بسم الله الرحمن الرحيم

جامعة الملك سعود
كلية علوم الحاسب والمعلومات
قسم نظم المعلومات

الورقة الثالثة

Remote Security

الأمن عن بعد

إعداد م/ مناحي حامد الطويل
425121609

إشراف د/خالد بن سليمان الغثبر

مقدمة:

سوف نتحدث في هذه الورقة عن الاتصال الشبكي عن بعد، وعن الخصائص والمخاطر الأمنية لهذه الشبكات وكيفية حمايتها عن طريق التشفير واستخدام اللوائح والسياسات الأمنية المناسبة.

الاتصال الشبكي- مشاركة الأنظمة عن بعد (نظرة أمنية):

إن النمو في الشبكات والاتصالات للأنظمة الموزعة قلص إلى حد ما الأنظمة المستقلة وأدى إلى خفض في متطلبات تشغيل الشبكات والوصول للبيانات والصيانة (ظهور فكرة الحواسيب البعيدة).

ماهوالحاسوب البعيد؟

هو عبارة عن جهاز حاسوبي أو خدمة معينة يمكن الإتصال بها عن بعد و التحكم بها عن طريق النظام وكأنها محليه ضمن الشبكه الداخلية.

المكاتب البعيدة

تستخدم هذه المكاتب عن طريق الاتصالات الشبكية أو الإنترنت لتوفير الخدمات عن بعد.

إدارة النظام:

تتم الإدارة عن طريق نظام مراقبة وتحكم وحيد لعدة أنظمه متباعدة.

الخصائص الأمنية والمخاطر المتوقعة

من أبرز خصائص الشبكات عن بعد:

- الحوسبة عن بعد وذلك عن طريق تنفيذ العمليات والحسابات الرياضية عن بعد.
- إمكانية مشاركة مجموعه من الأشخاص عن طريق الاتصال عن بعد ورؤية العرض في نفس الوقت.
- المساعدة عن بعد والدعم التقني:وذلك من خلال العمل على النظام من بعد في أماكن مختلفة بحيث تسمح للمستفيد إرسال واستقبال المعلومات بشكل آمن.

الأداء:

التحدي في هذه التقنية هو الوصول غير المنتهي لجهاز التحكم عن بعد واستغلاله في اختراق الشبكة. ولمواجهة ذلك التحدي يجب التأكد من الاتصال عن بعد بحيث يكون مصرح به وضمان وصول المعلومات بسريه ودون إختراق شبكي، لذلك يستخدم التشفير لمنع الأشخاص غير المصرح لهم من الوصول للبيانات.

مخاطر الاتصالات الشبكية :

- ضعف القوة <الطاقة الشبكية > مما يتيح للأشخاص (المصرح والغير مصرح لهم) بالتحكم في النظام
- مسح ملفات ,تركيب أنظمه ,تغيير الإعدادات والهيكلة من قبل المسئول المناوب للشبكة.
-دخول وسطاء عند التراسل.
- عدم التحقق بواسطة حساب المدير المحلي:

مما يتيح لمخترق الشبكة الصلاحيات التالية :

- *إمكانية الدخول من خدمة الطرفيات*
- *الخروج من النظام عن بعد.*
- *إدارة التعديل للملفات.*
- *أخذ القيادة وملكية الملفات والعناصر الأخرى* [9]

الأساليب الأمنية لحماية الشبكات المتباعدة:

الإرسال الآمن عن طريق المفاتيح :

- يجب فهم المفاتيح في عملية التحقق من مستخدمي النظام عن بعد (المفاتيح العمومية والخاصة).
- يجب تعريف المتصل عبر الشبكة والنقاط البعيدة.

الثغرات الأمنية المتوقعة:

عند الاتصال بحاسوب بعيد ,إذا لم تتأكد من أمن المفتاح، ولم يكن من الشخص المراد الاتصال به فإن المخاطرة تكمن في دخول شخص آخر وسيط يتمكن من رؤية المعلومات المرسلة فيما بين الطرفين وكشف اسم المستخدم وكلمة المرور ومن ثم استخدامها لعمل اتصال بالخادم عن بعد ورؤية خط السير وتدفق المعلومات من وإلى الخادم مع الطرف الآخر. [8]

استخدام التشفير:
يستخدم التشفير عند التراسل الشبكي عن بعد لتحقيق النقاط التالية:
- السرية وصحة المعلومات
- التحقق
- التواقيع الرقمية
- الشهادات (الوثائق)

خوارزميات التشفير:
يوجد نوعان لتشفير الأنظمة عن بعد:
1- المتماثل.
2- غير المتماثل.

وذلك عن طريق خوارزميات المفتاح السري (المتناسب)، خوارزميات المفتاح العمومي (غير المتناسب)، أو عن طريق خليط من بروتوكولات التشفير.

التواقيع الرقمية:
وهي أيضاً بطريقتين:
- التواقيع الرقمية مع المفاتيح العمومية
- التواقيع الرقمية مع المفاتيح الخاصة [1]

التأكد من الأمن الجوال:
الأمن عنصر أساسي في عمل الأجهزة والتطبيقات المتنقلة حيث أن توفر المعلومات يؤدي إلى زيادة في عدد الوحدات المتنقلة والعاملين عليها. ويكون الأمن عن طريق:
* التزامن الآمن باستخدام الأجهزة المكتبية.
* الأمن باستخدام المحطات العامة المتزامنة.
* الاتصال الآمن على شبكات VPN.
* الاتصال الآمن على الشبكات اللاسلكية سوياً مع دعم حلول VPN.

التحكم في الوصول للمعلومات
عند تصميم الشبكات المتباعدة يجب مراعاة الآتي:
- المستخدمين.
- المجموعات.
- القنوات.
- المدراء.
- التحكم على مستوى النهايات الطرفية.

الأمن والتقنية
لضمان أمن المعلومات هناك عدة تقنيات مستخدمة منها:
- التحكم عن بعد.
- أمن المستفيد البعيد والوكيل.
- أمن وسيلة النقل الشبكية.
- أمن الخادم.

ولعل التطبيق المتكامل للأمن لجميع هذه التقنيات هو (الحل الأمثل للمؤسسات الصغيرة ومتوسطة الحجم).

ماهي تقنية شبكات VPN الأفضل؟
استخدام الانترنت لربط أنظمة المؤسسات الصغيرة والمتوسطة الموزعة قاد إلى تحديات لأصحاب الأعمال في مكاتبهم البعيدة خصوصاً عند الاتصال عبر الأقمار.

هناك ثلاثة أمثلة لربط الشبكات مع المكاتب عن بعد:
- أنظمة قاعدة المستفيد.
- أنظمة الموردين (موقع إلى موقع).
- نظام المورد الوحيد والتكامل مع الجدر النارية.

توجد عدة طرق لبناء الأنظمة والشبكات الموزعة ولعل الأفضل في تكامل هذا البناء الذي يتيح التثبت والإدارة عن بعد وحل المشاكل, وتطبيق السياسات الأمنية على هذه المواقع ساعد على حفظ الوقت والمال على مدى التنفيذ الطويل للأنظمة.

- الفكرة الأساسية وراء الجدر النارية هو حماية حدود الشبكة المحلية من الانترنت وتقييد الوصول ,ولكن مع تقدم وأتساع الشبكة العنكبوتية والانترنت زادت التهديدات للحواسيب في المنظمات التيُتربط عن بعد مما أدى إلى وجود ثغرات أمنية في المؤسسات الصغيرة والمتوسطة.
للحد من ذلك تمتد الجدر النارية لتشمل جميع المستخدمين في الشبكة (في المكتب الرئيسي)خلف الجدار الناري (والمكاتب البعيدة)في الخارج.

السياسات الأمنية:
كما هو معلوم فإن الهدف من وضع السياسات الأمنية هو حماية وأمن معلومات المنظمة سواء كانت شبكة محلية أو عن بعد.

التحكم في السياسة:
- العبور أو عدم السماح كلياً بالاتصال بالشبكة
- قيود أكثر لدى المستفيد للمرور والاتصال بالبيانات المطلوبة.

التحقق : معظم الشبكات التي تتعامل مع المستفيدين عن بعد توفر خاصية التحقق من الحساب عند الدخول قبل الأتصال بالأنترنت أو القنوات. [6]

شكل1-[5]

إظهار السياسات الأمنية للشبكة :
الشركات الناجحة تجدها دوماً مستندة على سياسات أمنية قوية.
لايوجد لدى أي شركة، موظفين سعيدين بالسياسات المفروضة عليهم من الناحية الأمنية ولكنها مثل الحدود التي يجب عدم تجاوزها . وإليك أبرز النقاط التي يجب إتباعها:
1-الهدف من أمن الشبكات هو حماية نفس الشبكة أو الأجهزة الموجودة.
2-السياسات الأمنية لابد أن تكون مطولة ومعقدة.
3-يجب أن تكون محكمة بشكل تام.

لاتوجد طريقة معينة لصياغة السياسات الأمنية ولكنها تعد بعدة طرق , بحيث يمكن أن تعدل هذه السياسات فيما بعد.
الجنرال جورج باتون يقول :" *إن خطة جيدة إلى حد ما تنفذ الآن أفضل بكثير من خطة محكمة تنفذ الأسبوع القادم* " [3]
4-السياسات الأمنية تكتب مرة واحدة فقط.

إنشاء السياسة

السياسة الجذرية الأمنية (الأساسية) وتشمل:
- الحواسيب مقبولة الاستخدام: ويقصد بها جميع الأجهزة المستخدمة والحواسيب المكتبية والمتنقلة والخادمات.
- كلمات المرور.
- البريد الالكتروني.
- الشبكة.
- الوصول عن بعد: المخول لهم بالوصول لمعلومات
- ومواقع معينة وتحت أي أوضاع أو ظروف.
- الانترنت.

- اللاسلكية.
- الخادمات.

الأسئلة التالية قد تفيد مدراء الأمن عند دراسة أمن الأنظمة عن بعد:
-هل الوصول للبيانات عن بعد فقط للأشخاص المخول لهم بذلك؟
-هل الوصول اللاسلكي متاح.الوصول من مقاهي الانترنت.تحت أي ظروف وبأي جواز مرور؟
-ماهو العتاد والأنظمة والشبكة المستخدمة والتهيئة المطلوبة للوصول البعيد للبيانات؟
-هل ممكن الوصول من أجهزة خارج نطاق الشبكات المسموح بها أو غير المصرح بها؟
-كيفية التحقق من الشخص الذي يدخل على الملفات أو البيانات؟
-كيفية التحكم بالوصول البعيد. هل عن طريق كلمات المرور أو الأجهزة الرمزية, أم ماذا؟
-هل صلاحية الدخول تعطى لجميع الموظفين؟ أو لابد من أضافتهم عند الحاجة .وكيف يتم ذلك؟
-ماهي النشاطات المسموحة والممنوعة؟
-هل نشاط الحساب مراقب؟ .إن كان كذلك أبلغ الموظفين بذلك.
-بأي طرقا يجب على المستخدم حماية حساب الوصول عن بعد لديه؟
[3]

لماذا يعتبر تطوير السياسات الأمنية مهم؟
تكمن الأهمية في مدى قوة وحماية أجزاء المنظمة.

عملية التخطيط الأمني

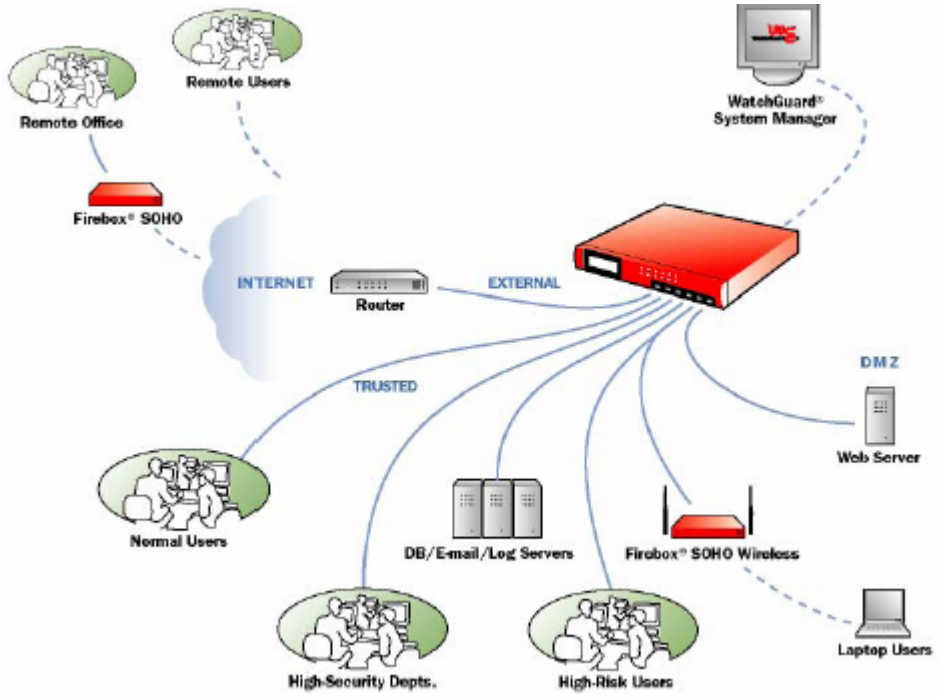
1-تطوير الفريق الأمني
2-تعريف الشفرات الأمنية
3-إنشاء السياسات والخطط لحماية الشبكة عن بعد
4-تصميم وتطوير الحلول الأمنية التي تحمي المصادر.

مفاهيم التخطيط الأمني: لابد أن تفي هذه المفاهيم بالتالي:
1-دعم الأهداف للمنظمة.
2-الأمن جزء من الإدارة الجيدة.
3-الأمن وسيلة تنظيمية جيدة.
4-التكلفة.
5-التنسيق بين أقسام المنظمة جميعها.
6- يجب أن تفحص وتراجع بشكل دوري (كل فترة).

حماية الشبكة:

1- ***الموجهات***: وهي نقطة الاتصال بالشبكات الأخرى عبر الانترنت ويجب أن تؤخذ بعين الاعتبار عند التصميم والتهيئة وبالذات من الناحية الأمنية بحيث لا يكون اسم المستخدم (أسم الحساب) أو كلمة المرور بالقيمة الافتراضية لها دوماً مما يتيح للمهاجمين فرصة الدخول.
2- ***الجدر النارية***: عند الاتصال بالانترنت من قبل الشركات, تجعل بعض المصادر والملفات متاحة للاتصال والحصول على المعلومات عن طريقها وهذا يجعل أجزاء من الشركة منفتحة.

الجدار الناري يحمي الشبكة الداخلية لدى الشركة من الهجمات المتوقعة الخارجية عبر الويب وذلك بإنشاء نقاط الحماية على حدود الشبكة وتعريف من له حق الدخول والملفات المتاحة التي يمكن الدخول عليها والاستفادة منها عن بعد.
عند اختيار الجدار الناري فإن عليك أن تضع في الحسبان حجم الشبكة وكمية المعلومات وحجم المؤسسة التي تحتاج أن تضع الحماية لها والنقاط البعيدة التي يجب المحافظة عليها.



رسم توضيحي-[5]1

ـ حماية اتصالات الشبكة
عن طريق التشفير الذي يوفر الاستفادة من الانترنت للمستخدمين المتنقلين ومكاتب الفروع المتباعدة.
ـ حماية محتويات الخادم
ـ حماية بيئة الحاسب المكتبي

العمليات والسياسات المهمة : من خلال:
-النسخ الاحتياطي والتخزين (الأرشفة) لجميع المعلومات الموزعة.
-اختبار النسخ.
-إلغاء وحجب جميع الخدمات غير الضرورية قبل الاتصال بالنظام .
-تغيير كلمات المرور تلقائياً.
-اختبار وتحديث الأنظمة عند وجود أخطاء جديدة.
-التشفير.
-اختبار أجهزة الشبكة المضافة والحديثة.
-عدم إعطاء كلمات المرور عبر الهاتف.
-إنشاء كلمات مرور أكثر أماناً. [7]

زيادة أمن الشبكات من خلال الفحص الأوتوماتيكي :
حماية الشبكة بواسطة:1-الجدر النارية
2-برامج مكافحة الفيروسات
3-أنظمة اكتشاف التطفل
4- VA: وهذه الأجهزة تعمل لفحص أمن النظام من خلال الأخطاء والثغرات التي قد تكون مدخلاً للمهاجمين لاختراق النظام والنظر إليه من زاوية المهاجمين لاكتشاف نقاط الضعف فيه.
أهمية الفحص الأمني:
تكمن أهمية الفحص للأسباب التالية:
- تزايد جرائم الانترنت
-التنظيمات الجديدة تفرض وجود معايير أمنية أعلى .
- تزايد هجمات المهاجمين والمتطفلين.

فوائد الفحص الأوتوماتيكي:

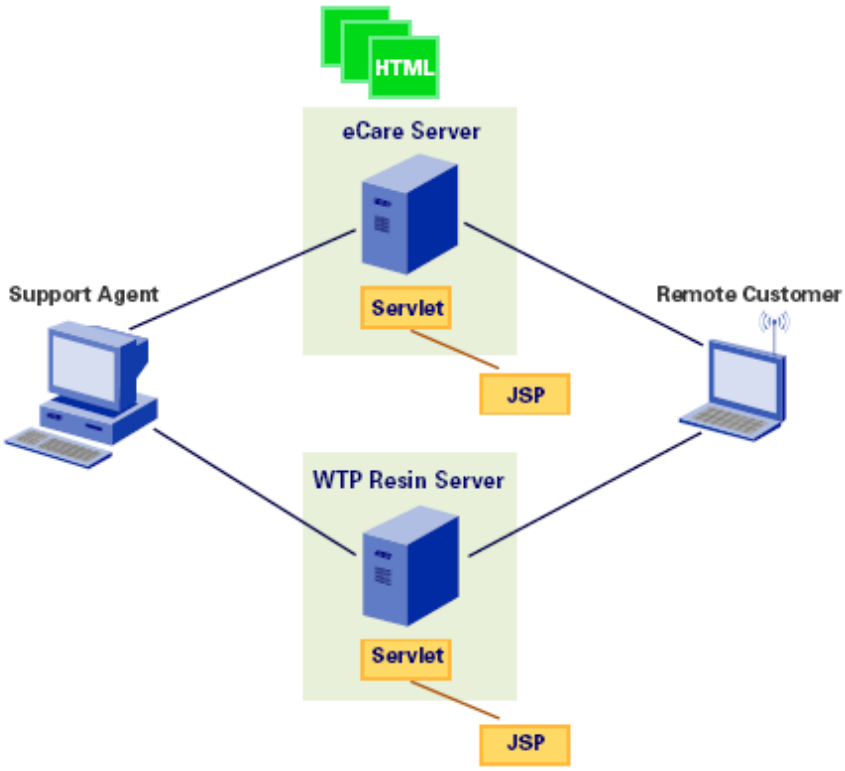
-زيادة الأدوات الأمنية الشبكية
-سرعة معالجة الثغرات الأمنية
-خفض التكلفة التشغيلية
-تقليل الأخطاء البشرية
-إمكانية زيادة وأتساع الشبكة وتمديدها(زيادة النقاط عن بعد).
-عدم الحاجة لزيادة العتاد أو البرامج.

فاحصات أمن الشبكة:

برامج ترسل البيانات إلى الشبكة ومن ثم تستمع وتتتبع الاستجابة أثناء الفحص. إن وجد أي ثغرة تشعر بها في تقرير وتبين الأجراء المتبع.

فوائدها:

-زيادة فاعلية الجدر النارية وأنظمة مكافحة الفيروسات واكتشاف التطفل
-إصلاح المشاكل بسرعة من خلال جدولة الثغرات وحلها حسب أهميتها
-خفض التكاليف وإدارة الرقع
-تقليل الأخطاء البشرية بمضاعفة الفحص
-إمكانية التمدد الشبكي لأي حجم
-البساطة في التركيب والتعامل [2]



رسم توضيحي[4]2

تطوير الوصول عن بعد للبيانات

في السابق كان الوصول إلى بيانات كبيرة نسبياً يتطلب الأتصال مع الحاسوب المركزي ولكنها كانت مقصورة على عدد مستخدمين محدود, ومع تطور التقنيات والحواسيب الشخصية أصبح بالإمكان الوصول إلى البيانات عن بعد وبشكل ميسر, ولعل تطور الشبكات والأنظمة الموزعة ساعد في ذلك.

اختيار نظام الوصول عن بعد

1-الشفافية بحيث يتصل المستخدم بالبيانات البعيدة وكأنه محلياً على حاسوبه الشخصي
2-فن الرسم البياني : والمشكلة في هذه النقطة عند عدم إسترجاع الرسومات من الناحية الأمنية
3-التكلفة

الأمن: عن طريق الآتي:
1-منع المستخدمين غير المصرح لهم (نظام التحقق من كلمات المرور)من قراءة أو الوصول للبيانات.
2- نظام الحواسيب الموثقة: عن طريق التأكد من عنوان المتصل أنه مسجل في نظام الوصول وقادم من طالب خدمة معروف وهذا يقودنا إلى مفهوم الخادمات الموثوقة عند صعوبة تتبع كل عنوان بحيث يتصل كل مستخدم إلى هذا الخادم عن طريق "وثوق مرئي", على أية حال فإنه يستلزم خادم مستقل مع صعوبة في الإدارة.
3-حجب المعلومات عن المتطفلين.
4-(السرية): -فحص المخرجات
-الحد من الوصول للمصدر
-التأكد من سلامة المعلومات وعدم تعديلها.

دعم نظام الوصول عن بعد
1-المصادر البشرية : -تحضير وتجهيز البيانات
-الدعم التقني
-دعم الأبحاث
-إستنتاج المتغيرات
2-الشبكة والأشتراك :-قوائم الرسائل
-المواقع
-المؤتمرات
-لجنة القيادة (التوجيه)

الخاتمة:
التهديدات الأمنية للأنظمة الموزعة متعددة، فمن الضروري حماية قنوات الاتصال والواجهات لأي نظام يحمل معلومات ممكن أن تكون موضع هجوم. البريد الشخصي، التجارة الإلكترونية والإجراءات المالية الأخرى أمثلة على تلك المعلومات. لذا فإن اللوائح الأمنية تصمم بحذر من أجل الحماية بحيث يبدأ تصميم الأنظمة الآمنة من قائمة التهديدات والافتراضات لأسوأ الأحوال والاحتمالات.
تعتمد الطرق الأمنية عن بعد على تشفير المفتاح الخصوصي والعمومي، ولذلك فإن خوارزميات التشفير تشفر الرسائل بطريقة لا يمكن فكها دون معرفة مفتاح فك التشفير.[1]

الهدف هو حماية كلمات المرور والبيانات من إرسالها بشكل واضح عبر الشبكة، بالإضافة إلى استخدام التشفير فإنه يوفر طريقة للتحقق من كلا المستخدم والمضيف وكيف أن المفاتيح تؤمن إنشاء خط اتصال آمن.[8]

أدوات وآليات أمن الشبكات أمثلة لفحص المخاطر والفوائد للأنظمة عن بعد ولذا يجب أن تقارن المنظمات باستمرار بين سهولة الاستخدام وقوة تلك التقنيات. [9]

References:

[1] G. Coulouris, J. Dollimore, T. Kindberg, *"Distributed Systems Concepts & Design"*, third edition, 2001, ch 7.
[2] Watchguard company, www.watchguard.com, *web-based vulnerability assessment, stronger network security through automated audits*, September 2003.
[3] Watchguard company, www.watchguard.com, *producing your network security policy*, October 2004.
[4] Netopia corporation, www.netopia.com, *Security & Technology overview*, Netopia. Inc.
[5] Watchguard company, www.watchguard.com, *The Integrated security appliance, the best solution for small to-mid sized enterprises*, March 2004.
[6] Watchguard company, www.watchguard.com, *defending the remote office: which VPN technology is best?* August 2004.
[7] Watchguard company, www.watchguard.com, *a practical guide for better security*, July 2004.
[8]Vandyke company, *Understanding Secure Shell Host keys*, white paper Vandyke software, www.Vandyke.com
[9]R. Humphrey, *Netmeeting 3.01 Remote Desktop Sharing: Security Concerns*, SANS 2003, SANS GIAC Practical paper, Assignment V1.4b Option1, may 20, 2003.