Peer-to-Peer Security

قبل أن أبدأ في موضوعي وهو أمن ال p2p هناك سؤال يقول .... ماهي ال ب2ب ؟
هي الشبكة التي يتم من خلالها تبادل الملفات بين أكثر من جهاز دون أن يكون هناك سيرفر ... وبالتالي فإن كل جهاز في الشبكة يزود غيره بالمعلومات ويطلب المعلومات بمعنى ان كل الأجهزه لها حقوق متساوية وكل جهاز فيها مزودا للمعلومات أو طالبا لها .
هناك برامج عديدة تعمل بطريقة ال p2p والتي تسمح بتبادل الملفات بين الأجهزه ... ومنها على سبيل المثال kazaa , napster , guntella , blubester
وهناك ايضا مايسمى بال Instant Messeging وهي البرامج التي تسمح للمحادثة بين شخصين أو اكثر اونلاين وقد يتعدى بعضها ذلك بأن يكون مجال للتحدث ومبادلة الملفات في نفس الوقت , ومن امثلتها yahoo messenger وهناك ايضا MSN messenger
كما أن تطبيقات مشاركة الملفات التي ذكرنا بعضها سابقا تختلف طريقة عملها من برنامج لاخر .. ففي napster انت بحاجة للاتصال قبل ذلك بسيرفر مركزي الذي يربط بين جهازين وتقوم بوضع فهرس يضم جميع الملفات التي تريد أن تشارك بها غيرك ... وبالتالي تكون المشاركة على هذه الملفات المختارة فقط ..
أما في guntella فلإن الاتصال بين شخص واخر عبر الانترنت ويكون تشارك الملفات على دراية منهم خطوة بخطوة فكل واحد منهم يحدد الملف الذي يريد مشاركة الجهاز الاخر به ويتم ذلك ..

لعلنا بعد هذه المقدمة البسيطة قد تبين لنا لماذا ال p2p خطرة .. وذلك لانها تسمح بتشارك الملفات وبالتالي فإنه من المحتمل أن يكون من بين تلك البرامج الفيروسات وال تروجن هورس ... بل انه من الممكن ان يتسلل جهاز لاخر والى الهارديسك له من خلال هذه البرامج ... لعلنا في الجزء القادم نحيط ببعض المخاطر الأمنية التي ممكن أن تتسبب بها ال p2p:

- تبادل الملفات التي من ضمنها الفيديو والموسيقى تسبب القلق لشركات ال hostin فمثلا في الجامعات هناك العديد من المستخدمين الذين يريدون تبادل ملفات الفيديو والموسيقى ولكن في نفس الوقت ليس لديهم برامج حماية ومضادات للفيروسات فيقعون في الكثير من المشاكل جراء ذلك ...

- في ال p2p يكون استهلاك ال bandwith عاليا جدا . واحتمالية ان يؤدي بذلك الى dos قليل , ولكن ذلك يؤدي الى صعوبة عمل المراقبة للأجهزة وخصوصا في المنظمات الكبرى كالجامعات مثلا

- الكثير من تطبيقات ال p2p لاتقتصر الملفات المتبادلة من خلالها على الموسيقى والفيديو . ومن هنا يمكن للمهاجم ان يرسل الفايروسات والتروجن هورس , والتي يمكن من خلالها عمل الكثير من الأعمال غير المشروعة للجهاز الضحية .

- كثير من الموظفين في الشركات يحبون هذه البرامج لكي يتبادلوا ملفات الموسيقى وبالتالي يكون هناك كم هائل للميقابايتس عبر الشبكة مما يؤدي الى ضعفها وقد يؤدي الى صعوبة خدمة الاطراف الاخرين في الشبكة والذين هم خارج الشبكة والعديد من المشاكل الأخرى

- وبما أن الكلام اصبح للموظفين في الشركات ... فانه من الممكن ايضا تسرب معلومات الشركة عن طريق هؤلاء الموظفين المشركين في تطبيقات ال p2p .

-

كان هذا فيما يخص برامج مشاركة الملفات أما الان فسنستعرض بعض الاخطار للنوع الاخر الذي يعد من ال p2p وهو instant messaging ومن الأخطار المحتملة ..

- بما ان بما ان الطريقة التي يتحدثون بها هي نص عادي بدون تشفير له فلإنه من الممكن أن يتجسس أحد على المحادثة وأن يقرأ مايكتب في جميع الجهازين .

- غالبا مثل هذه المحادثات تكون مع اشخاص يعرف بعضهم البعض ولكن في بعض الحالات تكون مع أشخاص غير معروفين ولذلك يجب الحذر من هذه المحادثات مع الأشخاص الذين لانعرف ماهي نوايا

- هناك بعض التطبيقات للIM تسمح للمستخدمين بتبادل الملفات وبالتالي تبادل ال IP مما يضاعف فرصة حدوث الخطر .
- أغلب برامج المحادثة المنتشرة عبر الانترنت هي بالحقيقة غير امنة لان بعضها تكون من اشخاص غير موثوقين وبالتالي الاطلاع على جميع المحادثات ..
-

وهناك مثال من الواقع يبين كيفية السوء الذي يحصل عندما تخدم شبكة ال p2p منظمة كبيرة جدا حصل مع احد الجامعات وهي جامعة بنيديكت والحاصل ان اكثر طلاب الكليات لايعلمون الفكرة في كيفية تقديم الخدمات فهم يستمعون الى الموسيقى عن طريق نابستر وكل الذي يعلمونه ان لديهم شبكة انترنت سريعة ..فقد كانوا يستخدمون حوالي ال 35 % من الباندويث .. وقد ادى السيل الكبير من الام بي ثري الى توقف مصادر النظام ... واصبح التحكم بذلك النظام في غاية الصعوبة ..كما حصل ضعف واضح في الشبكة ... ولكن تم اغلاق العديد من البورتس من قبل نابستر , وبدلا من محاربة ال ب2ب فقد قامت الجامعة بوضع حد معين للباندويث المستخدم في هذه البرامج . يقول كوينق مدير قسم تقنيه المعلومالت في نفس الجامعة ((الان نابستر لاتسمح للطلاب بأخذ اكثر من 5% من الباندويث ... وهي كمية تسمح لهم الاستمتاع بالتطبيقات دون أن يظر شبكتنا بضرر بالغ))

يأتي السؤال الان .... كيف اتخلص من أخطار مشاركة الملفات أو من أخطار تطبيقات ال p2p عامة ... طبعا لاأستطيع ان أتخلص من هذه الأخطار 100% ولكن كيف أقلل منها ... بالرغم من أن هناك نصيحة دائم ماتتردد بين مستخدمي ال p2p وهي ((أجعل جهاز خاص لتطبيقات ال p2p ولا تجعل في هذا الجهاز ملفات هامة)) وهذه المقولة ان دلت على شي فإنها تدل على خطر ال p2p ... مع العلم ان هذه النصائح ليست خاصة ببرنامج واحد لان كل برنامج له خاصياته وصفاته ولكن بشكل عام :

اولا نبدأ بالنصائح العامة ... والتي هي استخدام البرامج المضادة للفايروسات وتحديثها بإستمرار لكي تقوم بكشف الفايروسات الحاصلة عن طريق تطبيقات ال p2p والتخلص منها . وكذلك استخدام ال firewalls

ثانيا الخاصة بال p2p :
- في حالة مشاركة الملفات ... وعند وضع الفهرس الخاص بالملفات التي سوف تشارك بها تأكد من ان اختيار هذه الملفات يكون بشكل دقيق فهناك ملفات خاصة لاتريد ان يطلع احد عليها ... فلا تشارك بجميع ملفاتك وانما بالملفات التي تحتاج اليها .. كما لاتقوم بتحميل أي شيء الا بعد التأكد من صحته وذلك يكون ببرامج الكشف عن الفايروسات وغيرها فالقاعده تقول
Scan everything but Don’t shar everything
- اجعل برنامجك يدعم موافقتك قبل ان تحمل البرنامج وهنا تكون الفائدة عندما يكون جهاز مصابا بفايروس وينتقل الفايروس لك اليا من الجهاز ...
- تأكد بأن لايدار أي شيء اليا .. اجعل موافقتك تكون في كل شيء حتى لايستلم الجهاز الفايروسات وغيرها .
-على الأقل في الشركات الكبيرة والمنظمات الكبيرى حاول قدر المستطاع عدم استخدام تطبيقات ال p2p لما تسببه من ظغط للشبكة .
- في برامج ال IM دائما لاتقوم باعطاء ايا كان الباسوورد لكي لا يستخدمه بشيء سيء .
كما لاتقوم بالتحدث الا مع اشخاص تعرف نواياهم وتعرف من هم وماذا يريدون . لكي لايقومون بايذاء جهازك كما تحقق قبل ان تستقبل أي ملف من خلالها عن ماهية هذا الملف .

المراجع

كتاب Bible (network security)
http://cnscenter.future.co.kr/hot-topic/p2p.html
ومن هذا الموقع السابق يوجد عدة روابط عن ال p2p security استخدمتها .
http://infosecuritymag.techtarget.com/articles/february01/cover.shtml
http://www.pcmag.com/article2/0,1895,1472775,00.asp
http://www.extremetech.com/article2/0,3973,23565,00.asp
http://netsecurity.about.com/od/secureyourcomputer/a/aa093004.htm

كتبه .... هشام صالح الناصر 423100823