أمن المعلومات للشبكات الصغيره و المتوسطه

المهندس نواف صالح المنج

المحتويات

المقدمـــة :-

- تزداد تهديدات الامن اليكتروني في كل يوم و لا يمر يوم دون وجود خبر عن نـوع مـن الاختراقـات او سـرقة البيانـات . مـن يملكـون او يـديرون المنشـات الصـغيره و المتوسطه يعرفون ان امن المعلومات قضيه هامـه و انـه ينبغـي ان تمنح تلك القضيه اهتماما كبيرا و تكمن المشكله في معرفة اين تبدأ.

امـن المعلومـات ضـرورة ملحـة بـل يمكـن القـول أن أي مشـروع او منظمـة تتضمن حلاً تقنياً أو شبكة لا بد أن يرافقه مشروع لأمن المعلومات يسير جنباً بجنب معه حيث يشتمل على التجهيزات والأدوات اللازمة لحماية المعلومـات التي يجرى التعامل معها ومعالجتها ونقلها.

قد يكون من الصـعوبه بمكـان تطـوير وثيقـه واحده لسياسـات امـن المعلومـات تغطـي جميـع مسـائل امـن المعلومـات الضـروريه لـدى المنشـات الصـغيره و المتوسـطه حيـث ان الفكـره الاكثـر فاعليـه هـي تطـوير مجموعـه مـن وثـائق السياسات لتغطية كافة اساسيات امن المعلومـات و توجيههـا نحـو مستخدمين محدودين مما يعزز من كافة العمليات لجميع الاطراف

هذا الكتاب يلقي الضـوء علـى العناصـرالواجب اخـذها بالاعتبـار عنـد اعـداد و ادارة سياسات و اجراءات و خطـة امـن المعلومـات لـدى المنشـات الصـغيره و المتوسـطه . و يقـدم نموذجـا لمجموعـه مـن وثـائق سياسـات و خطـة امـن المعلومات و عملية التطوير المصاحبه لذلك .

الفصل الأول

التهديدات والهجمات ونقاط الضعف

- امن المعلومات ليس ترفاً وليس سبباً لصرف الأموال والجهود دون مبرر قوي وحاجة ملحه لذلك , لذلك فمن الضروري تطبيق انظمة المعلومات اللازمة لحماية المعلومات والأنظمة المعالجة من التعرف إلى التهديدات المحيطة بها والهجمات الإلكترونية التي قد تفتك بها فلكي تكون المعلومات في مأمن لا بد من التعرف إلى تلك التهديدات والهجمات من اجل تسخير الطاقات الفنية والإدارية لمجابهتها.
- في هذا الفصل نوضح بدون اسهاب أو الدخول في تفاصيل تقنية كثيرة حيث وضحنا بالحد الأدنى لما يجب معرفته عن أمن المعلومات والمخاطر والتهديدات والهجمات التي قتد تتعرض لها الشبكة الخاصة بك.
- حيث يحتوي هذا الفصل على الآتي :-

1- تهديدات الأمن الشائعة

2- أنواع الهجمات الإليكترونية التي قد تتعرض لها الشبكة.

3- لماذا تعتبر البرمجيات نقطة ضعف.

1- تهديدات الأمن الشائعة:-

- الديدان Worms:-

الديدان هي عامل مستقل قادر على الأنشتار داخل ذاكرة الحاسوب , ويمر من نظام إلى آخر عبر الشبكة العنكبوتية . إنه نوع من البرامج مختلف عن الفيروسات لا تهاجم الدودة البيانات الشخصية للمستخدم , بل تقوم بنسخ ذاتها عبر الأنترنت حتى تصيب أكبر عدد من الأجهزة.

- الفيروسات Viruses :-

هو برنامج مدمر يسعى للانتقال من جهاز إلى آخر لنشر أضراره انه يصيب الملفات التنفيذية عادة لكي يتمكن من الإنتشار عبر الشبكة. سابقاً وقبل استخدام الإنترنت كانت الفيروسات تنتشر عبر تبادل الأقراص المرنة فقط لقد كانت مراقبة استعمال هذه الأقراص كافية للحد من الفيروسات أما اليوم فتستعمل الفيروسات البريد الألكتروني للإنتشار عبر الأنترنت وتستطيع مستندات مايكروسوفت اوفيس وبسبب احتوائها على وظيفة الماكرو إخفاء فيروسات فتاكة.

- احصنة طروادة Togon horses:-

- يستند مبدأ هذا الهجوم على الدخول إلى نظام الضحية عبر برمجية ما. يمكن اضافة شيفرة الفيروس ضمن البرمجية عند إصدارها , وقد يحتوي ملف تنفيذي ما , تتلقاه عبر البريد الإليكتروني على حصان طروادة.

- يستطيع القراصنة بواسطة حصان طروادة التحكم كلياً بجهازك إنهم يستطيعون الوصول إلى جميع البيانات في القرص الصلب وحتى أنهم يستطيعون متابعة كل العمليات التي تقوم بها بحصولهم على صورة عما يحدث في شاشتك.

- البرامج التجسسية Spyware :-

البرامج التجسسية هي كل برنامج يراقب سلوكك على جهازك من مراقبة كتاباتك إلى مراقبة المواقع التي تزورها. والهدف من برامج التجسس يكاد

ينحصرفي امرين أولهما التجسس الخبيث لاستقساء معلومات سرية مثل كلمات المرور وأرقام الحسابات البنكية والآخر : لأغراض تجارية مثل معرفة أنماط المستخدم الاستهلاكية , أو محركات البحث الأكثر استخداماً , والمواقع التجارية الأكثر تسوقاً.

- ان تلك البرامج تستنزف طاقات الجهاز والاتصال دون اذن واضح منك وكما تعلم أن مجرد المراقبة , وتسجيل السلوك أو المعلومات يتطلب وقتاً من المعالج ومساحة من الذاكرة ووحدة التخزين الدائمة وجزءً من كمية البيانات المرسلة عن طريق وسيط اتصال.

- الرسائل غير المرغوب فيها او (المزعجة) Spam :-

يرد إلى صناديق البريد الإليكتروني كثير من الرسائل (المزعجة) غير المرغوب فيها ويعد كثير من الناس ان هذه الرسائل لا تعد هجمات الكترونية , ولكن واقع الحال يقول ان كثيراً منها يحتوي على ملفات بها برامج او أكوادخبيثه , ويمكن التخلص من هذا النوع من الرسائل بتفعيل عمليات التنقيح والفلترة الموجودة في خوادم البريد وكذلك توعيه المستخدمين بحذف جميع الرسائل غير المرغوب فيها وعدم الثقة في هذا النوع من الرسائل وعدم فتحها.

- التصيد Phishing :-

- التصيد الإحتيالي هو محاول للوصول على معلومات حساسة مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقة الائتمان غالباً لأسباب ضارة وذلك بالتنكر ككيان جدير بالثقة في إتصال إليكتروني.

- الانتحال أو الخداع Spoofing :-

هو هجوم يتم فيه انتحال شخصية شخص ما او برنامج ما فمثلاً قد يسرق الهاكر معلومات بطاقة الائتمان لأحد العملاء ويستخدمها مدعياً انه العميل او قد يدعى انه الطرف المستقبل فمثلاً يريد العميل ان يصل الى موقع

بنـك لكـن قـد يـذهب إلـى موقـع آخـر ينتحـل موقـع البنـك دون إدراك منـه ويحصل ذلك الموقع من خلال هذه الطريقة على معلومات العميل.

- افشاء المعلومات :-

هو تعرض المعلومات للإفشاء لأشخاص غير مصرح لهم بالوصول إليها مثال على ذلك مستخدم عمل مشاركة لملفات معينة خلال الشبكة والتي يجب ان تكون غير مشاركة , غير ذلك بعض الموظفين يميلون إلى مشاركة ملفات هامة مثل كلمة السر مع أشخاص آخرين والذي لا يتوجب عليهم معرفة كلمات السر الخاصة بهم.

- حجب او رفض الخدمة Deny of service Dos :-

- تعد الهجمات بواسطة رفض الخدمة خطيرة جداً وتؤدي إلى إيقاف خدمة تكلف كثيراً بالنسبة للهيئات التي يعتمد نشاطها على نظام معلومات في الواقع تهدف هذه الهجمات إلى إعاقة عمل النظام وليس الحصول على المعلومات لكن قد تؤدي إلى نتائج كارثيه فقد البيانات خلال معالجتها قرصنة كل بيانات القرص الصلب

- تعتمد هجمات Dos على مهاجمة الجزء الضعيف في بنية الشبكة مثلاً قد تستخدم الهجمات اعتمادا على ضعف الجهاز يستعمل بروتوكول IP من الممكن ارسال حزم IP بطول كبير جداً إلى هذا الحاسب عندها , وعندما يتلقى هذا الحاسب هذا الكم الهائل من البيانات التي لا يستطيع التعامل معها يقوم بإيقاف جميع الخدمات لان ذاكرته اصبحت مشبعة.

2- الهجمات الالكترونية التي قد تتعرض لها الشبكة :-

- كركيزة اساسية لفهم الحاجة إلى أمن المعلومات يلزم المختصين والجهات المسؤولة عن تطبيق أمن المعلومات فهم طبيعة الهجمات الإليكترونية و التعرف عليها و التقنيات المستخدمه فيها من اجل اختيار التقنيات و الاليات و الطرق المناسبه لمكافحتها و فيما يلي بعض الامثله للهجمات الالكترونيه والحاجة الماسة إلى أنظمة المعلومات اللازمة لحمايتها

- هجمات البرامج الخبيثة Malicious Code Attacks :-

تشمل هجمات البرامج الخبيثة بشكل اساسي هجمات فيروسات وديدان الحاسب الآلي وبرامج احصنة طروادة وبرامج الاختراق , وبرامج التجسس الإليكتروني.

وقد تتسبب هذه البرامج في أضرار كثيرة تتراوح ما بين الازعاج وفقد البيانات ووصولاً سرقة الأموال ومن هناء تبرز الحاجة اللازمة إلى وجود أنظمة مكافحة هذه البرامج وتهديداتها.

- هجمات الخداع spoofing Attacks :-

هي طريقة للتمكن من الوصول إلى الأجهزة بطريقة غير شرعية عن طريق خداع هذه الأجهزة , بإرسال رسائل مخادعة تحتوى على عنوان انترنت (IP) يجعل الرسالة تبدو كأنه قادمة من جهة موثوقة . وهنا تبرز الحاجة لأنظمة المعلومات التي تستطيع كشف ذلك ومجابهته , خاصة على مستوى الموجات وجدران الحماية.

- هجوم تعطيل الخدمة Denial of Service (Dos) Attack :-

في هذا النوع من الهجوم يرسل عدد هائل من طلبات الأتصال أو أوامر برتوكولات الشبكات مثل آمر (Ping) إلى الجهاز الضحية من اجل إغراقة في معالجة هذه الطلبات وتحميله اكثر من طاقته حتى وصوله لدرجة عدم الإستجابة ومن ثم عدم قدرته على القيام بمهامةالمعتاده . وقد تصل درجة الإغراق في بعض الأحيان إلى تعطيل الهدف نهائياً وخروجه

عن الخدمة وتبرز هنا أهمية وخطورة هذا الهجوم وضرورة مكافحته واكتشاف طلبات وأوامر الإغلاق وتعطيلها. خاصة مع انتشار الأجهزة والشبكات المرتبطة بشبكة الأنترنت التي تقدم خدمات الإنترنت المختلفة مثل خدمة المواقع (www) ونقل الملفات (FTP) والبريد الإليكتروني , والسبب في ذلك هو ان هذه الخدمات تستخدم برتوكول (TCP) الذي يمكن استخدام بعض اوامره كأوامر إغراق ليس فقط لأجهزة الحاسب الآلي إنما يمكن توجيهها لإغراق اجهزة الشبكة كالموجهات وجدار الحماية.

- هجمات الإلتقاط أو التشمم Sniffer Attacks :-

المتشمم هو برنامج أو جهاز يراقب البيانات المارة عبر الشبكة ويلتقطها ويمكن أن يكون هناك تشمم او التقاط شرعي لمراقبة الشبكة ومتابعتها وإدارتها ويمكن ان يكون غير شرعي لسرقة البيانات . ويعد هذا الهجوم خطير جداً على الشبكة لأنه يمكنه زرع المتشمم في مكان في الشبكة وغالباً لا يمكن كشفة وهذا ما يجعله محبباً لدى المهاجمين ويزداد الآمر خطورة إذا كان نقل المعلومات يجري على الشبكة سواءً كانت محليه او واسعه في شكلها الأصلي غير مشفره لأن المتششم في هذه الحالة يستطيع قراءة كلمات المرور وكذلك محتويات الملفات النصية مثل ملفات معالجة الكلمات وهنا تبرز أهميه توفير أنظمة الحماية التي تكشف وجود برامج واجهزة التششم ومكافحتها وكذلك الأنظمة التي تحول دون الاستفادة من المعلومات المسروقة في حالة نجاح المتششم في سرقتها كأن تكون مشفره مثلاً.

- هجمات الهندسة الاجتماعيةSocial Engineering Attacks :-

يخلط هذا النوع من الهجوم بين النواحي الاجتماعية واهتمامات الناس وبين المهارات الفنية في خداع الضحايا وكسب ثقتهم للأدلاء بمعلومات سرية يتم استغلالها لسرقة المعلومات والأموال إليكترونياً وقد انتشر هذا

النوع من الهجوم في الآونة الأخيرة انتشاراً كبيراً لأنه يعتمد على كسر أنظمة الحماية التقنية التي تطورت مع مرور الوقت وإنما يعتمد على كسب ثقة الضحايا وإيهامهم بأن من يطلب منهم معلوماتهم السرية (كاسم المستخدم وكلمة المرور وارقام بطاقة الائتمان) هو جهة موثوقة (مصرف مثلاً) وبعد ذلك يتم استغلال هذه المعلومات وانتحال شخصيات الضحايا وقد تم سرقتهم إليكترونياً عن طريق دخول يبدو شرعياً لأنظمة الحماية ومن الأمثلة الشهيرة على هذا النوع من الهجوم هو هجمات الاصطياد الإليكتروني.

- تفجير البريد الإليكتروني Mail Bombing :-

وهذا أيضاً هجوم على البريد الإليكتروني لكن بنوع من انوع هجوم تعطيل الخدمة وهو هجوم تفجير البريد الإليكتروني وما يحدث في هذا الهجوم هو ان المهاجم يوجه عدداً هائلاً من الرسائل إلى عنوان البريد الإليكتروني للضحية التي من خلالها يمكن اغراق الضحية بعدد هائل من الرسائل الإليكترونية حتى الوصول إلى درجة عدم قدرته على معالجتها ومن ثم يدخل في مرحلة تعطيله عن الخدمة.

وهنا تبرز أهمية أمن البريد الإليكتروني ,الذي اضحى وسيلة اساسية للتواصل وإنجاز الأعمال على المستويات الحكومية والخاصة كافة وعلى مستوى الأفراد

3- لماذا تعتبر البرمجيات نقطة ضعف ؟

- ان بناء البرمجيات ومنها أنظمة التشغيل مثل ويندوز عملية معقدة ولا تخلوا من الأخطاء , كما انها بحاجة إلى تحسينات مستمرة تبعاً لتغير ظروف استخدامها وطلبات المستخدمين. ومن ناحية أخرى فإن الحاجة إلى التحسين المستمر يفرضها وجود الثغرات الأمنية التي تكتشف بشكل مستمر في هذه البرمجيات مما يحتم إغلاق كل الثغرات قبل أن تستغل , واغلاقها يتطلب تحديث البرمجيات , واكتشاف الثغرات قد يكون من قبل الشركة المصنعة للبرنامج وعندها تقوم الشركة بخطوة استباقية تصدر فيها تحديثاً لسد الثغرات الأمنية التي اكتشفتها للتو.
- وفي احيان كثيرة يسبق المتطفلون إلى اكشاف الثغرات الأمنية فيطورن برامج سيئة تستغل هذه الثغرات ويحدث دماراً يتوقف حجمة على عوامل منها : مهارة المتطفل المصمم للبرنامج وسرعة اكتشاف الثغرات والتعامل معها بعبارة اخرى فإن تحسين البرمجيات يفرضها أمران :-

أ- ادخال وظائف جديدة أو تحسين البرامج الموجودة في البرنامج

ب-سد الثغرات الأمنية المكتشفة في البرمجيات للحد من إختراقها من قبل المتطفلين.

الفصل الثاني

تقنيات وأدوات وحلول

- ما يؤرق مالكي الشبكات الحاسب الالي و مستخدميها هو موضوع امن هذه الشبكات خاصة في ظل تزايد استخدام شبكة الانترنت غير الامنه.
  و ظهرت الحاجه الملحه الى استخدام وسائل و تقنيات حمايه خاصه لهذا الغرض كإستخدام جدران الحمايه و اجهزة كشف و منع التسلل,
- في هذا الفصل سوف نتعرف على بعض التقنيات و الادوات و الحلول لحماية الشبكه و كيفية عمل كل منها و الدور الذي يؤديه في حماية الشبكات و انظمة الحاسوب المختلفه وهي كالاتي:

FireWall

IDS/IPS

VLAN

UTM

WSUS

RAID

NAT

SIEM

1- جدار الحماية Firewall:-

- ان الفوائد والخدمات التي جاءت بها شبكة الإنترنت لم تأت خلواً من المنغصات , فراجت سوق الطفيلين (Hackers) الذين لا هم لهم سوى التلصص على معلومات الآخرين كما ظهر أناس يتمتعون بإلحاق الأذى بالآخرين أما بحذف وثائقهم المهمة أو العبث بمحتوياتها , أو انتشار البرامج السيئة مثل الديدان والفيروسات وأحصنة طروادة وغيرها.
- ولمقاومة تلك الأخطار والحد منها ظهرت تقنيات ومفاهيم متعددة , من أكثرها إنتشاراً جدران الحماية (Firewalls) التي تسمى أيضاً الجدران النارية ولتقريب المعنى للأذهان نقول أن جدار الحماية نظام مؤلف من برنامج (software) يجري في الحاسوب او جهاز خاص يسمى بالجدار الناري .

وفكرة الجدار الناري (جدار الحماية) تشبه فكرة نقطة التفتيش التي تسمح بمرور أناس وتمنع آخرين , بناءً على تعليمات مسبقة.

- وضع جدار الحماية :-

ولتوفير بعض الحماية لنفسها تقوم المنشأت بوضع جدار حماية لعزل شبكتها الداخلية عن شبكة الأنترنت. بيد ان هذا العزل لا يمكن ان يكون كلياً , وذلك للسماح وللجمهور بالإستفادة من الخدمات المقدمة وفي الوقت ذاته منع الطفيلين والمخربين من الدخول وتتاح من خلال البرنامج الموجود في جدار الحماية مراقبة المعلومات بين الشبكة الداخلية للمنشأة والعالم الخارجي ولتحقيق الغاية من جدار الحماية فإنه لا بد من وضعة في موقع استراتيجي يضمن ألاتخرج او تدخل إلى الشبكة الداخلية إلا عن طريقة.

- انواع جدار الحماية :-

يمكن تصنيف جدار الحماية من حيث الجهة المستفيدة منها إلى ما يلي

أ- جدران نارية للمنشأت الكبيرة (Enterprise) وهذا النوع توفره شركات كبرى متخصصة مثل (cisco) و (symantec) وغالباً ما توفر الشركة المصنعة انواعاً متعددة من جدران الحمايه تتفاوت من حيث سرعتها والخدمات التي تقدمها وهذا النوع من جدران الحماية تتميز بما يلي:-

- إن جهاز الحماية يكون غالباً في جهاز قائم بذاته مصمم لغرض معالجة البيانات بسرعة فائقة أي انه ليس برنامج يعمل في جهاز حاسوب عادي
- تعدد الخدمات التي يقدمها جدران الحماية مثل غربلة المضاريف والحماية ضد الفيروسات وحماية البريد الإليكتروني والتشفير
- ارتفاع كلفة الشراء والتشغيل

ب- جدران ناريه لحماية المنشأت الصغيرة :- وهذا النوع يشبة سابقة في كونه جهازاً مخصصاً قائماً بذاته إلا أنه لا يجار به من حيث سرعة معالجة البيانات او تعدد الخدمات المقدمة ولهذا فإنه أقل سعر من سابقة.

ج- جدران الحماية للأجهزة الشخصية :- عبارة عن برامج تحمل في الحاسوب الشخصي بحيث تمر من خلالها جميع المعلومات الخارجة من الحاسوب او الداخلة إليه.

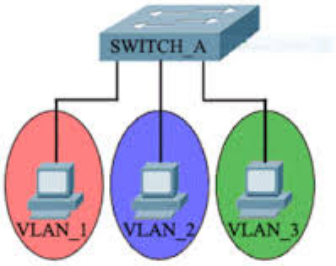
2- الشبكات المحلية الإفتراضية (Virtual V-LAN) :-

- قد اتت تقنيات المبدلات (الموزعات) (Switches) الحديثة امكانية إنشاء شبكات محلية إفتراضية او (تخيلية) (VLAN) كثيرة على مكونات الشبكة الفعلية (المادية) الواحدة نفسها. وبهذه الطريقة يمكن تقسيم الحاسبات الآلية في شبكة المنشأة التي قد تتكون من عدة شبكات محلية (LAN) مرتبطة بشكة واسعة (WAN) إلى عدة مجموعات إفتراضية تبدو كل واحدة منها كأنها مجموعة مستقلة. بغض النظر عن مواقعها الجغرافية مهما كانت متباعده. وتستخدم هذه الطريقة لتلبية حاجة المنشأة لتقسيم موارد الشبكة تبعاً لحاجة الأعمال والإجراءات لديها ولتحقيق مستوى أعلى من أمن المعلومات.
- تقدم الشبكات المحلية الإفتراضية عدة خدمات لتحسين امن المعلومات ورفع مستواه تتلخص في الآتي :

أ- فصل موارد الشبكة المهمة والحساسة مثل الخوادم في شبكة محلية افتراضية منفصلة لا يصل إليها الا المستخدمون المصرح لهم فقط.

ب-تساعد في الحماية ضد هجمات البرامج الضارة مثل الفيروسات بحيث إذا اصيبت شبكة افتراضية واحدة لا تنتقل العدوى إلى الشبكات الإفتراضية الأخرى

ج- تسهيل تطبيق سياسة أمن المعلومات بإختلاف أنواعها من خلال تطبيق السياسية المناسبة لكل شبكة إفتراضية على حده .



3- تقنية تحويل العناوين الرقمية(Network Address Translation) (NAT):-

- بعد زيادة عدد المستخدمين للأنترنت واحتياج كل مستخدم لـ (IP Address) خاص به للإتصال عبر الأنترنت في حين أن (IPV4) لم يعد يلبي هذه الإحتياجات بسبب سوء التوزيع مما يؤدي إلى نقص في توفر (Public IP add) لكل مستخدم تم اللجوء إلى حل يسمى (NAT) وهذا الحل يمكننا ببساطة من لوكان عندنا فرضاً شركة تتكون من (10) أفراد يستخدموا الأنترنت في عملهم. قبل هذا الحل كان لا بد من شراء (Public Add) من الـ (ISP) لكل فرد ليتمكنوا من استخدام الإنترنت في نفس الوقت أما مع هذا الحل يمكننا شراء (Public IP) واحد ليستخدمه الجميع
- يأتي دور تقنية الـ (NAT) عندما يرغب جهاز في الشبكة الداخلية الإتصال بجهاز خارج الشبكة الداخلية ولأن العنوان الرقمي للجهاز الداخلي غير معترف به خارجياً فإننا ننصب جهازاً وسيطاً بين الشبكة الداخلية وشبكة الإنترنت مهمته تحويل العنوان الرقمي الداخلي إلى رقم خارجي معترف به وغالباً ما يكون الجهاز الوسيط الذي يطبق تقنية الـ (NAT) إما جداراً نارياً (Firewall) أو الموجه (Router)
- العلاقة بين أمن المعلومات وتقنية الـ (NAT) :-

العلاقة تكمن في أن الجهاز الذي يقوم بتطبيق هذه التقنية هو في حقيقة الأمر يقف حائلاً بين الشبكة الداخلية وشبكة الإنترنت فلا يستطيع من كان مرتبطاً بشبكة الإنترنت معرفة العناوين الرقمية للأجهزة المرتبطة بالشبكة الداخلية. وهذا يسهم في حمايتها من عدد كبير من انواع الهجوم التي تشن بإستخدام شبكة الإنترنت بناءً على معرفة العناوين الرقمية

4- تقنية (All in one) (UTM) :-

- هي اختصار إلى (Unified Threat Management) وقبل الخوض في شرح (UTM) التي قد لا تكون غريبة على مسامع الكثيرين ممن يعملون في مجال أمن المعلومات وحماية شبكات الكمبيوتر
- جهاز (UTM) ببساطة هو عبارة عن جهاز لحماية شبكات الكمبيوتر وتقوم ببيعة العديد من الشركات مثل (Symantec) و (loktek) وغيرها وقد تم انتاج أجهزة (UTM) بعد ارتفاع معدل اختراق الشبكات للشركات وباتت غير قادرة على صد هجمات الهاكرز وغيرهم من مخربي مجرمي الإنترنت فسرية أمن المعلومات أهم مطلب للشركات
- تعتبر اجهزة (UTM) من أهم الوسائل للحماية فهو بمثابة جهاز (Firewall) متعدد الوظائف لذا تحرص الشركات والمؤسسات على شرائة وكما يفضل مشرفي شبكات الكمبيوتر (Network Administrator) استخدامه لأنه يقوم بعدة مهام تتعلق بحماية الشبكة مثل الحماية من الفيروسات – فلترة وتصفية المحتويات – محاربة البريد المزعج SPAM– ومراقبة حركة البريد الإليكتروني – الحماية من البرمجيات الخبيثة Malware وبرامج التجسس Spyware– تعطيل عمل برامج P2P - والتورنت – وبرامج VOIP - حجب المواقع المزيفة – مراقبة حزم البيانات وحركاتها من الطبقة الثانية إلى السابعة في نموذج OSI وتعمل أيضاً مع بعض أجهزة VPN وغيرها دون الحاجة إلى استخدام العديد من البرامج والأدوات لفعل ذلك وكما أنها سهلة التركيب والاستخدام وتوفر الوقت والمال.

5- اداة أو خدمة (WSUS) :-

- وهي اختصار لـ (Windows Server Update Service) وهي احدى خدمات مايكروسوفت التي تمكن المسئولين من إدارة وتوزيع التحديثات والإصلاحات العاجلة التي تصدر لمنتجات مايكروسوفت مثل (نظام تشغيل ويندوز – نظام تشغيل ويندوز سيرفر – مايكروسوفت اوفيس) وغيرها من المنتجات الموجودة على اجهزة الكمبيوتر في دومين الشركات
- يتم تحميل هذه التحديثات من موقع مايكروسوفت ومن ثم يتم توزيعها على أجهزة الكمبيوتر على الشبكة بهدف توفير إستخدام الأنترنت حيث يتم تحميل التحديثات مره واحده فقط عن طريق السيرفر وأيضاً ضمان عدم تنزيل اي تحديثات لم يختبرها ويوافق عليها مسؤول إدارة الشبكة في الشركة.
- حيث نستطيع القول بشكل مختصر ان مايكروسوفت Wsus Server وظيفته انه ينزل التحديثات updates من موقع مايكروسوفت ويوزعها على الأجهزة في الشبكة وبالتالي أن تعمل داونولد مرة واحدة فقط والميزة الأخرى أنك قادر على التصديقapprove على التحديثات updatesفي الأول قبل ما تنزل على الأجهزة لأن بعض الـ updates تعمل مشاكل عند تنزيلها على الجهاز.

6- تقنية الـ (RAID) :-

- قد تكون غير معروفة من قبل المستخدمين للكمبيوتر ولكن بالتأكيد هذه التقنية معروفة لدى اصحاب الشركات ومهندسي المعلومات والشبكات هي اختصار لـ Redundent Array Of Independance اي مصفوفة متكاملة مكرره من الأقراص غير مرتفعة الثمن.
- الـ RAID هي طريقة تخزين البيانات على اكثر من قرص في نفس الوقت بالإضافة إلى الأداء الأفضل والإتاحة الدائمة للبيانات وللرايد عدة انواع كل نوع له رقم محدد مثال على ذلك (Raid0 – Raid1 – Raid5 – Raid6)
- الفائدة من استخدام تقنية الـ Raid :-

أ- هذه التقنية تمكن الأقراص من النجاة من المشكلات العديدة التي تواجه أقراص التخزين سواءً كانت ميكانيكية أو الحالة الصلبة أثناء التخزين

ب-ملاحظةتغير في أداء الأجهزة في معدلات القراءة والكتابة مقارنة بوجود قرص واحد خارج المصفوفة.

ج- المساحة التخزينية والتي تمكنك من مجمع الأقراص المنفصلة من كيانات صغيرة إلى كيان واحد ذو مساحة تخزين كبيرة.

يجدر الإشارة ان هناك حلول اخرى للتخزين مثل (SAN - NAS) وتستخدم في الشركات الكبيرة والعملاقة.

7- أداة أو تقنية (Security information and event management) (SIEM):-

- امن المعلومات وادارة الأحداث :- هي عبارة عن تقنية أمنية على شكل تطبيق حيث عند تنزيله أو تثبيته علي سيرفر على الشبكة سوف يكون قادر على القيام بعده مهام أمنية (مراقبة الأجهزة والأنظمة والبرامج المختلفة).
- في أكثر الشركات أو المؤسسات يوجد عدة أنظمة تعمل مع بعضها البعض على سبيل المثال يوجد في الشركة جدار حماية (Firewall) وأيضاً اجهزة كشف ومنع التسلسل (IDS/IPS) أيضاً أجهزة شبكات راوترات وسوتيشات وسيرفرات بمختلف أنواعها مثل الأكتف دايركتوري Active directory وسيرفر الإيميلاتexchange server وغيرها
- نلاحظ أنه يوجد العديد من الأجهزة والأنظمة مع كثرة الأنظمة يصبح من الصعب مراقبتها ومتابعتها لذلك تم إنشاء نظام مركزي يسمى (Siem) يقوم بجمع الاحداث (Events) والتنبيهات الأمنية (Security alerts) من الأنظمة المختلفة الموجودة في البنية التحيتة للشركة بحيث يصبح مركزي ومن السهل مراقبته ومتابعة الأحداث الأمنية في مكان واحد
- امثله لأشهر أنظمة (siem) :-.

أ- IMB Security QRadar

ب-Mcafee Enterprise Security Manager

ج- Solarwinds Log & Event Manager

8- أجهزة كشف و منع التسلل IDS/IPS :-

- مراقبة الشبكه و التصدي للهجمات التي قد تتعرض لها و محاولات التسلل اليها تعتبر من النقاط المهمه الذي يجب توفيرها للشبكه و ذلك بهدف حمايتها.
- يوجد لدينا مجموعه من الاجهزه و البروتوكولات و البرامج التي من خلالها سوف تتمكن من عمل مراقبه للشبكه او منع التسلل اليها منها الاتي :-

أ- نظام كشف التسلل-(IDS) Intrusion detection system

- و هو نظام يقوم بمراقبة حركة البيانات في الشيكه و اذا وجد حركد بيانات مشبوهه يقوم بارسال تحذير او انذار الى جهاز مسئول الشبكه كي يتصرف و يمنع البيانات المشبوه فبها .
- البيانات المشبوه فيها مثل الفيروسات و البرامج الضاره - ديدان – محاولات اختراق – هجمات حجب الخدمه – و غيرها و التي تمر في الشبكه على شكل بيانات مشتبه فيها

ب- تظام منع التسلل (IPS) Intrusion prevention system

- هو نظام امن للشبكات الذي يقوم بمراقبة الشبكه و حركة المرور فيها و يعتبر تطوير لل IDS. و من المهام الرئيسيه لانظمة منع التسلل يقع في تحديد الانشطه الخبيثه و تسجيل معلومات عن النشاط و محاولة وقفه أو منعه أو التعامل معه و الابلاغ عن ذلك .

الفصل الثالث

سبع خطوات لأمن جيد

Seven Steps To Better Security

- هذا الموضوع يوضح الخطوات والمقاييس الأمنية الأساسية (base lines) التي على كل شركة او مؤسسة أن تضعها بعين الإعتبار لحماية الشبكة الخاصة بها أو لحماية أمن المعلومات لديها بشكل عام. هذه خطوات تفترض انه لا يوجد سياسية أمنية أو خطة أمنية مكتوبه ومنفذه على أرض الواقع للإطلاع على السياسات الأمنية وأنواعها والخطة الأمنية لا حقاً في هذ الكتاب

Seven Steps To Better Security:-

1- Protect Your Desktops and laptops

2- Keep Your Data Safe

3- Protect Your Network

4- Protect Your Servers

5- Use The Internet Safely

6- Secure Your Business applications

7- Manage Computers From Server

1 سبع خطوات لأمن أفضل :-

1- حماية أجهزة الكمبيوتر واللابتوب

2- الحفاظ على البيانات بشكل أمن

3- حماية الشبكة الخاصة بك

4- حماية الخوادم الخاصة بك

5- استخدام الأنترنت بشكل أمن

6- تأمين التطبيقات الخاصة بالعمل

7- إدارة أجهزة الكمبيوتر من خلال الخادم

1- الخطوة الأولى :- حماية اجهزة الكمبيوتر والمحمول:-

إذا كان هناك ثلاث خطوات احترازية يجب إتخاذها لحماية أجهزة الكمبيوتر التي في بيئة العمل لتكن تلك الخطوات الاحترازية الثلاث هي :-

أ- تحديث أنظمة التشغيل والبرامج.

ب- استخدام برامج مكافحة الفيروسات

ج- إعداد جدار الحماية (الجدار الناري)

أ- تحديث انظمة التشغيل والبرامج :-

- يعتبر الحفاظ على حاسوب ويندوز الخاص بك محدثاً من الأمور الهامة التي يجب أن تضعها بعين الإعتبار حيث يساهم ذلك في زيادة الإنتاجية وحماية الحاسوب وتطبيقاته من هجمات المتسللين الذين يستغلون عدم تحديث التطبيقات وأنظمة التشغيل لإيجاد نقاط الضعف التي تساعدهم على شن هجماتهم.
- من الخطوات البسيطة الممكن اتخاذها ضبط نظام التشغيل ويندوز مثلاً لعمل تحديث تلقائي لنظام التشغيل.

ب-استخدام برامج مكافحة الفيروسات:-

- مضاد الفيروسات او برامج مكافحة الفيروسات هو برنامج يتم استخدام لإكتشاف البرمجيات الضارة كفيروسات الحاسوب وأحصنة طروادة ودودة الحاسوب وذلك لمنعها بإلحاق الضرر بالحاسوب أو سرقة البيانات الشخصية عن طريق إزالتها أو إصلاحها
- من الخطوات التي يجب ان تتخذها هو تنصيب برنامج مكافحة الفيروسات لكل اجهزة الكمبيوتر في الشبكة. حيث تقوم برنامج مكافحة الفيروسات بعمل فحص للملفات والبرامج والإيميلات الموجودة على جهاز الكمبيوتر للتأكد من عدم وجود فيروس في حالة الإصابة بالفيروس يقوم برنامج المكافحة بعزلة أو حذفة.

- تحديث برامج مكافحة الفيروسات :- لأن هناك المئات من الفيروسات التي تصدر كل شهر يجب ان تحدث برامج مكافحة الفيروسات بإنتظام بأحدث تعاريف للفيروسات حيث يستطيع برنامج المكافحة الإمساك ومكافحة أحدث الفيروسات.
- امثلة على برامج مكافحة الفيروسات:-

1- Norton Antivirus

2-MacAfee VirusScan

3-Kaspersky Antivirus

ج- إعداد جدار الحماية (الجدار الناري) :-

- عندما تكون شبكة الحاسوب الآلي الخاصة بالشركة أو المؤسسة متصلة بشبكة الأنترنت أو اي شبكة خارجية فأن هناك طريقين للإتصال أحدهما يصل من الخارج إلى شبكة المنشأة والآخر من شبكة المنشأة إلى الخارج ولمنع اي وصول غير مصرح به لشبكة المنشأة فيجب استخدام أداة منع خاصة تسمى جدار الحماية أو جدار النار وهو اما يكون جهازاً مستقلاً خاصاً يصنع لهذا الغرض وبه برامجه الخاصة به أو يكون برنامج ينصب على أجهزة الحاسوب الآلي العادية.
- يعمل جدار النار كمصف أو منقح للرزم (Packets) البيانات الداخلة والخارجة من شبكة المنشأة وإليها أي أنه يكون طبقة عازله بين شبكة المنشأة والعالم الخارجي.
- تفعيل الجدار الناري الخاص بنظام ويندوز لأجهزة الكمبيوتر في الشبكة هو الخيار الأمثل.

2- الخطوة الثانية:- الحفاظ على البيانات بشكل آمن :-

- ان تنفيذ إجراء لعمل نسخ احتياطية بشكل دوري ومنتظم هو الطريقة السهلة لحماية المعلومات في العمل لديك , كما ان وضع صلاحيات للوصول إلى البيانات والمعلومات وتشفير تلك البيانات الهامة قد يساعد أيضاً في جعل بياناتك مأمنه بشكل جيد
- تخيل ان جميع ملفاتك التي خلال شهور وسنين قد محيت من حاسوبك فجأة لسبب أو لآخر . ماذا تقول عندها .. ياليتني حفظت نسخه من ملفاتي خارج الحاسوب وهو ما يسمى بالتخزين الإحتياطي.

1- تنفيذ اجراء لعمل نسخ احتياطية للبيانات الهامة :-

- حيث يتألف التخزين الإحتياطي من :-

1- البيانات المراد تخزينها من ملفات أو مجلدات.

2- وسيلة التخزين مثل الأقراص الصلبة والمدمجة للتخزين أو ملف مشاركة على شبكة.

3- برنامج التخزين الذي يقوم بتخزين او استرجاع البيانات.

- سوف نقتصر في هذا الجزء على برنامج النسخ الاحتياطي المدمج مع نظام تشغيل ويندوز.
- هناك أكثر نوع للـ (Backup) :-

1- Full Backup :- نسخة احتياطية كاملة لجميع البيانات المحددة والذي يتم نسخها إلى وسيط آخر.

2- Incremental Backup :- يعمل نسخة من البيانات التي اضيفت أو تعدلت أو تغيرت منذ آخر نسخ إحتياطي كامل Full Backup

- يتوجب عليك حفظ هذه النسخ الإحتياطة في مكان آمن وخارج نطاق المنشأة أو العمل

- ينصح بعمل اختبار لاسترجاع النسخ الاحتياطية في موقع خاص بالإختبار بهذه الطريقة يمكنك أن تتأكد من ان النسخ الإحتياطية تم نسخها بشكل جيد وتتعرف إذا ما كان هناك مشاكل قد تواجهك في عملية استرجاع البيانات.

2- تأسيس صلاحيات للمستخدمين :-

- كلا النظامين التشغيل ويندوز وويندوز سيرفر يمد بطريقة حماية ضد ضياع البيانات من الأنشطة التي يقمون بها الموظفون.
- حيث خلال نظام تشغيل ويندوز ونظام تشغيل ويندوز سيرفر تستطيع من خلاله تحديد مستويات الصلاحية المختلفه للمستخدمين بناءً على أدوارهم ومسؤولياتهم في الشركة أو المنظمة ويعتبر هذا أفضل من إعطاء الصلاحيات الكاملة (Admin Access) إلى كل الموظفين مما يحافظ على بيئة عمل آمنة والحد الأدنى من الصلاحيات.

3- تشفير المعلومات الهامة أو الحساسة :-

- التشفير هو العملية التي يتم من خلالها تغيير البيانات وجعلها في شكل غير مفهوم أو غير مقروء بحيث لا يستطيع إرجاعها إلى وضعها الأصلي إلا الشخص المصرح له فقط الذي لدية الأدوات اللازمة لذلك.
- التشفير يستخدم للتأكد من الموثوقية والسرية للبيانات التي تخزن أو تمر خلال الشبكة. فقط المستخدمين المصرح لهم والذين يملكون أدوات التشفير وفك تشفير الملفات يستطيعون الوصول إلى هذه الملفات.
- نظام ويندوز يقدم تقنية لتشفير الملفات والمجلدات.

3- الخطوة الثالثة:- حماية الشبكة الخاصة بك :-

- من الخطوات الأساسية التي يمكن ان تتخذها حيث ان هناك بعض المقاييس التي عمل على انقاص مخاوف الأمن للشبكة :-

أ- اعداد جدار ناري خارجي

ب-استخدام كلمات سر قوية

ج- استخدما خصائص الأمن للشبكة اللاسلكية

أ- إعداد جدار ناري خارجي :-

- الجدار الناري يتحكم بالوصول من والى الشبكة أو جهاز الكمبيوتر او حجب المتسللين من الوصول إلى الشبكة الخاصة بك والتحكم بالذي يستطيع موظف الوصول إليه خارج الشبكة
- الجدار الناري الخارجي يحمي جميع أجهزة الكمبيوتر والشبكة ويعتبر أيضاً خط دفاعي إضافي لأنه يجعل جميع أجهزة الكمبيوتر في الشبكة غير مرئية للعالم الخارجي.

ب- استخدام كلمات مرور قوية :-

- كلمة المرور هي اداة تخول الشخص للدخول لمكان خاص لا يدخله إلا أشخاص . معينون كلمة المرور تثبت للنظام انك فعلاً أنت من تدعي بأنك هو , كلمة المرور تحمي بياناتك الهامة والمعلومات الحساسة الخاصة بك.
- كلمة المرور هي احدى الطرق وأرخصها للتحكم بالدخول للنظام لذا يتحتم علينا ثلاثة أمور هي :-

1- الاختيار الأمثل لكلمة المرور لكي لا تكون سهلة التخمين.

2- المحافظة عليها وعدم اطلاع الغير عليها.

3- تغييرها دورياً

للمزيد من المعلومات يمكنك الاطلاع على السياسة الأمنية لكلمات المرور لاحقاً في هذا الكتاب.

ج- استخدام خصائص الأمن للشبكة اللاسلكية :-

- هناك عده نقاط التي نقوم بها لحماية الشبكة اللاسلكية وهي كالتالي :-

1- الغاء بث الـ SSID بحيث من يريد الاتصال بالشبكة اللاسلكية يجب أن يكون على علم بالـ SSID وإدخالها يدوياً

2- إختيار نظام تشفير قوي

3- إستخدام MAC Address بحيث يتم تحديد ال(MAC) للأجهزة المسموح لها بالوصول إلى الشبكة اللاسلكية.

4- يجب التأكد من الشبكة اللاسلكية لا تتجاوز خارج موقع العمل حيث توفر بعض WAP امكانية التحكم في قوة الطاقة

5-في حالة توفر هذه الخاصية في الـ WAP يمكنك إنشاء حساب لكل متصل بالشبكة اللاسلكية والحساب مكون من (اسم المستخدم وكلمة المرور) حيث كلمة المرور على الأقل (8 خانات ممزوجة من الحروف والأرقام والرموز).

4- الخطوة الرابعة:- حماية الخوادم الخاصة بك :-

- حيث هناك حماية فيزيائية وحماية برمجية :-

أ- الحماية المادية او الفيزيائية Physical security :-

- فهي تحمي أنظمة المعلومات من المخاطر المادية المباشرة كالوصول إلى مناطق غير مسموح بها والسرقة والتخريب المتعمد وعبث المعتدين والفضوليين , لذلك يجب وضع السيرفرات في غرفة خاصة (data center) يمكن إغلاقها وبحيث يكون التصريح للوصول إلى الخوادم التي تقع في مركز البيانات لأشخاص معدودين ولديهم الصلاحية لذلك

ب- الحماية البرمجية :-

- ونقصد بها تطبيق الحد الأدنى لمعايير الأمن الأساسية وذلك من خلال :-
  1- تحديث أنظمة التشغيل والبرامج
  2- استخدام برامج مكافحة الفيروسات
  3- تفعيل الجدار الناري

* تطبيق الحد الأدنى من الصلاحيات :-

- ان مبدأ تطبيق الحد الأدنى من الصلاحيات تملي أن المستخدمين يجب أن يمنحوا الصلاحيات لأداء أعمالهم فقط وليس أكثر من تلك من الصلاحيات.
- ان نظام ويندوز سيرفر يقدم إمكانية مستويات مختلفة من الصلاحيات للمستخدمين للموارد المحلية أو الموارد على الشبكة وذلك افضل من إعطاء صلاحيات كاملة مثل Administrator وذلك للمحافظة على بيئة آمنة لأجهزة الكمبيوتر أو الخوادم
- للمزيد من المعلومات يمكنك الاطلاع على السياسة الأمنية لحماية الخوادم لاحقاً في هذا الكتاب.

5- الخطوة الخامسة:- استخدام الانترنت بشكل امن :-

- توفر شبكة الإنترنت للعاملين في المنشأة لتسهيل القيام بأعمالهم والتواصل فيما بينهم ومع الجهات الخارجية حسب حاجة العمل وكذلك للحصول على المعلومات الضرورية من الشبكة وتصفح المواقع ذات العلاقة بعمل المنشأة من المواقع ذات الفائدة والمصداقية العالية .
- لقد أدى الإستخدام الواسع والمتسارع لخدمات الإنترنت إلى تحسين الكفاءة والوصول بشكل أكبر وأسرع لمصادر المعلومات الضخمة المتوافرة على شبكة الإنترنت إلا أن هناك بعض المخاطر المتأصله في إستخدام الإنترنت قد يتسبب في الأضرار البالغ بشبكة الحاسب الآلي الداخلية وقواعد البيانات والبيانات الحساسة للمنشأة وقد تعرضها للإختراق أو الفقد أو عدم التوافر

- نصائح لتصفح آمن :-

1- الذهاب إلى المواقع الموثوقة فقط.

2- لا تتصفح المواقع من السيرفر (الخادم) دائماً استخدم اجهزة الكمبيوتر لذلك.

3- لا تسمح لموقع الإنترنت أن ينصب برنامج ما لم تكن واثقاً من الموقع والبرنامج المراد تنصيبه

4- استخدم الجدار الناري أو الراوتر. عمل ذلك سوف يسمح لك لفلترة المواقع ويعمل حجب لحركة المرور للإنترنت من وإلى المواقع الخطيرة.

5- إستخدم برامج فلترة الويب Web Filtering Software حيث ان بعض الشركات تقدم منتجات (برمجيات) تعمل على فلترة الاستخدام للإنترنت بناءً على العديد من المعايير.

6- عمل الاعدادات الأمنية للمتصفح الذي تقوم باستخدامه.

7- المعرفة التامة بأنواع الملفات التنفيذية التي تحمل أكواداً ضارة مثل أكتف إكس Active X

6- الخطوة السادسة:- تأمين التطبيقات الخاصة بالعمل :-

- حيث قد يكون التطبيق Database Server أو Web Serverأو SharePoint Server أو Oracle Server

- من الخطوات الأساسية لحماية تطبيقات العمل الخاصة بك من المتلصصين غير مرغوب فيهم والتهديدات الآخرى نبدأ بتطبيق الحد الأدنى من المقاييس الأمنية للأمن في بيئة العمل الخاصة بك وهي كالتالي :

1- اعداد وتفعيل الجدار الناري

2- تنصيب برنامج مكافحة الفيروسات :- ان وجود برنامج مكافحة الفيروسات في السيرفر (الخادم) لها نفس أهمية وجود برامج المكافحة في أجهزة كمبيوتر المستخدمين. ابحث عن البرامج لمكافحة الفيروسات التي لها القدرة على كشف الفيروسات والتعامل معها والتي تعمل تحديثات دورية للفيروسات الجديدة.

3- حفظ نسخ احتياطية :- الحوادث تحدث من حين لآخر ويجب حفظ نسخة احتياطية للملفات الهامة وبيانات تطبيقات العمل لحمايتها من الضياع أو الفقد. أنظمة ويندوز توفر خاصيه أو أداة للنسخ الإحتياطي التي من السهل إستخدامها.

4- استخدام كلمات مرور قوية : كلمة السر يجب أن تكون متطلبة للدخول لأي جهاز كمبيوتر أو خادم في بيئة العمل. كلمة السر القوية يجب أن تحتوي على الحروف (الكبيرة والصغيرة) والأرقام والرموز وأيضاً يجب ان يتم تغيير كلمة السر دورياً وبإنتظام

5- تحديث البرمجيات وأنظمة التشغيل

- لان تطبيقات العمل تستخدم قواعد البيانات لحفظ بيانات التطبيقات . يجب وضع بعين الاعتبار الامن لقاعدة البيانات حيث يمكنك اتباع بعض النصائح للتعامل مع قواعد البيانات .

- نصائح للتعامل مع قواعد البيانات :-

1- تنصيب وإنزال التحديثات الضرورية لقاعدة البياناتService Pack وذلك لتحسين الأمان والأداء

2- تقييم الأمن للخادم الخاص بك بواسطة أداء MBSA (Microsoft Baseline Security Analysis)

وهي أداة مجانية يمكن تحميلها وإستخدامها لعمل مسح مستقل أو لكمبيوترات الشبكة لتحديد نقاط الضعف الأمنية. حيث بواسطة MBSA يتم تحديد التحديثات الضرورية لأنظمة التشغيل والتطبيقات

3- عزل الخادم فيزيائياً وعمل النسخ الإحتياطية بشكل منتظم

- تنظيم الوصول إلى المعلومات :-

أ- لا يجب ان كل شخص يمتلك الوصول إلى كل الموارد في بيئة العمل , إذا كنت تستخدم نظام التشغيل ويندوز سيرفر فأنت تستطيع تقييد الموظفين للوصول إلى المستندات وملفات العمل ويمكنك أيضاً تحديد الصلاحية للمستخدم هل مسموح له بقراءة الملف أو تعديله.

ب- اتبع الإرشادات الآتية لتنظيم الوصول إلى المعلومات :-

1- قم بتحديد الصلاحيات لمجموعة من المستخدمين وليس كل مستخدم على حده عمل ذلك سوف يوفر الوقت والجهد لإدارة أمنة للوصول.

2- إنشاء المجموعة (Group) يكون معتمد على الأدوار والمسئوليات مثلاً مندوبي المبيعات حيث يتم تحديد الصلاحيات المتعلقة لأداء المهام لهذا الدور أو المسؤولية.

3- إعداد حق الوصول للمعلومات لكل مجموعة إلى الحد الأدنى المطلوب والذي تمكن المستخدمين من أداء أعمالهم فقط.

7-الخطوة السابعه:- ادارة الكمبيوترات من الخادم

- لتوفير الوقت و المال و لتخفيض مخاطر الامن الى الحد الادنى. يجب ان يتم ادارة الكمبيوترت من السيرفر (الخادم) و ذلك لكسب العديد من الامور مثل التحديثات في الوقت المناسب – اعدادات خاصه – المراقبه و التحكم .

أ - التحديثات في الوقت المناسب :-

تستطيع نشر و توزيع التحديثات و إصلاحات الامن للبرمجيات و انظمة التشغيل من الخادم الى اجهزة الكمبيوتر للمستخدمين . بهذه الطريقه تستطيع ان تعلم ان التحديثات تم نشرها و تطبيقها في الوقت المناسب دون الحاجه الى تذكير المستخدمين للقيام بذلك بانفسهم . تستطيع عمل اختبارات للتحديثات قبل نشرها و توزبعها للتاكد من ان الكمبيوترات على الشبكه سوف تعمل بشكل جيد مع هذه التحديثات .

ب – اعدادات خاصه :-

تستطيع ان تعمل بعض الاعدادات الخاصه و تطبيقها و فرضها على مستوى المنشاه مثال على ذلك تستطيع منع المستخدمين في الشبكه من تنصيب البرامج و ذلك بتقييد صلاحية المستخدمين و منعهم من تنصيب البرامج او من تحميلها من الانترنت .

ج - المراقبه و التحكم .

الفصل الرابع
إنشاء سياسة أمنية

(Creating Security Police)

- يمكن القول انه لا توجد سياسة أمنية تغطي جوانب أمن المعلومات كافة في جميع إجراءات المنشأة فلا بد من وضع طريقة مناسبة للتعديل أو الإضافة على السياسة الأمنية وترك مجال لذلك وفق ضوابط محددة ويجب مراعاة إمكانية مراجعة السياسة الأمنية والتعديل عليها مع مرور الزمن أثناء التطبيق.
- الحاجة إلى السياسية الأمنية :- يجب أن تؤدي السياسة الأمنية أغراضاً كثيرة منها :-

1- حماية وأمن المعلومات

2- المساعدة في خفض المخاطر إلى الحد الأدنى

3- الاستجابة لأي حوادث أمنية تتم بصورة فعالة

4- إشراك الموظفين في جهود الجهة المعنية لتأمين اصولها المعلوماتية والمادية

5- المساعدة في متابعة الإلتزام بالأنظمة والتعليمات

- حيث الـ Institate SANS عرف مجموعة من العناصر التي يجب ان تكون متضمنة خلال السياسة الأمنية الجيدة هي الآتي :-

1- الهدف من وجود السياسة وسبب وجودها

2- المجال التي سوف تطبق عليه السياسة

3- الاصول المحمية :- تعرف الأصول التي سوف تحميها السياسة مثل Website- (الخوادم) – الأجهزة –Database

4- المسئوليات :- هذا المقطع من السياسية يعرف المسؤول سواءً كان شخص أو مجموعة أشخاص التي سوف تكون مسئوليتهم تنفيذ شروط أو تفاصيل السياسة.

5- العواقب المترتبة على عدم الامتثال للسياسة.

هناك العديد من الانواع للسياسات فهناك سياسات أمنيه عامه وتخصصيه و سياسات خاصه بالانظمه

سوف نتطرق في هذا الموضوع الى بعض الامثله للسياسات الامنيه التي قد تفيد من يقراها في انشاء سياسات امنيه للمنشأه الخاصه به

سياسات عامة :-

1- سياسة الاستخدام:-

- الهدف من السياسة : إنشاء سياسيات للحفاظ على الأجهزة والمعدات الخاصة بالمنشأة
- مجال السياسة : وهي القوانين والسياسات التي يجب على مستخدمي الشبكة الالتزام بها
- تفاصيل السياسة :-

أ- عدم الأكل أو الشرب أثناء العمل على الأجهزة لأن انسكاب احدى السوائل قد يتسبب في ضرر للجهاز.

ب-عدم استغلال موارد الشبكة في الأمور الشخصية والتي ليس لها علاقة بالعمل أمثلة :-

1. استخدام الطابعة الموجودة في الشبكة لطباعة أوراق شخصية
2. تخزين البيانات الشخصية في أجهزة العمل
3. استخدام الانترنت في رفع وتنزيل ملفات شخصية

- سياسة استخدام وتصفح الانترنت أثناء ساعات العمل على حسب احتياج العمل ويتم الإتفاق به مع الإدارة المسؤولة.
- عدم استخدام الإيميل(البريد الإليكتروني) الخاص بالعمل بالأمور التي ليست ذات صله بالأعمال الرسمية.
- كذلك عدم إستخدام منافذ الـ UPS حيث احتمالية إنتقال فيروس إلى جهاز الكمبيوتر

2- سياسة إدارة مستخدمي الشبكة :-

- الهدف من السياسة :-

إنشاء متطلبات الحماية بالنسبة لأجهزة المستخدمين

- المجال :-

تطبيق هذا على جميع أجهزة المستخدمين المتصلة بالشبكة والمتعلق بالعمل بناءً على هذه السياسة يتم تحديد المسموح والممنوع لكل موظف من موظفين المنشأة بناءً على القسم التابع له ومنصبة واحتياج العمل.

- تفاصيل السياسة :-

1. الملفات الموجودة على الشبكة المسموح بالدخول إليها وغير المسموح بالدخول إليها.
2. يسمح للمستخدم العمل على الأنظمة والتطبيقات الموجودة في الجهاز.
3. عدم تثبيت اي برنامج أو نظام بما في ذلك المجانية دون الحصول على أذن من قسم أمن المعلومات وتقنية المعلومات .
4. على المستخدمين الحفاظ على كلمة السر والامتثال الكامل لسياسة كلمة المرور (وهذا ينطبق أيضاً على حسابات البريد الإليكتروني) .
5. يجب تعطيل الأجهزة الموجودة على جهاز المستخدم مثل (Flopy (Removable Disk–USB–DVD–CD–Disk
6. صيانة الأجهزة للكمبيوتر ونقلها من الشبكة يجب ان يكون مقيد من أمن المعلومات وتقنية المعلومات
7. لا يسمح بتغيير إعدادات نظام التشغيل
8. لا يحتوي النظام الخاص بأجهزة المستخدمين على اي حسابات محلية أخرى.

3- سياسة الحماية :-

- بيان السياسة :-

هي التي يتم فيها تحديد السياسة الأمنية التي سوف يتم اتباعها داخل أجهزة الشبكة.

- الهدف :- من السياسة إنشاء معيار محدد لحماية أجهزة المنشأة
- تفاصيل السياسة :-

1. كلمة السر الخاصة بالموظفين داخل الشبكة ويجب ان تتمثل لسياسة كلمة المرور من حيث المدة الزمنية للتغيير – عدد الخانات التي تحتويها كلمة السر وأنواعها.
2. تثبيت برنامج مضاد للفيروسات على الأجهزة ويتم تحديثه دورياً.
3. توزيع الصلاحيات في داخل الشبكة على الموظفين بناءً على منصب كل موظف في الشركة والقسم التابع له.
4. اجهزة وادوات الحماية التي سوف يستخدمها في الشبكة مثل تفعيل جدار الحماية وضبط إعداداتها.
5. يجب ان يتم عمل نسخ إحتياطية للبيانات المهمة داخل المنشأة
6. تحديد الصلاحيات للدخول إلى الخادم.
7. اي تغيرات تحدث على الأجهزة للسيرفرات يجب أن تتابع من قبل قسم أمن المعلومات وتقنية المعلومات.
8. الدخول المميز للأنظمة مصرح به للـ Administrator حيث مصرح لهم بالدخول بصلاحيات كاملة.

4- سياسة أدارة الشبكة :-

- تهدف هذه السياسة بتحديد مهام تتعلق بإدارة ومراقبة الشبكة مثل :-

أ- التحديثات إنزالها (أنظمة التشغيل – مكافحة الفيروسات - التطبيقات)

ب- طرق ومواعيد الإحتفاظ بنسخ إحتياطية للبيانات الموجودة على الشبكة

ج- تحديد سياسة مراقبة الشبكة

د- توزيع مهام إدارة الشبكة على فريق مهندسي الشبكة IT .

- سياسات أمنية متخصصة:-

1- السياسة الأمنية لكلمة المرور :-

- استخدام كلمات مرور تتكون خطياً من الأحرف(أ - ي)والارقام من (صفر-9) والرموز (% , @ , & ... إلخ)
- تغيير كلمة المرور الخاصة دورياً ويمكن وضع تاريخ صلاحية محدد لكلمات المرور من قبل مدير الشبكة أو النظام بحيث تكون غير صالحة للاستخدام بعد ذلك التاريخ.
- تعطيل (إلغاء) كلمة المرور بعد ثلاث محاولات خاطئة وعادة ما يتحكم مدير النظام بذلك.
- عدم الاطلاع الغير على كلمة المرور الخاصة بك.
- لا تقوم بإستخدام كلمة المرور نفسها في عده حسابات وأنظمة مثال على ذلك (استخدام كلمة المرور نفسها للبريد الإليكتروني وللدخول إلى الشبكة الداخلية) .

2- سياسة استخدام البريد الإليكتروني :-

- عدم استخدم البريد الإلكتروني في الأمور ليست ذات صلة بالعمل
- ضغط الملفات الكبيرة الحجم قبل إرفاقها بالبريد الإليكتروني
- التأكد أن رسائل البريد الإليكتروني الصادر منك تتضمن عناوين الاتصال الخاصة بك
- التأكد ان المرفقات البريد الإليكتروني هي نفسها ما قصدتها وليس غيرها فالإهمال في ذلك قد يؤدي إلى إرسال معلومات مهمة وحساسة إلى جهات ليس لها حق في الاطلاع عليها.
- الإبلاغ عن اي خطأ ارتكبته أو بريد إليكتروني أرسلته بالخطأ أو ورد إليك بالخطأ أو استقبلته وفيه روابط غير موثوقة أو برامج ضارة

3- سياسة حماية الخوادم :-

- الهدف :-إنشاء معيار معين لحماية أجهزة السيرفرات في المنشأة.
- المجال :- تطبيق على جميع أجهزة الخوادم التي يتم تشغيلها في المنشأة
- الأصول المحمية :-هي اجهزة السيرفرات في الشبكة.
- تفاصيل السياسة :-

1. يجب تحديث أنظمة التشغيل لجميع أجهزة الخوادم
2. يجب ان يتم تنصيب برامج مكافحة الفيروسات على جميع أجهزة الخوادم وتحديثها دورياً
3. يجب ان يتم تفعيل الجدار الناري للأنظمة التشغيل في أجهزة الخوادم
4. يجب القيام بعمل نسخ إحتياطيةBackup بشكل دوري منتنظم.
5. يجب على مديري النظام بإستخدام كلمات مرور قوية معقدة لجميع أجهزة الخوادم

6. اي تغيرات تتم على أجهزة الخوادم يجب أن نتابع من قبل قسم أمن المعلومات
7. الدخول والخروج عن بعد لأجهزة الخوادم يجب ان يكون عن طريق نظام محكم
8. يجب ان يتم تزويد جميع أجهزة الخوادم بأحدث وسائل الخدمات والحماية.
9. عزل السيرفرات من أجل حمايتها عن طريق الشبكات الإفتراضية-V LAN
10. يجب ان يضع جميع اجهزة الخوادم في مكان محدد يمكن التحكم فيه (مركز البيانات)

4- سياسة حماية اجهزة المستخدمين :-

- الهدف :- هو انشاء متطلبات الحماية للأجهزة الخاصة بالمستخدمين بالمتصلة بالشبكة
- المجال :-تطبيق هذه السياسة على جميع أجهزة الخاصة بالمستخدمين المتصلة بالشبكة والمستخدمين بالعمل.
- الأصول المحمية :-هي اجهزة الكمبيوتر وللمستخدمين في الشبكة.
- تفاصيل السياسة :-
  1. تحديث نظام التشغيل لجميع الأجهزة في الشبكة
  2. استخدام برامج مكافحة الفيروسات وتحديثها في جميع أجهزة الشبكة
  3. تفعيل الجدار الناري على أنظمة التشغيل في جميع أجهزة الشبكة.
  4. صيانة أجهزة الكمبيوتر ونقلها واتصالها بالشبكة أو تحميل برنامج معين يجب أن يكون مقيد من قسم أمن المعلومات وتقنية المعلومات
  5. لا يسمح للمستخدمين بتثبيت وإزالة أي برامج للأجهزة الخاصة بهم.
  6. استخدام كلمات مرور قوية لجميع أجهزة الشبكة.

5- السياسة الأمنية لاستخدام شبكة الأنترنت :-

- التأكد من المواقع أو الصفحة المراد زيارتها على شبكة الأنترنت
- صلاحية إستخدام الإنترنت أثناء ساعات العمل بتم تحديده من قبل الإدارة العليا وحسب إحتياجات العمل.
- لا تقوم بتنزيل الصور والفيديوهات التي ليس لها علاقة بعمل المنشأة
- عدم تنزيل البرامج أو تثبيتها من الأجهزة على الأنترنت دون أذن مسبق
- أثناء استخدام الأنترنت – مستخدمي التصفحات عليهم التأكد من استخدام البروتوكول (Https) وليس (Http) عند تسجيل الدخول إلى الأنترنت
- التأكد من موثوقية مصادر الروابط المستخدمة للدخول إلى المواقع.
- لا تتخطى رقابة الشبكة للدخول إلى مواقع محجوبة

الفصل الخامس

إنشاء خطة أمنية

(Creating Security Plan)

- هناك اربع خطوات لإنشاء خطة أمنية جيدة والأربع خطوات هي :-

تقييم	Assess
خطط	Plan
نفذ	Execute
راقب	Monitor

- هذه الخطوات تفترض انه لا يوجد سياسية أمنية أو خطة أمنية مكتوبه ومنفذه على أرض الواقع
- قبل البداية بهذه الخطوات الأربعة حاول أن تقوم بالأمور التالية :-

1. استخدام الخطوات السبع لأمن جيد المذكورة في هذا الكتاب كقائمة تدقيق لأمور الأمن لديك , طبق هذه الخطوات لكل الأجهزة الموجودة في منشأتك .
2. حدد أولويات خطة العمل بناءً على احتمال وتأثير هذه المشكلة أو الفجوة .
3. حدد المخاطر بناءً على الأولويه وقرر كيف تتجنبها أو التخفيف منها.
4. حدد المصادر والمسؤوليات وقم بتنفيذ خطتك ثم راقب خطتك من أجل التأكد أنها متمثلة ومنفذه في الواقع بشكل صحيح.

• الخطوات الأربع لإنشاء خطة أمنية :-

1. الخطوةالأولى :- تقييم Assess

- مراجعة المهارات والمعارف لديك بحيث تحدد اذا كنت بحاجة إلى مساعدة أو تدريب أو مستشار خارجي.
- تحليل الحالة الأمنية الحالية للأمن في منشأتك:- استخدم احدى الطرق الآتية:-

أ- مراجعة السبع خطوات لأمن جيد المذكورة سابقاً في هذا الكتاب

ب-استخدام MBSA : وهو برنامج مجاني يقوم بفحص النظام والأنظمة على الشبكة لتحديد الإعدادات الخاطئة وتحديثات الأمن غير موجودة لديك

ج- استعن بمسؤول حماية الشبكة في منشأتك أن وجد

- حدد الاصول التي تحتاج إلى حماية مثل المعدات والبرمجيات والبيانات والوثائق وغيرة
- صنف معلوماتك اعتمادا على درجة أهميتها وحساسيتها باستخدام الآتي :-

Public	عام
Internet	داخلي
Confidential	خاص
Secret	سري

- تنبأ بالتهديدات مثل (حجب الخدمة –الإنتحال– انتهاك المعلومات – الإنكار – ضع في اعتبارك استخدام برامج لفحص التعرض لهذه التهديدات)

2. الخطوة الثانية :- خطط Plan

- تذكر ليس الهدف ان نعالج او تفادي جميع المخاطر بغض النظر عن التكلفة ولكن الهدف تقليل المخاطر إلى الحد الأدنى
- لكل مخاطره حدد كيف سوف تتجنبها أو التخفيف منها.
- قم بإنشاء خطة تحتوي على :-

أ- تحديد سياسة التي تعرف متطلبات للمنشأة والإستخدام المقبول

ب- تحتوي على إجراءات لمنع والإستجابة للحوادث الأمنية.

ج- تعكس ثقافة المنظمة

د- حدد الوقت المستغرق لتنفيذ الخطة

هـ- طرق التعامل مع خرق الأمن

3. الخطوة الثالثة :- التنفيذ Execute

- إعطاء جميع طاقم فريق العمل التدريب المختص بالأمن إذا كانت ضرورة لذلك
- عدل الخطة إذا كان هنالك ضرورة
- قم بتنفيذ الخطة

4. الخطوة الرابعة :- راقب Monitor

- البحث عن التهديدات الجديدة والمخاطر الجديدة حتى تكون مدرك لذلك وذلك يتم عن طريق الإشتراك بالنشرات الأمنية وتدريب المستخدمين
- قم بتعديل الخطة إذا حدثت تغيرات للمنشأة أو المعدات أو البرامج.
- مراجعة أعمال الصيانة قيد التنفيذ مثل :-

أ- تحديث برامج مكافحة الفيروسات

ب-تدريب موظف جديد

ج- عمل نسخة احتياطية

• الخطة الأمنية :-

-تحتوي على المواضيع الأتية :-

1- السرية والموثوقية

2- البنية التحتية للشبكة والأنظمة

3- حالة الامن الحالية

4- الأولويات

5- خطة العمل

6- تدريب المستخدمين

7- التنفيذ والامتثال لأعمال الصيانة

1- السرية والموثوقية :-

- لان هذا المستند يحتوي على معلومات أمنية هامه فهو يعتبر سري ويجب الاحتفاظ بهذا المستند بعيداً عن الأشخاص غير المصرح لهم بقراءته أو الاطلاع عليه
- يجب عدم الاحتفاظ بهذا المستند مخزن في السيرفر أو إرساله عبر الإيميل
- فقط النسخ الورقية هي المتطلب لحفظ هذا المستند.
- الأشخاص المصرح له بالاطلاع على هذا المستند يتم تحديده من الإدارة العليا

2- البنية التحتية للشبكة والأنظمة (Network And Systems):-

- نفترض ان المنشأه تحتوي على الشبكة الداخلية الآتيه :-

- أجهزة الكمبيوتر 42 جهاز كمبيوتر
- اللابتوب 8 لا بتوب
- الطابعات 5 طابعات
- الخوادم 4 سيرفر

أ- الخادم الأول :- (Active Directory – DNS – DHCP)

ب- الخادم الثاني :- (إيميل سيرفر)

ج- الخادم الثالث :- (خادم ملفات)Files Server

د- الخادم الرابع :- Database Server

- السيرفرات والعديد من الأجهزة مربوطة بكابل للإتصال بالشبكة و البقية متصلة بالوايرلسWAP .
- معظم الكمبيوترات تعمل على ويندوز 7 .

3- حالة الأمن الحالية :-

- بمعرفة الحد الأدنى لمتطلبات الأمن والحماية للأجهزة والشبكة وقائمة التدقيق التي ذكرت على عدة خطوات (سبع خطوات لأمن جيد) وإستخدام برنامج MBSA استطعنا تحديد نقاط الضعف في نظام الأمن لدينا والتي تحتاج إلى إعادة النظر فيها وإتخاذ إجراءات لمعالجتها.

برنامج مكافحة الفيروسات	Virus Protection
جدار الحماية	Firewall
التحديثات للأنظمة والبرامج	Updates
كلمات السر	Passwords
الأمن للشبكة اللاسلكية	Wireless Security
تصفح الويب	Web Browsing
الأمن المادي الفيزيائي	Physical security
النسخ الإحتياطية	Backups
برنامج الفلترة الـ SPAM	SPAM Filtering

4- الأولويات :-

- حيث تم تصنيف الأولويات على حسب المخاطر وهي بالترتيب كالآتي :-

أ- الردع للدخيل Intruder Deterrence:-

- تنصيب الجدار الناري
- تنصيب برامج مكافحة الفيروسات
- أمن الشبكات اللاسلكية
- التأكد من أن كل الأجهزة تعمل على تحديث تلقائي لآخر التحديثات
- تدريب المستخدمين وشرح السياسات

ب-منع السرقة Theft Prevention:-

- حماية أجهزة اللابتوب
- نقل السيرفرات إلى مكان محدد أمن ويغلق (Data Center)
- الحماية المادية لأجهزة الكمبيوتر واللابتوب
- جرد الأصول

ج- إدارة ومنع الكوارث Disaster Prevention :-

- انشاء سياسة للنسخ الاحيتاطي
- التأكد من النسخ الإحتياطي لبيانات المستخدم الهامه
- دورياً وبإنتظام عمل أختبارلإسترجاع النسخ الإحتياطي.

د- الأمن الداخل والسريه Internet Security :-

- إنشاء سياسة لكلمة المرور
- انشاء سياسه لحماية و الوصول للمعلومات

5- خطة العمل :

- بعد إجراءات التدقيق والتقدير للمخاطر والتهديدات ونقاط الضعف في المنشأة , تم ابتكار خطة الأمن التالية :-

1- تحديد وشراء وتنصيب جهاز جدار حمايه خارجي.

2- تفعيل الجدار الناري المدمج مع نظام ويندوز على كل اجهزة الكمبيوترات والسيرفرات.

3- تنصيب برنامج مكافحة الفيروسات على كل الأجهزة للكمبيوترو الخوادم وإعدادها بحيث تعمل تحديث تلقائي لآخر التحديثات.

4- على الشبكة اللاسلكية قم بتنفيذ ما تم ذكرة في موضوع (سبع خطوات لامن جيد) لحماية الشبكه اللاسلكيه سابقا في هذا الكتاب .

5- تحديد وشراء وتنصيب برنامج الفلترة الرسائل المزعجة
SPAM Filtering Software

6- مراجعة جميع الأجهزة والسيرافرات تعمل تحديثات تلقائية لنظام التشغيل والبرامج .

7- مراجعة النسخ الاحتياطية وإجراءات الاستعادة لها :

- عمل نسخ احتياطي كامل اسبوعياً Full Backup

- عمل نسخ احتياطي Incremental يومياً.

8- استخدام سيرفر مخصص لعمل التحديثات لأنظمة التشغيل والتطبيقات لجميع الأجهزة وذلك يتم عن طريق (WSUS) على حسب حجم والاحتياجات الأمنية للمنشأة

9- اعداد ويندوز سيرفر لتفعيل سياسة كلمة المرور

10-استبدال الكمبيوترات التي تعمل على نظام التشغيل Windows 7 الى احدث نظام تشغيل من ويندوز وهو ويندوز 10

6- تدريب المستخدمين User Training:-

- ساعتان من التدريب قد تكون كافية لمجموعات صغيرة كنتيجة لهذه التغيرات

التدريب سوف يغطي المواضيع الآتية :-

1. أهمية أمن المعلومات.
2. كلمات السر.
3. الوقاية من الفيروسات.
4. التصفح الأمن للأنترنت.
5. التحديثات لأنظمة التشغيل والبرمجيات.
6. شرح السياسات الخاصة بالمستخدمين(السابق ذكرها في الفصل السابق)
7. العواقب المترتبة على عدم الإمتثال للسياسة.
8. حماية أجهزة اللابتوب .

7- التنفيذ والامتثال لأعمال الصيانة:-

- شهرياً يتم التأكد من الآتي :-

1. النسخ الإحتياطي وإجراءات استعادة النسخ الإحتياطي بشكل جيد .
2. التأكد من تحديث كلا نظام التشغيل ومكافحة الفيروسات.
3. مسؤول حماية الشبكة عليه الإشتراك بالمنشورات الأمنية المتخصصة والمقدمة من مايكروسوفت ومزود برنامج مكافحة الفيروسات.

المراجع العربيه

1- الخطوه الاولى نحو امان الشبكات توماس, طوم (2004)
2- امن المعلومات بلغه ميسره (خالد بن سليمان و القحطاني)
جامعة الملك سعود – 2009
3- الدليل التعليمي لشبكات سيسكو – عبدالله الاسعد
4- المرجع الشامل في الشبكات (LAN) – المهندس عمار العريان
5- امن المعلومات (د ذيب بن عايض القحطاني)
مدينة الملك عبد العزيز للعلوم و التقنيه – 2015

المراجع الاجنبيه

1- وليام ستولينج (اساسيات امن الشبكات)
2- Sybex compita security+ study Guide
Seven Edition Emanelt dulaney

المراجع من شبكة الانترنت

Www.microsoft.com

www.wikipedia.org