شبكات ال"بير 2 بير" والمخاطر المحدقة بمؤسساتكم

Brian Wilson الكاتب
CCNA, CSE, CCAI, MCP, Network+
Slimjim100@gmail.com
http://anti-hacker.info
www.middlegeorgia.org
Translated by medfox2010@hotmail.com ترجمة

قد يكون معظمنا سمع عن شبكات و خدمات "البي 2 بي" مثل " كازا" و "اليموير" ، ولكن ما لا نفكر به هو ان المؤسسات هي المسؤولة عن انشطة شبكاتها . عندما يستخدم الموظف ، البائع أو الزبون شبكة مؤسساتكم ، هل تعلمون حقا مادا يفعلون ؟ حسنا ، بالنسبة للمؤسسات مثل الفنادق ، مقاهي الانترنت أو اماكن استخدام الشبكة للعامة عموما ، فان نسبة اساءة استخدام الشبكة تكون عالية . لدلك فأنت تحتاج الى تقييد بعض الاستخدامات والى سوف تجد نفسك عرضة لانهاء خدمتك من طرف مزود خدمة الانترنت أو اسوأ من دلك تتلقى دعوى قضائية من طرف المصالح المختصة . بالنسبة لبقية اصحاب المؤسسات ربما تودون معرفة مخاطر التراخي بخصوص امن الشبكة والتكلفة الحقيقية لدلك . قد يرغب موظفوا مؤسستكم في تصفح الانترنت في اي وقت من اوقات اليوم ، المسألة سوف تكون آمنة ادا كنتم تفلترون المواقع ، ولكن بعض المشاكل التي تحصل من خلال تصفح الانترنت من العمل ، هي عندما يقوم الموظف بتحميل او تركيب برمجية المشاركة المعروفة ب "البير 2 بير" ، المعظلة الكبرى هنا هو ان اكثر من 80 بالمائة من محتوى هدا النوع من البرامج المستظافة على الحواسيب يكون مسروق حقوق الطبع أو عبارة عن فيروسات . هدا يعني أ نه ادا علم صاحب المحتوى الحقيقي بدلك فمؤسستكم تعتبر هي المسؤولة عن السرقة ناهيك عن مخاطر الفيروسات و برمجيات "التروجان" التي تخرب بيانات مؤسستكم .

لدلك فالخطوة الأولى لحماية مؤسستكم من المسؤولية هي معرفة هده المخاطر ، فمعظم المؤسسات التي تجاوزت هده المسألة تقوم ب"فلترة" المواقع ، تأمين الشبكة و كدلك تدريب الموظفين . من الأمور التي يمكن ان تفعلها كدلك ، هوالتأكدمن تركيب جدار ناري أو ما يعرف ب " الفايروول" ومعرفة المنافد التي يستخدمها برنامج "البير 2 بير" بعد دلك تكون على الطريق الصحيح لوقف البرنامج .

سوف أورد هنا قائمة لأكثربرامج و شبكات "البير2بير" شعبية ، لدلك فالفنادق ، مقاهي الانترنت واماكن الاتصال اللاسلكية العامة وغيرها يجب ان تغلق هده المنافد كي يتجنبوا مشاكل حقوق الطبع الناتجة عن استخدام اتصالهم بالانترنت :

البرنامج * BearShare, Mopheus, Limewire, Gnutella
المنفد 6346 and 6347 TCP, UDP
* Kazza, Grokster
1214 TCP, UDP
* Autonp, BeNapster
6699 TCP
* Napster, Duskter, Gnap
6700 TCP
* Inapster, Jnap, WinMX
6701 TCP
* Edonkey
4661, 4662, 4665 TCP, UDP
* iMesh

4329 TCP

القائمة أعلاه هي مجرد بعض برامج ومنافد ال"بير 2 بير" ، لدلك فانه يوصى دائما باستشارة مزود الخدمة لضمان تزويدكم باحدث البرمجيات والبرامج قصد حماية مؤسستكم . بالاضافة الى اغلاق المنافد هناك امور أخرى تستطيع القيام بها منها : ان تفرض سياسة استخدام الشبكة على جميع المستخدمين و تقوم بتحديث جميع برمجيات حماية شبكتك (من مضادات الفيروسات و ملفات التجسس و موقف الاعلانات "اد بلوكرز") ، وكدلك ان تقوم بتدريب المستخدمين على اخطار الانترنت .

من أبرز الاخطار التي تواجه شبكات المؤسسات هي التي تأتي من المستخدمين انفسهم ، لدلك فالوسيلة الوحيدة لضمان أمن شبكتك هو التأكد من معرفتهم التامة بقانون الشبكة . لدلك فعندما يدرك مستخدموا شبكتك اخطار الانترنت ومسؤوليتهم التامة كمستخدمين ، فعند ئدن فقط تكون أقرب الى مكان عمل رقمي آمن . فمعظم شبكات الارشاد المحلية عادة تقدم ما ناقشناه آنفا وربما تحتاج الى اتخاد خطوات اضافية لتلبية احتياجات عمل مؤسستك . فمع HIPPA& Sorbian Oxley ليس هناك ما يدعوالى الخوف من تحمل مسؤولية شبكة شركتكم ، فكما نراه دائما فالاعلام فالمؤسسات تدرس الصعوبات بخصوص المسؤولبات المشتركة .