن تتخذ بعض الاحتياطات البسيطة للحد من مخاطر الوصول غير المصرح به.

كل عام الشركات والحكومات والمنظمات الأخرى تصرف مليارات الدولارات كنفقات متعلقة بأمن الشبكات، كما أن معدل نفقات هذه الجهات يبدو في زيادة مستمرة. ومع ذلك، عندما تبحث الشركات لإيجاد المجالات التي يمكن من خلالها خفض الانفاق من بنود الميزانية، أثبت تاريخياً أنها تلجأ للخفض أولاً من موازنات التخطيط وأمن الشبكات والمعلومات.

* لماذا يعتبر أمن الشبكات مهماً ؟؟

إن الشبكات بشكل عام و شبكة الانترنت بشكل خاص سلاح ذو حدين، فهو مدخل للكثير من الاشياء النافعة، ولكن مع الأسف فهو يفتح المجال أمام الكثير من الاشياء المؤذية للدخول إلى حياتنا، وثمة العديد من المسائل الأمنية الواجب الاعتناء بها للابقاء على سلامة تشغيل أجهزة الكمبيوتر والشبكات «وهنا يجب البحث عن أهم القضايا الأمنية وبعض الحلول لها».

ربما يبدو للبعض سخيفاً أن نطرح هذا السؤال «لماذا يعتبر أمن الشبكات مهماً؟» إنه لمن المهم بالنسبة للمنشآت تقدير لماذا يريدون تحقيق أمن الشبكات بشكل عام والحواسيب بشكل خاص، وتحديد الكيفية التي سيتم بها تحقيق ذلك، بل هو أيضاً أداة مفيدة للاستخدام عند السعي للحصول على إذن الادارة التنفيذية لتأمين النفقات المتعلقة بالأمن.

يعتبر أمن الشبكات والحواسيب مهم للأسباب التالية:

1- حماية أصول الشركة «شبكات وحواسيب» واحد من الأهداف الأساسية لأمن الشبكات والحواسيب هو حماية أصول الشركة.

وبالمناسبة هنا لا نعني بكلمة الأصول الأجهزة والبرامج التي تشكل الحواسيب والشبكات. الأصول: هي المعلومات التي يتم حفظها في أجهزة الحواسيب للشركة وشبكاتها.

من ذلك عليك أن تطرح السؤال التالي: ما هو أمن المعلومات؟

يعني أمن المعلومات إبقاء معلوماتك تحت سيطرتك المباشرة والكاملة، أي بمعنى عدم إمكانية الوصول إليها من قبل أي شخص آخر دون إذن منك، وأن تكون على علم بالمخاطر المترتبة عن السماح لشخص ما بالوصول إلى معلوماتك الخاصة.

أنت بأننا أكيد لا ترغب أن يكون للآخرين مدخلاً لمعلوماتك الخاصة، ومن الواضح أن معظم الأشخاص يرغبون في الحفاظ على خصوصية معلوماتهم الحساسة مثل: كلمات المرور - معلومات البطاقة الائتمانية وعدم تمكين الآخرين من الوصول إليها، والكثير من الأشخاص لا يدركون بأن بعض المعلومات التي قد تبدو تافهة أو لا معنى لها بالنسبة لهم قد تعني الكثير لأناس آخرين، وخصوصاً إذا ما تم تجميعها مع أجزاء أخرى من المعلومات. فعلى سبيل المثال لا الحصر: يمكن للشركة الراغبة في الحصول على معلومات شخصية عنك للأغراض التسويقية أن تشتري هذه المعلومات من شخص يقوم بتجميعها من خلال الوصول إلى جهاز كمبيوترك بشكل غير شرعي. ومن المهم كذلك أن تفهم أنك حتى ولو لم تقم بإعطاء معلوماتك لأي شخص عبر الانترنيت، فقد يتمكن بعض الأشخاص من الوصول إلى نظام كمبيوترك للحصول على المعلومات التي يحتاجونها دون علم أو إذن منك.

لذلك وبالعودة لما سبق، تعتبر المعلومات أصول حيوية للشركات وهي ما يهتم به أمن الشبكات والحواسيب، ويوفر كل هذا حماية وسلامة وتوافر المعلومات في الوقت المناسب.

ومن هنا يمكن تعريف المعلومات: بأنها البيانات التي يتم تنظيمها والوصول إليها بطريقة منسقة وذات معنى.

ب- للحصول على ميزة تنافسية: تطبيق وتطوير سياسات أمن معلومات فعّال يعطي المنشأة ميزة تنافسية على المنشآت المنافسة لها.

إن لأمن الشبكات أهمية خاصة في ساحة خدمات الانترنيت العالمية والتجارة الالكترونية. ويمكن أن تعني الفرق بين الخدمة واسعة القبول واستجابة العملاء دون المتوسط على سبيل المثال: كم من الناس تتوقع أن يستخدم نظام الخدمات المصرفية عبر الانترنيت لبنك ما لو يعلمون أن النظام اخترق بنجاح في الماضي؟

بالتأكيد سيكون العدد قليل جداً ، بل سوف يذهبون إلى استخدام الخدمات المصرفية عبر الانترنت لمؤسسات مالية أخرى منافسة.

4- للتوافق مع المتطلبات التنظيمية والمسؤوليات الائتمانية:

الموظفون المسئولون في كل شركة تقع عليهم مسؤولية ضمان سلامة وصحة المنشأة، جزء من هذه المسؤولية تشمل ضمان ديمومة عمل المنشأة، وبناءاً عليه فإن المنشآت التي تعتمد على أجهزة الحاسوب في استمرار عملها يجب أن تضع سياسات وإجراءات معالجة تهتم بمتطلبات أمن المعلومات.

- هذه السياسات والإجراءات ليست ضرورية فقط لحماية أصول الشركة ولكن أيضاً لحماية المنشأة من المسؤولية.
- للتحقق المرجح أيضاً يجب على المنشآت حماية استثمارات المساهمين وتعظيم العائد، بالإضافة إلى ذلك إن العديد من المنشآت تخضع للتنظيم الحكومي، والذي غالباً ما يفرض على متطلبات السلامة والأمن للمنشأة، مثلاً: معظم الشركات المالية تخضع للتنظيم الاتحادي، وعدم الامتثال للمبادئ التوجيهية الاتحادية يؤدي إلى مصادرة المؤسسة المالية من قبل الجهة التنظيمية الاتحادية.

في بعض الحالات، موظفوا الشركات الذين لم ينجزوا مهامهم التنظيمية والائتمانية يخضعون للمساءلة الشخصية من قبل المؤسسات المالية التي يعملون بها عن أي خسائر تتكبدها الشركة.

5- للحفاظ على وظيفتك: وأخيراً لتأمين موقف الفرد الوظيفي داخل المنشأة ولضمان آفاق المستقبل الوظيفي، ومن المهم أن يضع الشخص نفسه في مكان يهتم بوضع تدابير تحمي الأصول التنظيمية. ينبغي أن يكون الأمن جزء من كل شبكة ورشبكة اتصالات - حاسوب ... أو تصميم مدير الأنظمة. عدم أداء المهام الوظيفية بشكل كافي يؤدي إلى إنهاء الخدمة

لا ينبغي أن يكون الهاجس الذي ينتج تلقائيا لفشل في نظام أمن المعلومات، ولكن إذا ثبت بعد التحري الدقيق بعد وقوعه، وتم تحديد أنه الفشل قام نتيجة لعدم وجود سياسات وإجراءات مناسبة أو عدم الامتثال للإجراءات القائمة، فإنه يتحتم على الإدارة التدخل واجراء بعض التغييرات.

هـ- هناك شيء واحد يجب وضعه في الاعتبار هو أن أمن الشبكات يكلف مال:

إنه يكلف مال للتوظيف ويكلف مال لتدريب الموظفين، وابقائهم في المنشأة، يكلف مال لشراء الأجهزة والبرمجيات لتأمين شبكات المنشأة،

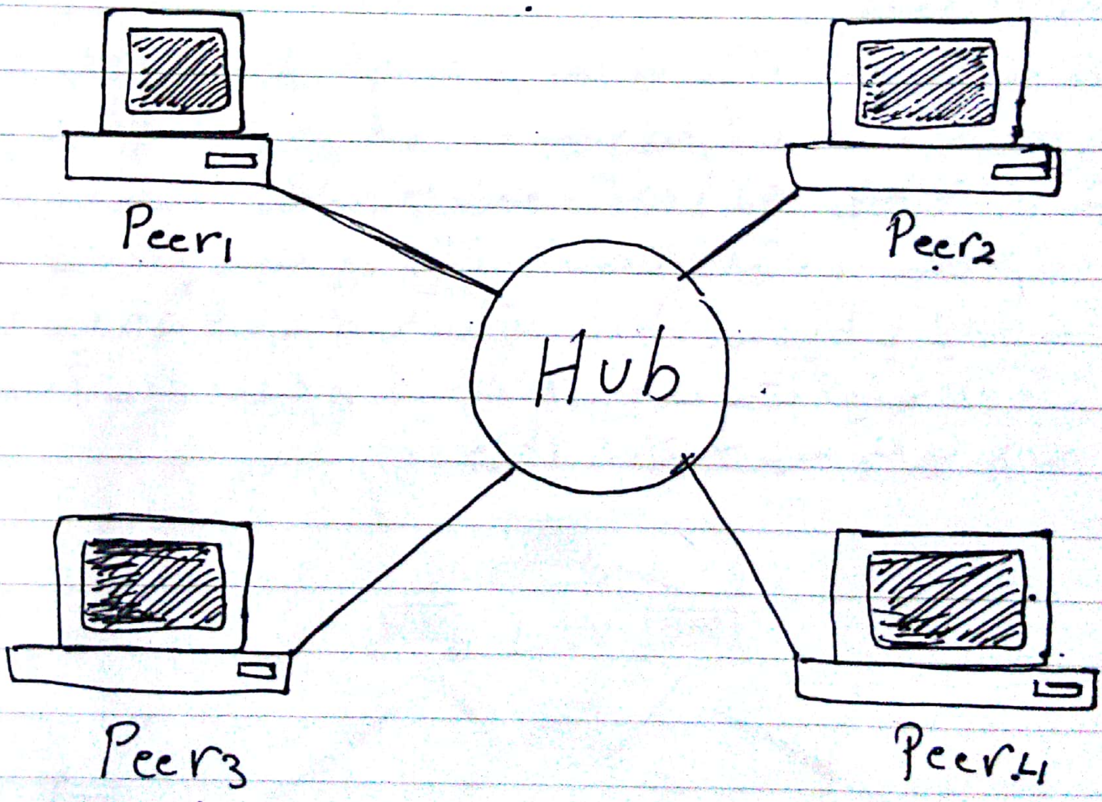
[redacted]

ونتيجة لكل ذلك فإن أمن الشبكات ليس رخيصًا، ومع ذلك فإنه أرخص من التكاليف الناتجة عن اختراق شبكة المؤسسة.

* أساسيات أمن الشبكات

الحاجة إلى أمن الشبكات متطلب جديد نسبياً، قبل ثمانينيات القرن الماضي أكثر الحواسيب لم تكن مرتبطة بشبكة. ولم يكن ذلك بسبب عدم وجود رغبة لربط الأجهزة بل كان نتيجة لعدم وجود التقنية.
وكانت معظم الأنظمة كبيرة أو أنظمة متوسطة يتحكم بها وتدار مركزياً.
يتواصل المستخدمون مع أجهزة الحاسوب المركزية من خلال شاشات فرعية، وكانت تلك الشاشات ذات قدرات محدودة، تتطلب الشاشة اتصال فعلي على منفذ مخصص، وفي كثير من الأحيان تستخدم منفذ أو منافذ الاتصالات التسلسلية التي تستخدم بروتوكولات خاصة مثل RS-232، وعادة ما يتطلب منفذ واحد لكل شاشة واحدة.
شركة IBM للمنتجات الرقمية وبعض الشركات الأخرى المصنعة للحواسيب طورت بعض الاختلافات على هذه التصميمات لأمن الشبكات. وذلك من خلال استخدام مخدمات الشبكات الطرفية، ولكن المفهوم الأساسي كان هو نفسه.
لم يكن هناك شيء ما يعادله ما لدينا اليوم من تكنولوجيا، حيث مئات أو الآلاف من الاتصالات عليك أن تتصل بالنظام من خلال حلقة أو دائرة شبكة الكترونية واحدة.
بعد الثمانينيات من القرن الماضي، إبان بزوغ تطوير أجهزة الحاسوب الشخصية (PC) ووضع معايير قياسية لبروتوكول الشبكات وانخفاض تكلفة عتاد الأجهزة وتطوير تطبيقات برمجية جديدة جعل الشبكات عامة ومستخدمة أكثر بكثير من السابق.
ونتيجة لذلك شهدت الشبكات المحلية LAN والشبكات الواسعة WAN والحواسيب الموزعة نمواً هائلاً خلال تلك الفترة.
- عند بداية تطور الشبكات المحلية LAN كانت آمنة نسبياً، آمنة لأنها كانت أساساً معزولة، ولم تكن مرتبطة بالشبكات الواسعة النطاق WAN، لذلك طبيعتها المستقلة أدت إلى الحفاظ على موارد الشبكة.

في الواقع الشبكات الواسعة النطاق WAN سبقت الشبكات المحلية LAN وكانت متواجدة منذ فترة، لكنها عادة كان يتم التحكم فيها مركزياً، وعليه الوصول إليها من قبل عدد قليل من الأفراد في معظم المنشآت.
إن شبكات WAN الدوائر المستأجرة أو المملوكة الخاصة أو المؤجرة كانت آمنة نسبياً لأن الوصول إلى الدوائر محدود النطاق. وللتوصيل موقعين عادة يتطلب دائرة توصيل من نوع نقطة-نقطة. والشكل التالي يوضح شبكات النطاق الواسع WAN من نوع نقطة-نقطة:



شكل: شبكات WAN نوع نقطة-نقطة

وبالتالي اذا أردنا ربط موقع ثالث للموقعين السابقين، فإن ذلك تتطلب دائرتين إضافيتين أي يصبح الاتصال كالتالي:
A - B , A - C , B - C

Sheabli

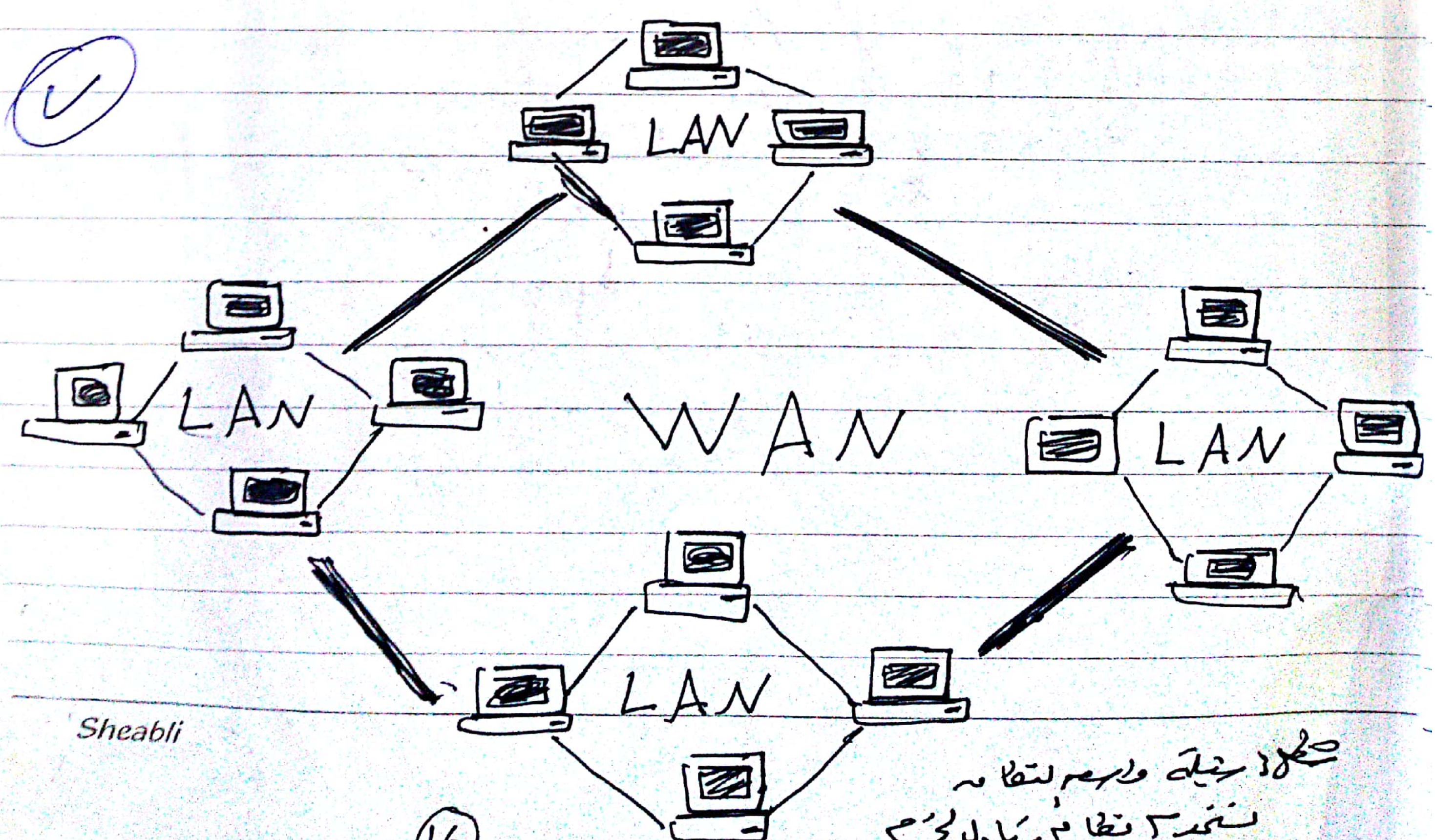
إن تطوير بروتوكولات حزم البيانات مثل X.25 وبروتوكول التحكم بالإرسال/بروتوكول الانترنت TCP/IP أدى إلى تخفيض تكلفة تركيب الشبكات واسعة النطاق. وهذا ما جعلها أكثر جاذبية للمستخدمين.

هذه البروتوكولات سمحت للعديد من الأنظمة المشاركة في استخدام الدوائر (الوصلات).

عدد كبير من الأشخاص أو المنشآت يمكنهم الآن الاتصال عن طريق الشبكة المشتركة، وبناءً عليه لم يعد من الضروري استخدام نظام ربط الأنظمة نوع نقطة إلى نقطة.

عندما بدأت نقاط الضعف تظهر مع تطوير هذه البيئة من الأجهزة الموزعة، التي تستخدم نظم مشاركة الحواسيب، واستخدام نظام الحزم المعتمدة على بروتوكولات مثل TCP/IP ومفهوم النظم الموثوقة بشكل عام إن الأنظمة في شبكة الاتصال تثق في بعضها البعض، ولكن قد يصبح الموقف سيئاً في كثير من الأحيان نتيجة لربط شبكات محلية LAN آمنة نسبياً إلى شبكات واسعة النطاق WAN غير آمنة.

والشكل التالي يوضح مفهوم تبادل الحزم.



شبكة واسعة النطاق
تستخدم نظام تبادل الحزم

Sheabli

في بيئة التوزيع هذه يكون التركيز على توفير سهولة الوصول والربط بين الشبكات.

بأن أمن الشبكة كان يعامل كأمر ثانوي، هذا إذا وضع بالحسبان من الأساس. ونتيجة لذلك فإن العديد من الأنظمة تكون مفتوحة ومعرضة بشكل كبير للتهديدات لم تكن موجودة في السابق.

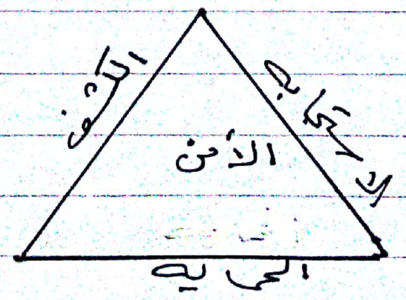
- الانترنيت هي النظام الأكثر شهرة في استخدام هذا النوع من الشبكات. تستخدم شبكة الانترنيت بروتوكول TCP/IP الذي يهدف في المقام الأول لربط اجهزة الحاسوب بطريقة سهلة وفعالة وذلك بغض النظر عن نظم التشغيل الخاصة بها.

الأمن لم يكن في ذلك الوقت جزءاً من التصميم المبكر للبروتوكول TCP/IP، وهذا كان سبباً للعديد من الهجمات على نظام دوائر التي تم فيها استغلال نقاط الضعف الموجودة في تصميم البروتوكول. وكان أحد الاحداث المعروفة «دودة الانترنيت» التي تسببت في جثو الانترنيت على ركبتيه وذلك في عام 1986.

واليوم يعتبر الأمن أكثر أهمية من سهولة الوصول.

* مثلث الأمن

إن أضلاع مثلث الأمن هي الوقاية والكشف والرد على ذلك تمثل أساس أمن الشبكات. وينبغي أن يكون مثلث الأمن الأساس لجميع السياسات الأمنية والتدابير التي تطورها المنشأة وتقوم بتطبيقها.



شكل: مثلث الأمن

Sheabli

- الحماية: إن أساس وقاعدة مثلث الأمن هو الوقاية. لتوفير مستوى مقبول من الأمن بأنه من الضروري اتخاذ تدابير لمنع استغلال نقاط الضعف، وذلك بعمل خطط أمن الشبكات.
ينبغي على المنشآت التركيز على التدابير الوقائية أكثر من الكشف والاستجابة.
إنه أسهل وأكثر كفاءة وأقل تكلفة لمنع حدوث أمني من الاكتشاف أو الرد. تذكر أنه من المستحيل وضع خطط أمنية من شأنها أن تمنع جميع نقاط الضعف من الاستغلال، لكنه ينبغي للشركات أن تتخذ تدابير أمن وقائية قوية تكفي لتثبيط المجرمين المحتملين. وهذا ما يجعلهم يتجهون إلى أهداف أقل سهولة.

- الكشف: هذا ما تم إعداد التدابير الوقائية، بأنه يجب وضع الإجراءات لتمكين التنفيذ هادئاً وذلك من أجل الكشف عن الشاكل المحتملة أو الخروقات الأمنية.
في حال مثلث التدابير الوقائية، بأنه من المهم جداً أن يتم الكشف عن الشاكل على الفور. كلما تم الكشف عن مشكلة بسرعة فإنه من السهل التصحيح والإصلاح.

- الاستجابة: تتابع المنشآت خطط تحدد الرد المناسب على الاختراقات الأمنية وينبغي أن تكون الخطط مكتوبة وتحديد الشخص المسؤول عن كل الإجراءات مع تحديد مستويات التصعيد المختلفة.

قبل البدء في مناقشة هذه عن أمن الشبكات وأمن الحواسيب، نحن بحاجة لتحديد ما تنطوي عليه الخطط أولاً: حيث أن أمن الشبكات غالباً ليس مشكلة تقنية بل هو مشكلة تكون متعلقة بالعمل. والتقنية هي الجزء السهل من الأمر. أما الجزء الصعب منه وضع خطط أمنية تناسب مع حجم المنشأة العملية وعمل الموظفين عن الالتزام بالخطط.

وبعد ذلك يتقسم على الشركات الإجابة على بعض الأسئلة الأساسية أيضاً في ذلك ما يلي:

م - كيف يمكن تعريف أمن الشبكات؟

ب - كيف تعرف المستوى الأمني المناسب؟

للإجابة عن هذه الأسئلة، فإنه من الضروري تحديد ما تريد أن تحاول حمايته.

* أمن المعلومات

قبل كل شيء، فإنه كما رأينا سابقاً فإن أمن الشبكات يهتم بأمن أصول الشركة من المعلومات. كثيراً ما نغفل عن حقيقة أن المعلومات وقدرتنا على الوصول إليها هو ما نحاول حمايته، وليس أجهزة الحاسوب والشبكات.

يمكن أن نعرف أمن المعلومات بالشكل البسيط التالي:

أمن المعلومات = السرية + الصحة + توفر المعلومة + عمليات الوصول إليها

لذا لا يمكن أن يكون هناك أمن معلومات بدون سرية، وهذا يعني أن المستخدمين الغير مصرح لهم لا يمكنهم اعتراض المعلومات أو نسخها، أو تكرارها.

ثم نفس الشيء فإن التكامل ضروري بحيث يكون للمنشأة ما يكفي من الثقة في دقة المعلومات للعمل عليها.

علاوة على ذلك يتطلب أمن المعلومات أن تكون المنشأة قادرة على استرجاع البيانات، تعتبر تدابير أمن المعلومات لا قيمة لها إذا لم تتمكن المنشأة من الوصول إلى المعلومات الحيوية التي تحتاجها للعمل في الوقت المناسب.

وأخيراً تعتبر المعلومات غير آمنة بدون وجود صلاحيات تحدد المستخدم النهائي الذي يسمح له بالوصول إليها.

من بين العديد من عناصر أمن المعلومات، يجب التأكد من الأمن المادي للأجهزة وتوظيف الأشخاص المؤهلين وتطوير السياسات والإجراءات والالتزام بها، وتعزيز ومراقبة الشبكات والأنظمة. وتطوير تطبيقات برمجية آمنة.

من المهم أن نتذكر أن أمن المعلومات ليس فقط حماية الأصول من المتسللين الخارجيين. في معظم الأحيان تأتي التهديدات من داخل المنشأة ((لقد وجدنا العدو، إنه نحن))

أمن المعلومات أيضاً يختص بالإجراءات والسياسات التي تحمي المعلومات من الحوادث، وعدم الكفاءة، والكوارث الطبيعية. هذه السياسات والإجراءات يجب أن تعالج ما يلي:

- النسخ الاحتياطي وجميع الضوابط ((تكوين - وسائط))
- التعافي من الكوارث وتخطيط الطوارئ.
- سلامة البيانات

من المهم أيضاً أن نتذكر أن أمن الشبكات ليس مطلقاً. الأمن نسبي، لا يجب التفكير في أمن الشبكات كطيف ينطلق من: غير آمن جداً ← آمن جداً.

مستوى الأمن للنظام أو الشبكة يعتمد على موقعه على طول هذا الطيف بالنسبة للأنظمة الأخرى. فهو إما أكثر أمناً أو أقل أمناً من الأنظمة الأخرى بالنسبة إلى التالي المنقطع. وليس هناك شيء اسمه شبكة آمنة تماماً ونظام آمن تماماً.

موازنات أمن الشبكة

أمن الشبكة هو الفعل المتوازن الذي يتطلب نشر ((الدفاعات المناسبة)) يجب أن تكون الدفاعات التي يتم نشرها أو تنفيذها متناسبة مع التهديد. تحديد المنشآت ما هو مناسب بعدة طرق:

كتحقيق التوازن تكلفة الأمن مقابل قيمة الأصول التي تحمون
موازنة المحتمل مقابل الممكن ((موازنة للتهديدات الأكثر وقوعاً))
موازنة احتياجات الأعمال مقابل الاحتياجات الأمنية.

Sheabli

يجب على المنشآت تحديد مقدار التكلفة التي سوف تترتب على اختراق كل النظام أو الشبكة، أو بعبارة أخرى، كم سيكلف بالعملة الصعبة فقدان المعلومات أو الوصول إلى النظام أو سرقة المعلومات. عن طريق ميزانية فيها تقدير للتكلفة التي سوف تترتب على اختراق النظام أو الشبكة.

عليه للمنشآت تحديد الحد الأعظمي «الأعلى» الذي هو على استعداد للدفع لحماية أنظمتهم. بالنسبة للعديد من المنشآت هذه العملية ضرورية لأن الأنظمة هي شريان الحياة بالنسبة للمنشأة، وبدونها لا وجود للشركة.

تحتاج المنشآت إلى تحقيق التوازن بين تكلفة الأمن مقابل تكلفة التهديدات الأمنية.

عموماً، حيث أن الاستثمار في الأمن في زيادة، فإنه ينبغي أن تتطابق الخسائر المتوقعة، كما يجب على الشركات ألا تستثمر في الأمن أكثر من قيمة الأصول التي يراد حمايتها، وهنا عليها استخدام تحليل فوائد التكاليف المالية.

علاوة على ذلك، يجب على المنشآت أن توازن التهديدات المتوقعة مقابل التهديدات المحتملة. إذ أنه من المستحيل الدفاع ضد كل نوع ممكن من الهجوم. من الضروري تحديد ما هي أنواع التهديدات أو الاعتداءات التي لديها احتمال حدوث أكبر ومن ثم تحمي المنشأة ضدها.

على سبيل المثال، من الممكن أن تخضع المنشأة لنوع من أنواع المراقبة مثل VAN ECK أو التعرض للهجوم عن طريق تردد الراديو عالي الطاقة HERF، لكن الاحتمال ضعيف.

من المهم أيضاً تحقيق التوازن بين احتياجات العمل والحاجة إلى الأمن، وتقييم تأثير التشغيل لتنفيذ التدابير الأمنية. التدابير والإجراءات الأمنية التي تتعارض مع عملية المنشأة تعتبر عديمة الفائدة.

هذه الأنواع من التدابير عادة ما يتم تجاهلها أو الالتفاف حولها من قبل موظفي الشركة. لذلك يعملون إلا خلق الثغرات الأمنية بدلاً من إغلاقها. بقدر الإمكان، ينبغي أن تكمل التدابير الأمنية للاحتياجات التشغيلية والتجارية للمنشأة.

حظ مراقبة VAN ECK: هو رصد لشاشة جهاز حاسوب أو غيره من المعدات الإلكترونية عن طريق الكشف عن مستويات منخفضة من الانبعاثات الكهرومغناطيسية عن بعد.

سلاح تردد راديو عالي الطاقة HERF: هو جهاز يمكنه أن يعطل التشغيل العادي للمعدات الرقمية مثل أجهزة الحاسوب والمعدات الملاحية من خلال توجيه انبعاثات تردد راديوية عالية الطاقة HERF عليه.

تقييم المخاطر:

فكرة تقييم المخاطر أمر بالغ الأهمية لتطوير الدفاعات المناسبة. لإجراء تحليل المخاطر، تحتاج المنشآت لفهم التهديدات ونقاط الضعف المحتملة.
الخطر: هو احتمال أن يتم استغلال نقطة ضعف، فيما يلي قائمة بالخطوات الأساسية لتقييم المخاطر:

١- تحديد وترتيب أولويات الأصول
٢- تحديد نقاط الضعف
٣- تحديد التهديدات واحتمالات وقوعها
٤- تحديد التدابير المضادة
٥- عمل تحليل التكاليف والعوائد
٦- تطوير السياسات والإجراءات الأمنية.

لتحديد وترتيب أولويات أصول المعلومات ووضع تحليل التكاليف والعوائد، من المفيد طرح بعض الأسئلة البسيطة مثل التالية:
أ- ما هو الشيء الذي تريد حمايته
ب- لماذا تريد حمايته
ج- ما هي قيمته
د- ما هي التهديدات
هـ- ما هي المخاطر
و- ما هي الآثار المترتبة عند حدوثه
ز- ما هي السيناريوهات المحتملة
ح- كم ستكلف خسارة المعلومات أو البيانات؟

Sheabli

إن تحديد أولويات الأصول والنظم يكون عن طريق تقييم قيمتها بالنسبة لها. المقاييس لتقدير قيمة الأصول يمكن أن تكون: <u>تكلفة الاستبدال</u>، <u>تكلفة فقدان الأصول</u> أو <u>تكلفة تسرب الأصل</u> مثل المعلومات السرية التي حصل عليها منافس.

من الضروري أيضاً تضمين تكاليف غير مرئية "أكثر غموضاً" مثل فقدان <u>ثقة العملاء</u>.

نماذج الأمن

هناك ثلاثة أساليب أساسية مستخدمة لتطوير أمن الشبكة. وعادة ما تستخدم الشركات مزيج من الأساليب الثلاثة لتحقيق الأمن وهي:

- الأمن من خلال الغموض
- نموذج الدفاع المحيط
- نموذج الدفاع العميق

● الأمن عن طريق الغموض

الأمن عن طريق الغموض يعتمد على التخفي للحماية. المفهوم الكامن وراء هذا النموذج هو أنه إذا كان لا أحد يعرف وجود شبكة أو نظام ما، فإنه لن تكون عرضة للهجوم. وبالتالي الشيء الأساسي هو أن تخبأ الشبكة أو على الأقل لا يتم الإعلان عن وجودها فإن ذلك يؤدي الغرض كنظام أمن.

المشكلة في هذا الأسلوب هو أنه لن يعمل على المدى الطويل، حالما يتم اكتشاف الشبكة، سوف تكون الشبكة معرضة للخطر تماماً.

● دفاع المحيط

نموذج دفاع المحيط مشابه لقلعة بها خندق. عند استخدام هذا النموذج من أمن الشبكات فإن الشركات تقوي أو تعزز محيط الأنظمة والأجهزة بنوعية محدودة، أو تخفي الشركة شبكتها خلف جدار حماية نارية لتعزل شبكتها الآمنة عن الشبكات الغير موثوق بها. هذا النموذج لا يفعل الكثير لتأمين الأنظمة الأخرى في الشبكة، الافتراض هنا هو أن أسلوب دفاع المحيط كافي لوقف أي دخلاء من الخارج وبناءً عليه تكون الأنظمة الداخلية آمنة.

هناك العديد من العيوب في هذا المفهوم : أولاً هذا النموذج لا يفعل شيئاً لحماية الأنظمة الداخلية من الهجوم من الداخل. كما ناقشنا سابقاً، فإن غالبية الهجمات على شبكة الشركة يتم شنها من شخص داخل المنشأة.

ثانياً : تقريباً دائماً ما يفشل دفاع المحيط في نهاية المطاف، وعندما يحدث ذلك فإن الأنظمة الداخلية تكون مفتوحة على مصراعيها للهجوم.

⑤ - الدفاع في العمق

الأسلوب الأكثر قوة يمكن استخدامه هو نموذج الدفاع في العمق. أسلوب الدفاع في العمق يتألف من أجل الأمن من خلال تقوية ومراقبة كل نظام على حدة.

كل نظام هو جزيرة تدافع عن نفسها. كما أن هناك تدابير إضافية تتخذ على أسلوب دفاع المحيط، ولكن أمن الشبكة الداخلية لا يبقى مستقلاً عن أنظمة الدفاع في المحيط. هذا الأسلوب أكثر صعوبة في التحقيق ويتطلب من جميع النظم ومسؤولي الشبكة القيام بدورهم في العملية.

مع ذلك في ظل هذا النموذج من غير المرجح أن يتم المساس بالشبكة الداخلية في حال أن أحد مسؤولي النظام ارتكب خطأ، على سبيل المثال وضع جهاز مودم غير آمن في النظام، عند استخدام الدفاع في العمق فإن النظام الذي تم تركيب المودم فيه قد يكون عرضة للاختراق بينما تكون الأنظمة الأخرى في الشبكة قادرة على الدفاع عن نفسها. كما ينبغي على الأنظمة الأخرى أن تكون قادرة على الكشف عن أي محاولة اختراق من أي نظام مخترق في الشبكة. أيضاً هذا الأسلوب يوفر حماية أكثر ضد العمليات الداخلية.

ملاحظة : إن الأنظمة المخترقة الداخلية تكون سهلة الكشف نسبياً.

// المصطلحات //

* مصطلحات أساسية

← التهديدات

التهديد: هو أي شيء يمكنه أن يعطل عمل أو وظائف أو سلامة أو تواجد الشبكة أو النظام للاستخدام.

هناك أنواع مختلفة من التهديدات: هناك تهديدات حوادث طبيعية مثل الفيضانات والزلازل والعواصف. وهناك تهديدات غير المقصودة والتي تنتج عن الحوادث والأخطاء الناتجة عن الإهمال. وأخيرًا هناك التهديدات المقصودة والتي تكون تنتج لسوء النية.

أي نوع من أنواع التهديد يمكنه أن يكون مميتًا للشبكة.

← نقاط الضعف «الثغرات»

الثغرة هي نقطة ضعف تكون في التصميم أو التهيئة أو تنفيذ الشبكة أو النظام، الشيء الذي يجعلها عرضة للتهديد. معظم نقاط الضعف عادة ما يتم إرجاعها إلى واحد من ثلاث مصادر:

1- ضعف التصميم: الأجهزة والبرامج التي تحتوي على عيوب في التصميم والتي يمكن استغلالها. مثلاً عندما يتم إنشاء الإنترنت كانت تحتوي على ثغرات أمنية، مثال على ذلك: ثغرة إرسال البريد في النسخ الأولى لنظام يونكس UNIX. عيوب إرسال البريد مكنت القراصنة من الحصول على هذه الدخول إلى النظام الأصلي في نظام البريد وكانت ثغرة يونكس، حيث أنه تم استغلال هذه العيوب في مناسبات عديدة.

2- سوء التنفيذ: الأنظمة التي تم تكوينها بشكل غير صحيح تكون عرضة للخروج، هذا النوع من الضعف عادة ما يكون ناجمًا عن قلة الخبرة، عدم التدريب الكافي أو عدم تنفيذ العمل بصورة متقنة. مثال على هذا النوع من الضعف أن لا تحتوي النظام على امتيازات تقيد الوصول للملفات التنفيذية الحساسة، وبالتالي السماح للمستخدمين غير المصرح لهم بتعديل هذه الملفات.

٢- سوء الإدارة: الإجراءات الغير كافية وعدم كفاية التأكيد والموازنة.
الإجراءات الأمنية لا يكمن أن تعمل في فراغ، يجب أن تكون موثقة ومراجعة.
حتى الأعمال البسيطة مثل النسخ الاحتياطي اليومي للنظام يجب أن يتم تحقيقه،
وهناك حاجة أيضاً لفصل المهام بين الوظائف وازدواج الأخرى،
بهذه الطريقة، يمكن للمنشأة أن تضمن تقيد الموظفين بالإجراءات،
وأن يوجد شخص واحد لديه السيطرة الكاملة على النظام.

في حين أن هناك ثلاثة مصادر فقط لنقاط الضعف، فإنها يمكن أن تظهر في
نفسها بطرق كثيرة:

- نقاط ضعف مادية:

إن القاعدة الأولى لأمن كانافان (Canavan) هي لحماية مكونات الأنظمة
والشبكات، هل الكمبيوتر ومعدات الاتصالات ووسائط التخزين في مكان
آمن؟

أجهزة الاستضافة المركزية وموديم الشبكات يجب أن توضع في غرف مؤمنة يدخلها
فقط الموظفون المصرح لهم. وينبغي أيضاً أن تبقى أجهزة التوجيه ومعدات
الاتصالات في مواقع آمنة مقيدة الوصول. إضافة لذلك الوسائط المهمة
القابلة للحركة مثل وسائط النسخ الاحتياطي يجب أن تخزن في المنطقة الآمنة.
يستطيع الموظفون المخولون فقط الوصول إليها.

وكجزء من هذه العملية، تحتاج المنشأة إلى الأخذ في الاعتبار البيئة المادية والطبيعية
التي تعمل فيها. ينبغي أن تنظر إلى احتمال حدوث الزلازل والحرائق والفيضانات
وغيرها وتخطط وفقاً لذلك.

التخطيط السليم للمرافق المادية يمكن أن يخفف كثيراً من آثار الكوارث الطبيعية.
على سبيل المثال: المنشآت في المناطق المعرضة للزلزال تحتاج إلى تثبيت معداتهم
في هيكل المبنى بحيث لا تسقط من الجدران أو من النوافذ أثناء وقوع زلزال قوي.

المنشآة التي تكون واقعة في مناطق الفيضانات يجب أن لا تضع غرف
الأجهزة الحاسوب الخاصة بها في أقبية المباني.

• الأجهزة والبرمجيات:

عيوب التصميم في الأجهزة والبرامج تجعل الأنظمة عرضة للهجوم. على سبيل المثال: فشل ارسال رسائل البريد الالكتروني في الإصدارات الأولية لنظام تشغيل يونكس مكنت القراصنة من الحصول على امتيازات الوصول الى النظم.

• نقاط الضعف للوسائط

الأقراص والأشرطة والوسائط الأخرى عليها ان تتعرض للسرقة، لفقدانه، أو العطب، عملية نسخ المعلومات وأخذها من مراقبة المؤسسة دون اكتشافها. ووفقا لذلك، تحتاج الشركات الى ضمان سلامة جميع الوسائط التي تحتوي على معلومات حيوية.

• نقاط ضعف بث الإشارة - اعتراض المعلومات

الإشارة المرسلة من المعدات الكهربائية عملية اعتراضها من بعد ومراقبتها باستخدام أجهزة متطورة في عملية يشار إليها أحيانا بـ بوصف شائع إلى (VAN.ECK) الملاحظات تحتاج أيضا الى أن تكون قلقة بشأن اعتراض معظم اشكال الاتصال.

الاتصال: هو تبادل المعلومات عبر وسيط. على هذا النحو، فهو بطبيعته عرضة للاعتراض والرصد والسرقة والتغيير، والانقطاع.

كل وابط تستخدم لنقل المعلومات عليها استغلالها. متحسس الشبكات أو متحسس حزم الاتصالات هي أدوات القراصنة المشتركة التي يمكنها أن تقرأ حركة مرور البيانات عندما تمر عبر شبكة. أيضا الثغرات ربما تسبب ضررًا أكثر مما ينفع القراصنة وذلك عندما يتعلق الأمر بحركة الاتصالات.

• نقاط الضعف البشرية:

الاهمال البشري، اللامبالاة، الكسل، الجشع، والغضب تمثل أكبر تهديدات للشبكات والنظم وتسبب الكثير من الضرر من بقية العوامل الأخرى مجتمعة.

Scanned by CamScanner

* التدابير الصارمة

التدابير الصارمة هي التقنيات أو الأساليب المستخدمة للدفاع ضد الهجمات وحيد أو مقلل نقاط الضعف في الشبكات أو الأنظمة.

⊛ - مصطلحات أساسية إضافية

قبل الشروع في مناقشة جدية لأمن الشبكة، من الضروري أولاً تعريف بعض المصطلحات الأساسية المتعلقة بأمن الشبكة.

هذه المصطلحات هي الأساس لأي مناقشة لأمن الشبكات، وهي العناصر المستخدمة لقياس أمن الشبكة. ليتم اعتبارها فتقديمه بما فيه الكفاية على طول الطيف الأمني، يجب أن يعالج النظام بشكل كافٍ ثلاثة: تحديد الهوية - المصادقة - التحكم في الدخول أو الاذدناب - التواجد والسرية وسلامة والمسؤوليات - عدم الانكار.

P - تحديد الهوية:

تحديد الهوية ببساطة هو عملية تحديد البيانات إلى كيان آخر أو تحديد هوية الفرد أو الكيانات الذين نتواصل معهما.

ب - المصادقة:

تقدم المصادقة كدليل على أن الشخص الذي تدعيه أو حاول أنه تكونه.
المصادقة أمر بالغ الأهمية إذا أريد أن تكون هناك ثقة بينه طرفين. المصادقة مطلوبة عند الاتصال بواسطة شبكة أو تسجيل الدخول إلى الشبكة.
عند الاتصال بشبكة يجب أن تسأل نفسك سؤالين:

أ - من هو أنا أتواصل
ب - لماذا أعتقد أنه هذا الشخص أو الكيان هو أو هي أو من يدعي أنه يكون هو الشخص الحقيقي؟

إذا لم تكن لديك إجابة جيدة للسؤال «ب»، فمن المحتمل أن تكون أخطأت في الإجابة على السؤال الأول.

عند تسجيل الدخول إلى الشبكة، تستخدم ثلاثة سيناريوهات أساسية للمصادقة، وهي: شيء تعرفه - شيء لديك - شيء يتعلق بك

- شيء تعرفه: السيناريو الأكثر استخداماً هو شيء تعرفه وعادة ما يكون شيئاً تعلم أنه لصاحبه هويتك مثل كلمة سر، أو رمز، أو تسلسل. يقوم الأمن على فرضية إذا كنت تعرف كلمة المرور السرية أو رمز المرور فإنه يجب أن تكون الشخص الذي تدعيه وبناءً عليه يؤذن لك باستخدام الشبكة. على الرغم من أن هذا السيناريو يستخدم على نطاق واسع إلا أنه غير آمن تماماً، فمن السهل الاكتشاف عليه واختراقه.

- شيء لديك: "شيء ما لديك" يتطلب مفتاح، مثلاً، أو بطاقة رمزية، بعض الأدوات أو شيء الذي يتيح لك الاستخدام. ويعتمد الأمن على مفهوم أن الأفراد أو الكيانات المصرح لها فقط يمكنهم استخدام جهاز معين. يعيب هذا السيناريو أن "الشيء" يمكن أن يضيع أو يسرق.

- شيء يتعلق بك: "شيء ما يخصك" المصادقة تعتمد على السمات المادية أو السلوكية ويشار إلى هذا النوع بالمصادقة الحيوية (Biometric)، ووفقاً لنظام الـ Biometric يمكن مصادقة الحيوية بناءً على بصمات الأصابع، أو صوت الشخص أو مسح قزحية العين.

هذه تقنيات المفاتيح يمكن استخدامها.

هذه النظم إذا صممت بشكل صحيح فإن التحايل عليها أو اختراقها يكون صعباً للغاية. الحيلة هي العثور على نظام واحد يعمل بشكل صحيح.

2 - التحكم في الوصول "الترخيص"

وهذا يشير إلى المقدرة على التحكم في مستوى استخدام الأفراد والكيانات لشبكة أو نظام، وكم المعلومات التي يمكنهم الحصول عليها.

مستوان في التصريح يحدّد في الأساس ما الذي يسمح لك أن تفعله بمجرد المصادقة لك والسماح لك باستخدام الشبكة أو النظام أو لبعض الموارد الأخرى مثل البيانات أو المعلومات.

إن التحكم بالوصول هو تحديد مستوى إذن استخدام نظام أو شبكة أو معلومات ((على سبيل المثال مصنفة سرية أو سرية للغاية)).

د - توفر النظام :

هذا يشير إلى ما إذا كانت الشبكة أو النظام أو الأجهزة أو البرمجيات موثوقة بها ويمكن استعادتها بسرعة وبشكل كامل في حال حدوث انقطاع ما لحدث.

من الناحية المثالية ينبغي أن لا تكون هذه العناصر عرضة لهجمات الحرمان من الخدمة.

هـ - السرية :

وهذا أيضاً يمكن أن نطلق عليه الخصوصية أو السرية، ويشير إلى حماية المعلومات من الكشف الغير مصرح به. وعادة ما يتحقق إما عن طريق تقييد الوصول إلى المعلومات أو عن طريق تشفير المعلومات بحيث تصبح غير مفيدة للأفراد أو الكيانات الغير مصرح لها بالاطلاع عليها.

و - سلامة المعلومات

يمكن التفكير في هذا على أنه دقة المعلومات. ويشار إلى هذا على أنه القدرة على حماية المعلومات والبيانات أو الإرسال من التعديلات الغير مصرح بها أو غير المتحكم فيها أو الاعتراضية. مصطلح السلامة أيضاً يمكن أن يستخدم في إشارة إلى سير عمل الشبكة، النظام أو البرنامج التطبيقي.

عندما يستخدم المصطلح في الإشارة إلى المعلومات أو البيانات هناك عادة متطلبات للسلامة أولاً: يجب أن تكون البيانات متسقة مع المتطلبات الداخلية. على سبيل المثال: العمليات الحسابية يجب أن تكون دقيقة، جمع الأرقام في عمود الودائع في حساب الشركة المصرفي يجب أن تساوي إجمالي المبالغ المحفوظ لهذا العمود من الودائع

ثانيًا: يجب أيضًا أن تكون البيانات متسقة مع المتطلبات الخارجية، فمجموعة البيانات التي تمثل الودائع يجب أن تتطابق مع ما أودع فعليًا في الحسابات المصرفية.

كما يجب أن تكون البيانات متاحة في الوقت المناسب وكاملة.

إذا كانت البيانات تعطي مؤشر متأخر يوميًا أو أسبوعيًا، فإن سلامتها تكون موضع تساؤل. وبالمثل إن لم يتم تسجيل جميع البيانات فإن سلامتها أمر مشكوك فيه.

تكون سلامة البيانات عن طريق منع التغييرات غير المصرح بها أو غير الملائمة في البيانات، وضمان التنسيق داخليًا وخارجيًا، والتأكد من أن سمات البيانات الأخرى " مثل التوقيت " تتسق مع المتطلبات.

يمكن استخدام السلامة في إشارة إلى أسلوب عمل الشبكة أو النظام أو البرامج التطبيقية. على سبيل المثال: عند استخدام مصطلح السلامة في إشارة إلى النظام فهذا يعني أن النظام يعمل وفقًا للتصميم والمواصفات والتوقعات حتى في ظل الظروف الحرجة مثل الهجوم أو الكارثة

" تبقى سلامة النظام عالية حتى في ظل الضغوط "

ﻫ: المساءلة:

وهذا يشير إلى القدرة على تتبع أو تدقيق النشاط الذي يقوم به فرد أو كيان في الشبكة أو النظام.

هل يقوم النظام بعمل سجل للتدقيق يحتوي على الأعمال التي أجريت والملفات التي تم استخدامها، والمعلومات التي جرت عليها عمليات تغيير.

و: عدم الإنكار " التثبيت ":

القدرة على منع الأفراد أو الكيانات من إنكار أن المعلومات أو البيانات أو الملفات تم إرسالها أو تم استخدام هذه المعلومات أو الملفات أو تغييرها، عندما يكونوا في الواقع قد قاموا بذلك. هذه الإمكانية ذات أهمية عالية للتجارة الإلكترونية وبدونها يمكن للفرد أو الكيان أن ينكر أنه أو أنها المسؤول أو المسؤولة أداة المسؤول عن صفقة مالية وبالتالي فهو غير مسؤول ماليًا عن ذلك.

(1)

التهديدات ونقاط الضعف والهجمات

قبل أن نبدأ مناقشتنا للتهديدات، ونقاط الضعف والهجمات، من المهم مراجعة أساسيات البروتوكولات وخصوصاً بروتوكول TCP/IP ونموذج OSI ذي السبع طبقات.
هذا الاستعراض مهم لأن الكثير من الهجمات التي تحدث اليوم تستغل بعض نقاط الضعف الكامنة في تصميم البروتوكولات، وخصوصاً بروتوكول TCP/IP.
في الواقع الهجمات تستخدم وظائف البروتوكولات لاختراق هذه البروتوكولات.

* البروتوكولات The Protocols

البروتوكولات ليست أكثر من مجموعة من القواعد أو المعايير الرسمية التي تستخدم كأساس للاتصالات.
لقد تم تصميم البروتوكولات لتسهيل الاتصالات. سوف نستخدم ضابط البروتوكول في سفارة للتوضيح كيفية عمل البروتوكولات. وظيفة ضابط البروتوكول هو ضمان التواصل السليم بين السفارة والبلد المضيف. وظيفة بروتوكول الشبكة مشابه لذلك، فهي أيضاً تعمل لضمان الاتصالات بين أجهزة الشبكة. فقبل أن تقوم الأجهزة بعملية تبادل البيانات، فإنه من الضروري للأجهزة الاتفاق على القواعد "بروتوكول" التي ستحكم فترة الاتصال.

* - ١ - النموذج OSI المرجعي:

إن نقل المعطيات من طرف لآخر بالشبكة يلزم كما نعرف دعامة مادية (أسلاك) أو هرتزية للاتصال، ومن أجل وصول هذه المعطيات بشكل صحيح وبنوعية جيدة مقبولة للطرف الموزع إليه، فإن ذلك يتطلب بنية منطقية أو مادية معينة.
إن نموذج OSI المرجعي هو نموذج ذو سبع طبقات تم تطويره من قبل الهيئة الدولية للمواصفات والمقاييس International Standardization Organization: ISO وذلك في عام 1978.
إن النموذج OSI: Open Systems Internation اختصاراً من موديل أو نموذج المرجعية ISO وهو يشمل مختلف المستويات للنموذج ISO، حيث أن المستوى الثاني يؤدي لتصحيح الأخطاء.

إن الطبقات السبعة للنموذج المرجعي هي:

1- طبقة ١ : المستوى المادي الفيزيائي

2- طبقة ٢ : مستوى التركيب trame أو ربط البيانات

3- طبقة ٣ : مستوى الحزمة " مستوى الشبكة " Paquet

4- طبقة ٤ : مستوى الرسالة message أو مستوى النقل

5- طبقة ٥ : مستوى الجلسة أو الدورة session

6- طبقة ٦ : مستوى التقديم présentation

7- طبقة ٧ : مستوى التنفيذ application

1- طبقة ١ : المستوى الفيزيائي :

Couche 1 : Le Niveau physique

المستوى الفيزيائي يؤمن الوسائط الميكانيكية، الكهربائية.... لتفعيل العمل والاستمرارية ومن ثم التوقف عن العمل للوصلات الفيزيائية المخصصة لنقل العناصر الثنائية.

هذا المستوى له هدف قيادة العناصر الثنائية لا يحتاجهم على الدعامة الفيزيائية. وبالتالي هذا المستوى يحدد كل المواد والبرامج الضرورية من أجل النقل الصحيح للعناصر الثنائية ومنها :

- الانترفيس Interface للوصلات التجهيزات :

الـ Interfaces تطابق أو تقابل ما هذا الجزء الموجود على الهواتف، الأجهزة الحواسيب).... وهي لا تحدد فقط المآخذ الفيزيائي مع عدد أسلاكه، جهده، حركته،.... وإنما كل البرمجة اللازمة والضرورية لحمل العناصر الثنائية لنقل بشكل صحيح للمستقبل.

- الموديمات Modems :

Modulator - DeModulator

المودم هو الذي يحول الإشارة الثنائية المنتجة بواسطة التجهيزات الطرفية إلى إشارات ثنائية وتكون مجرّدة بشكل جيبي الذي يسمح لها بالانتشار بنوعية عالية

- المضاعفات Multiplexors وعكسها DeMultiplexors

وهي من أجل التركيز للعديد من الأقنية في قناة الاتصال العادية من آلات مختلفة وذلك على خط واحد من أجل الذهاب لنفس المكان،

أما الـ DeMultiplexors فتكون ضرورية من أجل الطرف الآخر وذلك من أجل إعطاء مسارات الأقنية التي تضمنت .

- عقد النقل : Noeuds de transfert

إن العقدة تشكل الجهاز العنصر الوسيط بين المرسل والمستقبل، وهي تأخذ كل عاتقها بلوكوتا المعلومات، التركيبات، الحزم المتواجدة على مرحلة من أجل إرسالها باتجاه خط الحزم 2 الصحيح.

- مختلف التجهيزات النوعية الضرورية لضمان استمرارية الإرسال الفيزيائي مثل: الشكاليب في حالة الاتصال بالطبقة المركزية.

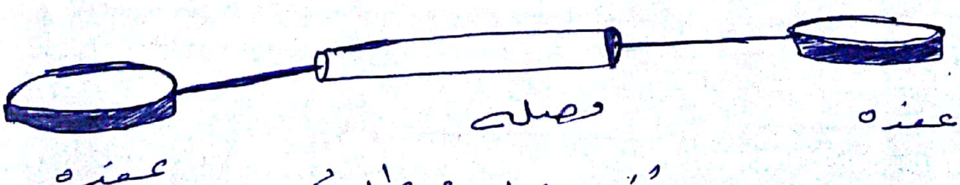
ج - طبقة 2: مستوى التركيب : Couche 2 : Le Niveau trame ربط البيانات

إن هذا المستوى يهتم بتأمين انتقال البيانات بطريقة معتمد عليها خلال رابط مادي وبعبارة أخرى توصيل الإشارة من أحد أطراف السلك إلى الطرف الآخر.

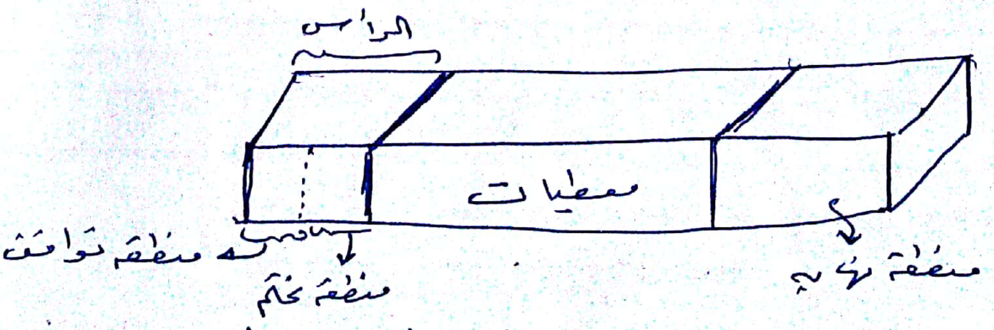
إذاً الوظيفة الأساسية لهذا المستوى: تخص إعادة التعرف على بداية ونهاية المعلومة، بحيث يمكنه أن يكون منقول بالدعامة الفيزيائية والمستقبل بشكل صحيح عند المستقبل.

إذاً في نموذج OSI 2 كما قلنا سابقاً، فإن هذه الطبقة تتولى توجيه البيانات وتضمن أن البيانات متوجهة إلى الوجهة الصحيحة.

الشكلين التاليين يوضحان ذلك



شكل : وصلة معطيات



شكل : trame كاملة

مستوى التركيب هذا كان مسؤولاً بشكل أساسي بكشف الأخطاء بالخط وتصحيح هذه الأخطاء بواسطة طرق ملائمة.

لذلك هذا المستوى عُدِّل بشكل كبير بنهاية التسعينات.

إن تعديل وظائف هذا المستوى كان بتحسين نوعية خطوط الهاتف (مثل استخدام الليف البصري) حيث أنه لا يوجد أخطاء أو على الأقل عدد الأخطاء صغير جداً من أجل عدم المعرقلة.

والسبب الآخر للتعديل هذا المستوى يكمن بالتحول لشبكات المعلومات إلى الشبكات ملتي ميديا حيث أن معدل خطأ البث مسموحاً من عدد كبير من التطبيقات مثل محادثات الهاتف - الفيديو يكون أفضل من الضجيج الأصوتي.

٢- طبقة ٣: مستوى الحزمة

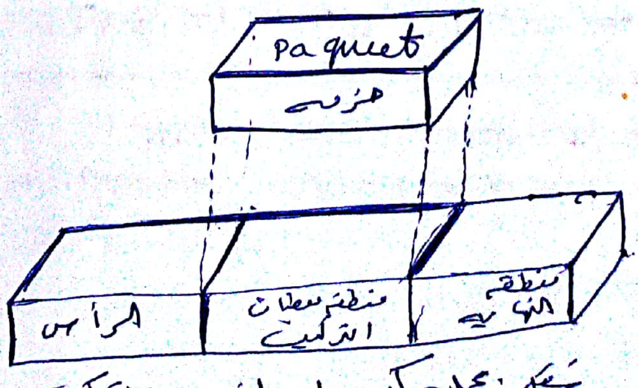
couche 3: Le Niveau paquet.

دور مستوى الحزمة يكون بنقل الحزم المشكلة للتدفق من طرف المستخدم إلى المستقبل للوصول لنفس الشبكة.

وبتعبير آخر: مستوى الحزمة الذي يسمى طبقة الشبكة بحالة الجيل الأول، هذا المستوى يسمح بالتوجيه وبشكل صحيح لحزم المعلومات حتى المستقبل للوصول بالشبكة وذلك بالعبور لعقد النقل الوسيطية.

فإذا كان المرسل والمستقبل غير متوضعين على نفس الشبكة، فإن أول مستوى حزمة ينقل المعطيات من المرسل باتجاه عبّارة (الجيتواي تسمح بالمرور من شبكة لأخرى) وبالتالي مستوى حزمة آخر الذي يقوم بتوجيه الحزم على الشبكة الثانية وهكذا حتى المستقبل.

ملاحظة: الحزمة بخلاف التركيب لا تقدم أية وسيلة لإعادة معرفة بدايتها ونهايتها، فمن أجل تنفيذ نقل الحزم من عقدة لعقدة، فإن مستوى الحزمة يستخدم مستوى التركيب من أجل كبسلة الحزمة في التركيب الذي يسمح بمعرفة بداية ونهاية الحزمة كما هو موضح بالشكل



شكل: عملية كبسلة الحزمة بالتركيب

...ال الرابع (10 درجات): لتنفيذ العبارة التالية، يطلب تحديد ما يلي.

(5)

إن مستوى الحزمة يستوجب ثلاثة وظائف أساسية :

- التحكم بالتدفق - التوزيع - العنونة

ويجب الملاحظ جيداً أن هذه الخواص تكون ظاهرة في مستوى التركيب في حال عدم وجود مستوى الحزمة

• التحكم بالتدفق : يسمح بتجنب الاختناقات بالشبكة

• التوزيع : يسمح بتوجيه الحزم المعلومات باتجاه طرف استقبالها.

• العنونة : كما تم الاشارة سابقاً بأن حالتي نقل المعلومة للمستقبل "توزيع - تبديل" فإنه يستخدم إما العنوان الكامل وإما مرجعية Référence .

من أجل الوصول بالحزمة وتطوير مستوى الحزمة فإنه من الممكن التمييز والاختيار بين نموذجين للعمل :

أ- نمط بوصلة Connection-Oriented :

وهو عبارة عن نوع من العمل الذي يفرض على المرسل الطلب من المستقبل السماح له ليتم نقل البيانات المعلومات، وبكلام آخر المرسل والمستقبل يكونان على توافق من أجل نقل المعطيات.

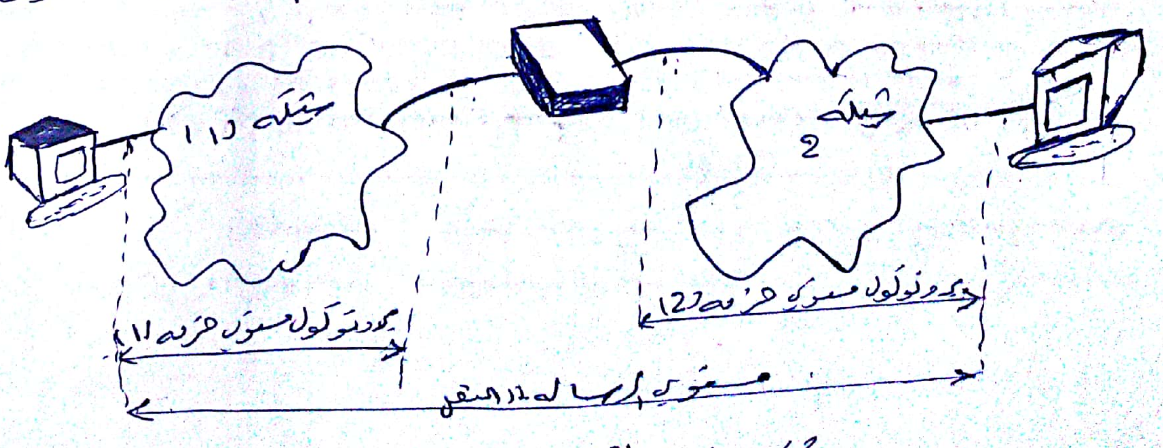
وهذا النمط يستخدم في بروتوكولات TCP ، ATM ، X25 HDLS

ب- نمط بدون وصلة Connection less .

في هذا النوع من العمل فإن المرسل يمكنه ارسال المعلومة باتجاه المستقبل بدون طلب إذنه والبروتوكول IP و Ethernet تستخدم هذا النمط .

ج- طبقة ٤ : مستوى الرسالة "النقل" couche 4: le Niveau Message.

مستوى الرسالة يؤمن نقل الرسائل من المرسل إلى المستقبل وهذا النقل يسمى طرف لطرف الذي يمكنه أن يعبر العديد من الشبكات كما هو موضح بالشكل.



شكل : مثال لمستوى 4

٥- الطبقة ٥ : مستوى الدورة "الجلسة"

Couche 5 : Le Niveau Session

هذا المستوى يُغذي بالوسائط الضرورية للتنظيم و توافق أو تزامن المحادثة أو الاتصال بين المشتركين.

هذه الطبقة من اسمها تدل على أن الهدف هو فتح و اغلاق الدورة بين المشتركين أو المستخدمين وبما أنه من غير المفيد ارسال المعلومة إذا لم يكن هناك مستقبل ليقوم باستقبال هذه المعلومة، فإن بروتوكول الدورة أو الجلسة يكفل ذلك ومنه أن المستخدم البعيد أو ممثله (لا على رسائل الكترونية مثلاً) موجود.

إذاً إن مستوى الدورة مكلف بالوظائف الضرورية لفتح الوصلة وحفاظ على ذلك وإغلاقها بالإضافة لخدمات عديدة (مثل تركيب نقاط تزامن).

من أجل إمكانية فتح وصلة مع آلة بعيدة، فإن طبقة الدورة يجب أن تمتلك اللغة الواضحة للطرفين الأخرى لذلك فإنه قبل فتح الدورة، فإنه من الإجباري المرور بنفس الوقت بمستوى التقديم (6) لضمان وحدانية اللغة وكذلك بمستوى التطبيق (7) من أجل العمل بإقترانات محددة بشكل متجانس ومتناسق.

وهذا ضروري لجعل الآلات الغير متجانسة مرتبطة بالاتصال.

٦- الطبقة ٦ : مستوى التقديم

Couche 6 : le Niveau pésentation

إن مستوى التقديم présentation يُعنى بأمر تركيب المحتوى للمعلومات، وبتعبير آخر فإن الطبقة 6 تضع بقالب أو بإطار المعطيات لجعلهم مفهومين من قبل المرسل إليه.

هذه الطبقة تلعب دوراً مهماً في الحصول على الوسط المتجانس، وهذه الطبقة عبارة عن وسيط لا يمكن الاستغناء عنه من أجل الفهم المشترك لتركيب الوثائق المنقولة بالشبكة، وذلك لأن مختلف الآلات الموصولة لا تلجأ لنفس التركيب أو التعبير فإذا كانت الآلات موصولة بشكل مباشر فيما بينها، فإن المعطيات من واحدة يمكن أنه لا تكون مفهومة من قبل الآخرين.

لذلك إن طبقة التقديم تُزوِّد بلغة نحوية مشتركة لكل المشتركين الموصولين.

فإذا كانت اللغة المشتركة هي Z وإذا كانت الآلة X ستتكلم مع الآلة Y فإن الآلتين ستستخدمان المترجمات X بـ Z و Y بـ Z لضمان التحاور بين X و Y

٧- الطبقة ٧ : مستوى التطبيق Couche 7: Le Niveau Application

مستوى التطبيق يشكل الطبقة الاخيرة للنموذج المرجعي، وهي واجهة المستخدم النهائية، وهذا يساهم في عملية تطوير تبادل المعلومات.
وهذه الطبقة او المستوى تشمل واجهات لكل الوظائف الضامنة للاتصالات بين الانظمة.
إن مستوى التطبيق مبني بواسطة اصناف كبيرة من التطبيقات، وهي تكون وفق ISO كما يلي:

- Message Handandling System MHS عملية الرسائل الالكترونية
- Directory Service: DS خدمات الدليل
- File Transfer Access and Management FTAM من أجل نقل الملفات والعالجة عن بعد
- Distributed transaction Prossessing DTP
- تسمح بسؤال قاعدة المعطيات الموزعة او اجزاء من النظام.
- Virtual Terminal VT : الطرفية الافتراضية ؛
  تسمح بالعمل على آلة عن بعد كما لو أنها هي عبارة عن آلة محلية
- Office Document Interchange Format ODIF
  من أجل تطبيقات النقل وإدارة أو تنظيم الوثائق المضبوطة.
- Office Document Architecture ODA
  وهي بنية الوثيقة المكتبية
- JTM
  Job Transfer and Manipulation
  المعالجة ونقل الاعمال الطابعة لارسال برنامج لآلة عن بعد وبالتالي تستطيع معالجة المعطيات
- MMS
  Manufacturing Message Service ; خدمات البريد الصناعي
- برامج FTP لنقل الملفات

* مجموعة بروتوكول Tcp/Ip

منذ اجل اتمام البروتوكول Ip ، قامت وزارة الدفاع الامريكية اضافة بروتوكول Transmission Control protocol Tcp الذي يحدد الـ Interface مع المستخدم

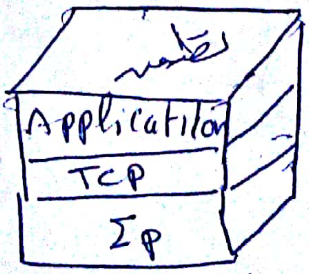
إن هذا التطوير تم تحت اشراف وكالة مشروع ابحاث الدفاع المتقدم (DARPA) وذلك عندما واجهت علماء وزارة الدفاع مشكلة ربط آلاف اجهزة الحاسوب التي تعمل بأنظمة تشغيل مختلفة.

علينا التفكير بأن مجموعة Tcp/Ip كشريان الحياة بالنسبة للانترنيت. وقد تم تبني مجموعة بروتوكول Tcp/Ip على نطاق واسع لانه معيار بروتوكول مفتوح يمكن تنفيذه على اي منظمة بغض النظر عن الشركة المصنعة، بالاضافة لذلك فهو مستقل عن اي اجهزة شبكة مادية.

يمكن تنفيذ Tcp/Ip على انترنيت X.25 ونظام توكن رانج To Ken ring ضمن المنصات الاخرى.

ان Tcp هو بروتوكول نمط بوصلة وهو معد لاتمام البروتوكول Ip من أجل تحديد الـ Interface تم استخدام ذكرنا سابقا، وهذا البروتوكول يطابق المستوى 4 من النموذج المرجعي.

البروتوكول Ip والبروتوكول Tcp كمجاميع كاملة ومجموعة Tcp/Ip التي تمثل تشكل بنية طبقية على التوالي لمستوى الحزمة ومستوى الرسالة من النموذج المرجعي وتم اكمال ذلك "موديل انترنيت" بواسطة طبقة ثالثة تسمى مستوى التطبيق الذي يضم مختلف البروتوكولات التي عليها تبنى خدمات الانترنيت: الرسالة الالكترونية - نقل الملفات - - - - . الشكل التالي يبين الطبقات الثلاث لبنية الانترنيت



ان بروتوكول Tcp يضم المهام المستوى 4 من النموذج المرجعي وهو بروتوكول معقد بشكل كافي

وهذا ما يمنح العديد من الخيارات التي تسمح بحل كل مشاكل ضياع الحزمة في المستويات الادنى، وبشكل خاص ان الجزء الضائع يمكن ان يكون مسترجع لها نفس معينة

ملاحظة: كما ان البروتوكول Tcp يستعمل النمط بوصلة فان البروتوكول UDP User Datagram protocol يستعمل النمط بدون وصلة، المستعمل كمكمل للبروتوكول Ip فانه يعمل بنمط بدون وصلة وهو ملائم كافة للتطبيقات التي ليست بحاجة للتحكم