Тема 20. Планиране на политиката за мрежова сигурност

Политиката за мрежова сигурност включва редица административни, организационни и технически мероприятия.

Административните мероприятия се отнасят до:

- подбор на персонала – при назначаване на нови служители и при промяна на йерархията трябва да се вземе под внимание и риска от злонамерени действия на служителите;
- административни нареждания – забрана за инсталиране на програмни продукти; съгласие и информираност за работа с конфиденциална информация; забрана за изнасяне на файлове с документи и други данни.

Организационните мероприятия включват:

- създаване на документи с правила за инсталиране на компютърните системи, правила за полагане на кабелните системи на локалната мрежа;
- създаване на длъжностни характеристики на служителите в частта им за работата с компютърни системи и електронни документи.

Техническите мероприятия включват:

- въвеждане на нива на сигурност на операционната система;
- политика за използване на паролите;
- криптиране на файловете;
- използване на цифрови подписи;
- използване на протоколи за сигурност при предаване на данните по мрежата;
- използване на защитни стени и прокси сървъри;
- спазване на правилата за антивирусна защита;
- физическа сигурност на данните.

Политиката за мрежова сигурност изисква използване на комбинирани методи за сигурност.

Мрежов администратор

Функционирането на система за информационна сигурност без компетентен компютърен специалист е невъзможно. При изпълнение на служебните си задължения той има достъп до цялата информация във фирмата. Всяко съмнение в добронамерeността на администратора е заплаха за мрежовата сигурност.

Забрана за инсталиране на програмни продукти на работното място

Произволното инсталиране на безплатен и условно безплатен софтуер носи рискове в сигурността на системата. Посещенията и свалянето на софтуер от различни сайтове е опасно, много често свалените файлове и дори скриптовете в сайтовете съдържат злонамерен код. Особено внимание трябва да се отдели на Active-X компонентите, които обикновеният потребител може да инсталира. Те могат да включват освен обявените функции и програми от тип „задна врата”. Много от Active-X програмите, скриптовете, безплатните програми изпращат информация от компютъра на който са стартирани, като интерес представляват примерно e-mail

адресите, собствения и тези, с които потребителят контактува. Препоръчва се инсталирането на Active-X компонентите да бъде забранено със средствата на браузера, за всички сайтове извън описаните в списъка „Доверени сайтове". Свалянето от Интернет на програми и инсталирането от потребителите без разрешение на мрежовия администратор на какъвто и да е софтуер, трябва да бъде категорично забранено.

Нива на сигурност на операционната система

Съвременните операционни системи с файлова система NTFS позволяват въвеждане на нива на сигурност. Всеки потребител притежава собствен акаунт с парола за достъп. *Акаунтът се състои от потребителско име и параметри за влизане в мрежата, зададени за конкретния потребител.* Тази информация се въвежда от администратора и се съхранява в мрежата от операционната система. За всеки потребител се задават:

- права за достъп до системата и нейните ресурси;
- време за влизане;
- потребителска директория;
- дата на изтичане.

Важен момент при задаването на тези настройки е дефинирането за всеки акаунт на достъпа до ресурсите на системата!

Операционната система предлага ключови потребителски акаунти, които автоматично се активират по време на инсталацията.

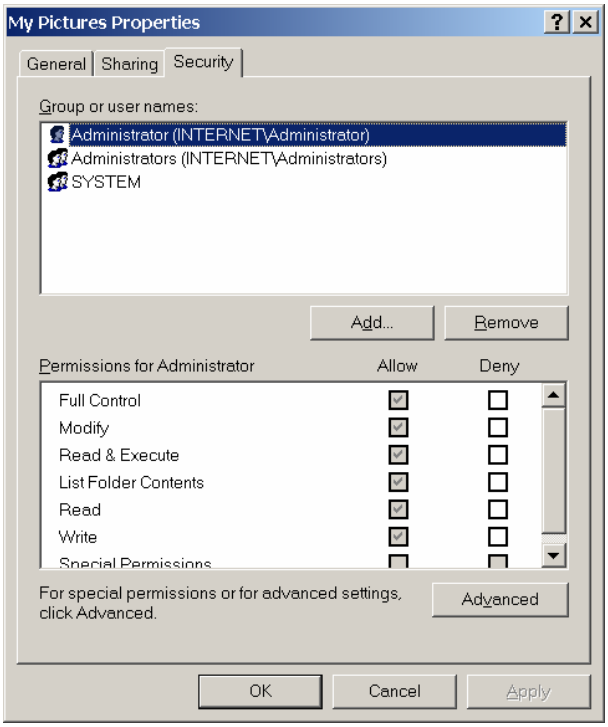
Administrator – първоначален акаунт. Той е с пълни права в мрежата и може да:

- стартира мрежата;
- инсталира файлове и програми на операционната система;
- настройва първоначалните параметри на системата за сигурност;
- създава други потребителски акаунти;
- поделя директории и принтери.

Guest – посетителски акаунт. Дава временен достъп до мрежата на някой, който няма акаунт.

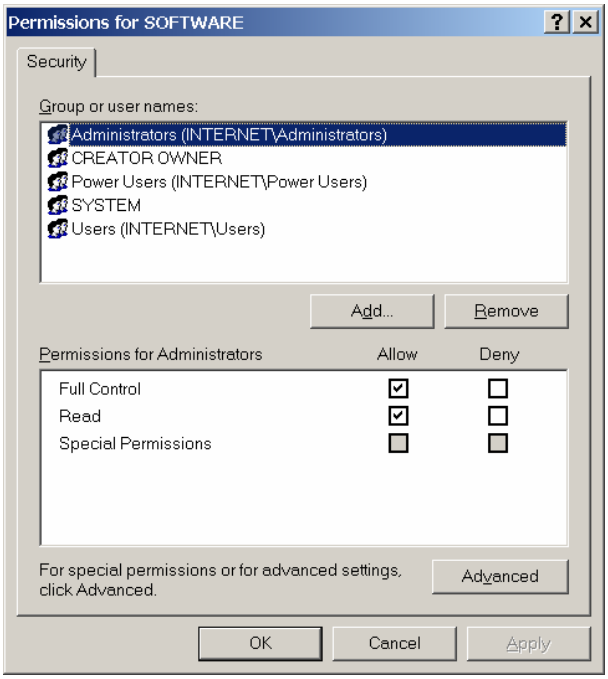
Мрежовите операционни системи могат да поддържат хиляди акаунти. Мрежовият администратор ще бъде затруднен, ако реши да извърши някакви настройки върху всички акаунти или дори само върху част от тях. Почти във всяка мрежова операционна система различни потребителски акаунти се обединяват в един общ акаунт, наречен ***група***. *Групата е акаунт, съдържащ други акаунти*. Основната причина за въвеждането на групите е улесняване на администрирането. Групата дава възможност на администратора да третира голям брой потребители като един-единствен акаунт.

Правата за достъп се настройват за групата и всичките й членове автоматично ще получат и наследят тези права. Правата за достъп за различните групи могат да бъдат различни. Така например за потребителите в *Group_1* може да бъде разрешен пълен достъп до *file1.doc* - да могат да четат, променят и съхраняват файла, но за потребителите от *Group_2* – само да четат този файл.



Фиг. 20-1. Управление на правата на групов акаунт

Освен на NTFS[1] ниво, правата за достъп до папка или файл могат да се задават и чрез ключовете в Windows Registry. Това ограничава потребителите във възможността им да инсталират програми и да ги конфигурират.



Фиг. 20-2. Управление на правата на групов акаунт в Windows Registry

Home Edition версиите на Windows XP и Windows Vista предлагат ограничено поддържане на сигурност – дефинирани са само три вида потребители: администратори, обикновени потребители и гости. Задаване на NTFS права е възможно само в режима Safe Mode.

Всяка фирма или организация трябва да изгради своя политика за контрол на достъпа до ресурсите на системата.

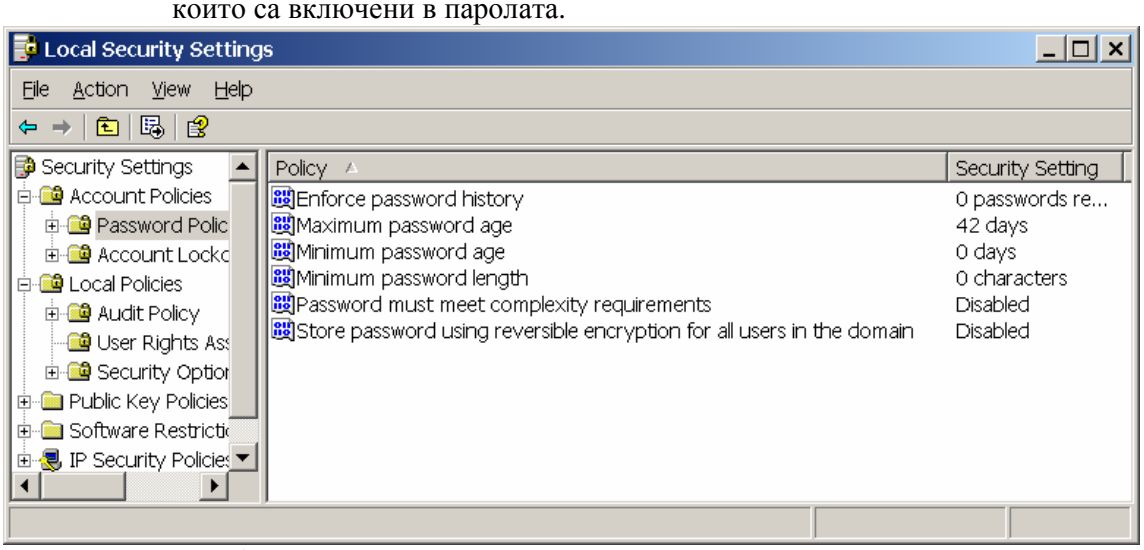
[1] NTFS - New Technology File System е файловата система използвана от Windows NT, 2000, XP, Vista

Сигурност на паролите

Важен момент от политиката за мрежова сигурност е използването на възможно по-трудни за разгадаване пароли.

Политиката за сигурност на паролите трябва да включва следното:

- Паролата не трябва да съдържа имена на роднини, рождени дати, адреси, телефони;
- Да не се използват смислени думи, които се съдържат в речниците. Комбинацията между букви и цифри е добър вариант;
- В паролата да има включени главни и малки букви на случайни позиции (например DoYspGO);
- Паролата ***трябва*** да бъде лесна за запомняне от потребителя. В противен случай тя ще бъде записана на хартия, което не е желателно;
- Да се използват дълги пароли (поне 8 символа);
- Периодично потребителите трябва да сменят паролите си;
- Съвременните операционните системи притежават възможности за задаване на правила при въвеждане на потребителските пароли – минимална дължина, история, срокове за изтичане на паролата, както и изисквания към символите, които са включени в паролата.



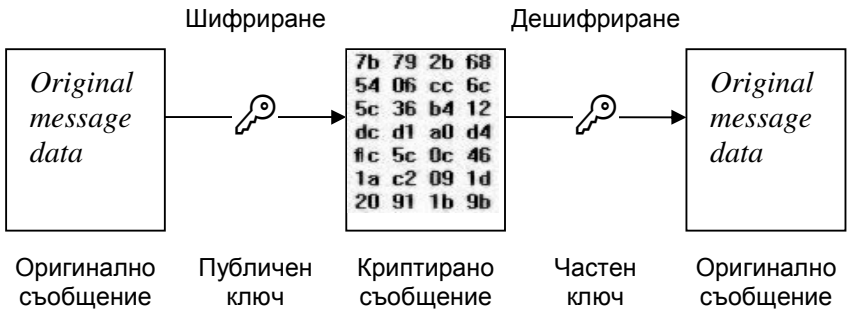
Фиг. 20-3. Конфигуриране на политика за сигурност на локална Windows система

Криптиране на файлове

Политиката за сигурност на данните във фирмата включва и засекретяване на данните чрез използване на криптографски методи.

Криптирането е процес на преобразуване на данните във форма, трудна за разбиране от другите.

При криптиране на файловете в една компютърна система единствено техният създател ще има достъп до тях. Криптирането използва код или ключ за разбъркване (шифриране) на данните и след това за тяхното подреждане (дешифриране). Разработени са програмни продукти за криптиране на информацията (писма, документи, бази от данни и др.). Те се базират на следните основни криптографски методи: криптиране с публичен ключ, криптиране със секретен ключ и др.



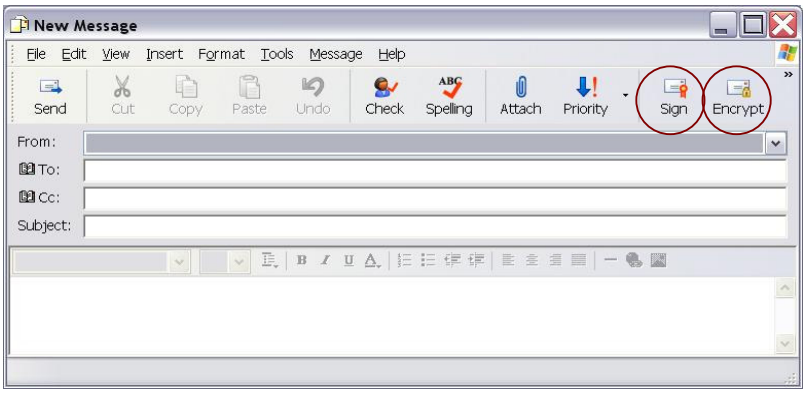
Фиг. 20-4. Използване на шифриране с публичен ключ

Цифрови подписи

Цифров подпис е наложило се в практиката наименование на използването на PKI услуги (Public Key Infrastructure) – услуги с публичен и частен ключ.

Използването на системи за криптиране със секретен ключ може да доведе до много голямо ниво на сигурност. Методът DES (Data Encryption Standard) с достатъчно дълъг ключ се използва за правителствени и военни цели. За целите на обикновените граждани достатъчно ниво на сигурност може да осигури дори криптиращата система на архиватори като WinZip и WinRar. Проблемът при такава криптирана комуникация е в доверието. Тъй като криптиращият ключ е известен и на изпращача и на получателя, и двамата могат да създадат подменено копие на данните, като по никакъв начин не е възможно да се докаже кой е направил подмяната.

Използването на PKI – услуги с публичен ключ решава този проблем. PKI извършва две действия – подписване и криптиране.



Фиг. 20-5. Изпращане на писмо с Outlook Express

За да се *подпише цифрово* писмо или документ е необходимо изпращачът да притежава електронен подпис. За изпращане на подписано писмо с Outlook Express след създаване на писмото е необходимо да се избере бутона ‘Sign’. След избор на ‘Send’ – операционната система извежда запитване за персоналния идентификационен номер (PIN) и изпраща писмото. Подписването на данните не ги ‘скрива’ от получателите. Всеки може да отвори подписан файл или писмо. Цифровото подписване гарантира:

автентичност	получателят на съобщението е сигурен, че подписващият е този, за който се представя;
цялост	съдържанието не е променено или фалшифицирано след поставяне на цифровия подпис;
неотменимост	цифровият подпис доказва съдържанието, подписалият го не може да го отрече.

Криптирането (Encrypt) от своя страна има за цел да направи съобщението тайна за всички други освен за получателя му. За да се изпраща криптирана електронна поща е необходимо получателят на писмото да има цифров подпис, а не изпращача.

В Република България поставянето на цифрови подписи е регламентирано от Закона за електронния подпис и електронния документ. Комисията за регулиране на съобщенията (КРС) регистрира доставчиците на удостоверителни услуги. Те предлагат Удостоверения за универсален електронен подпис (УУЕП), който има силата на собственоръчно поставен подпис. Останалите цифрови подписи, които се използват (например за целите на електронно банкиране) се наричан Обикновени електронни подписи и те нямат правна сила. УУЕП се признават от държавната и общинската администрации, включително Националната агенция по приходите (НАП), Националния осигурителен институт (НОИ), Агенцията по вписванията и др.

Сигурност на данните по мрежата

Данните, които пътуват по мрежата могат лесно да бъдат прихванати и прочетени от други потребители. За да се гарантира сигурност на данните изпращани по мрежата са разработени отделни програми и протоколи.

IPsec (*Internet Protocol security*) представлява набор от протоколи за защита на данните, обменяни в мрежа, с помощта на услуги за защита и цифрови сертификати с публични и частни ключове. Той работи в мрежовия слой на OSI модела и реализира сигурност на данните на ниво пакети. IPSec използва два протокола:

- *Authentication Header (AH*) – осъществява проверка на самоличността на изпращащия IPsec.
- *Encapsulating Security Payload (ESP*) – гарантира конфиденциалност на самите данни.

SSL (*Secure Sockets Layer*) е друго средство за гарантиране на сигурността на данните. Той използва криптиране с публичен и частен ключ. Работи в приложния слой на OSI модела.

Програми за защита на електронната поща

При изпращането на писма по електронната поща не се гарантира конфиденциалност. Писмата по време на своето пътуване до получателя преминават през различни сървъри. На всеки от тези сървъри може да бъде направено копие от тях. Затова са разработени програми за защита на електронната поща:

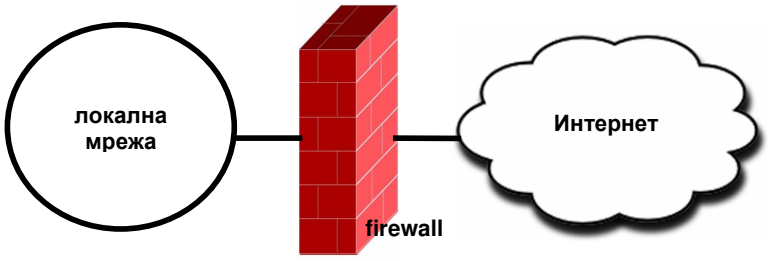
- Pretty Good Privacy
- Kerberos
- Baltimore Mail Secure и др.

Защитни стени и проксита

Важен момент от защитата на една локална мрежа е използването на ***защитна стена (firewall).*** Защитната стена се поставя между вътрешната мрежа и външния свят (Фиг. 20-6). Firewall се използва срещу злонамерени атаки от отдалечени компютри. Също така тя позволява да се регламентира и ограничи достъпа на програмите и потребителите в локалната мрежа до Интернет услуги.

Забележка:

Терминът FireWall идва от строителните норми на САЩ и не следва да се превежда дословно. FireWall са защитни, огнеупорни стени, каквито трябва да притежават сградите за възпрепятстване на пожарите. В този смисъл правилният превод е 'защитна стена'.



Фиг. 20-6
Защитна стена

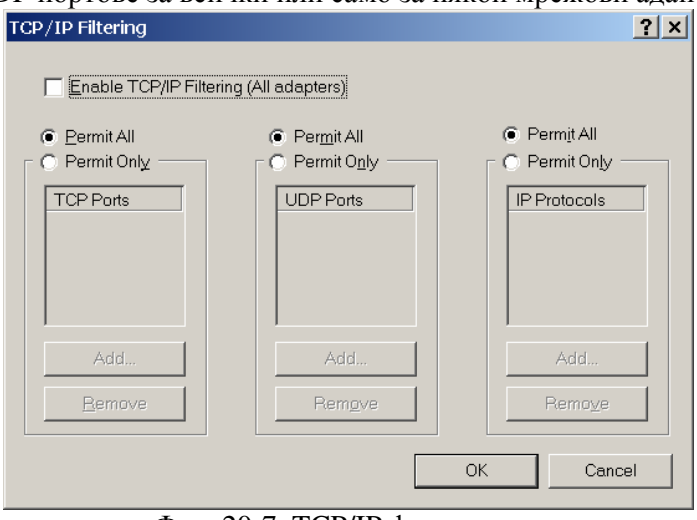
Защитната стена е програма, която следи за мрежовия трафик в двете посоки – към локалната мрежа и от локалната към външния свят. Защитата може така да бъде конфигурирана, че да позволява пропускането на някои протоколи и услуги и спирането на други. Вариантите за защита могат да бъдат два:

- разрешаване на всички услуги, с изключение на специално забранените;
- забрана на всички услуги, с изключение на специално разрешените.

Вторият вариант е за предпочитане. В този случай всички непознати протоколи се отхвърлят.

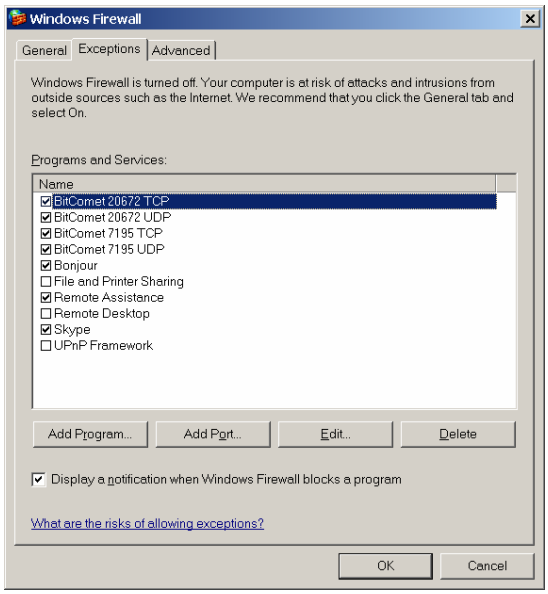
За изграждане на надеждна защитна стена е необходимо съответната програма – firewall да бъде конфигурирана правилно. Обикновено се въвеждат правила за филтриране на мрежовия трафик.

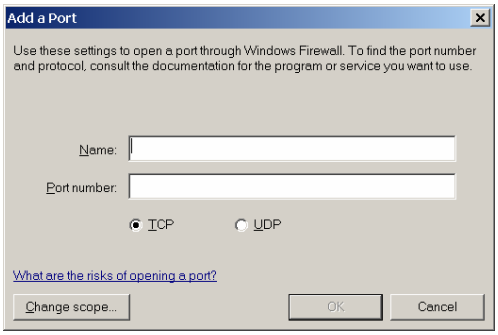
TCP/IP протоколът в Windows XP позволява филтриране. Могат да се разрешават определени TCP и UDP портове за всички или само за някои мрежови адаптери.

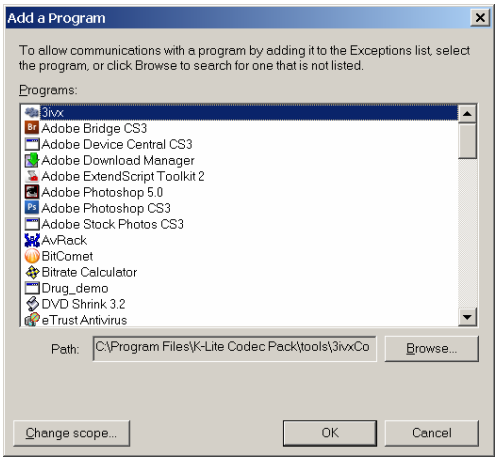


Фиг. 20-7. TCP/IP филтриране

Windows Firewall е вградена в Windows програма ‘Защитна стена’. Тя позволява разрешаване на мрежов достъп на определени програми до зададените портове. Проблем при използване на Windows Firewall е, че някои червеи и „Троянски коне” успяват да я заобиколят и да си конфигурират самостоятелно разрешение за достъп.







Фиг. 20-8. Конфигуриране на Windows Firewall

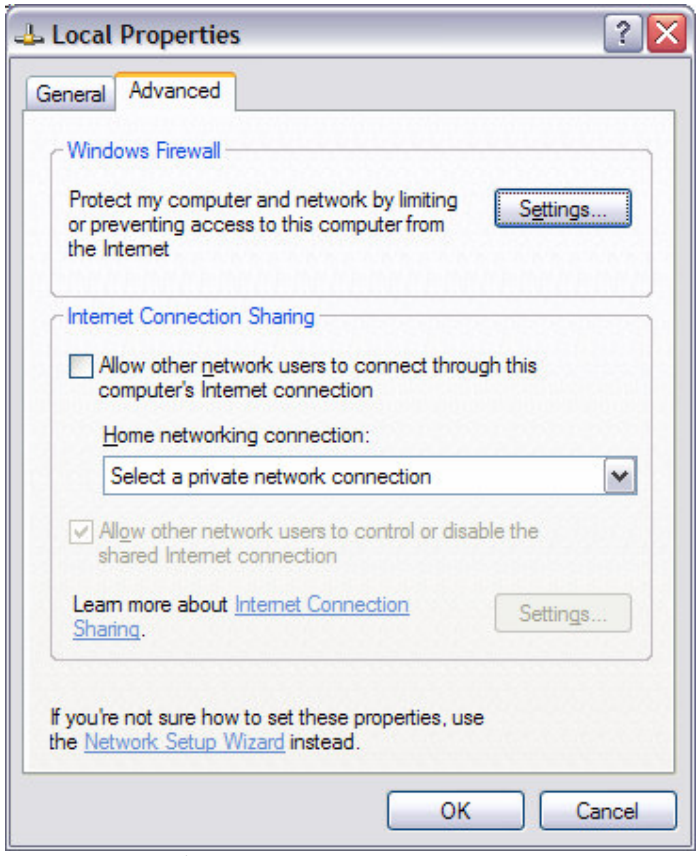
На пазара съществуват множество програми от вида ‘Защитна стена’. Те позволяват полесно администриране – по примери (By Example). При входящ или изходящ трафик те извеждат съобщение на потребителя, който може да разреши или да забрани действието, да създаде правило за забрана и разрешаване на това действие в бъдеще.

Прокси (Proxy) сървърите до преди няколко години се използваха масово за осигуряване на достъп на няколко компютъра до Интернет с една обща споделена връзка. Днес прокси сървърите продължават да намират приложение, най-вече като сървъри за филтриране на информация. Техните филтри позволяват създаване на списъци със забранените за посещение сайтове, списък на забранените ключови думи, които не могат да се съдържат в адреса (URL) или в текста на страницата, забраняват зареждането на файлове, които представляват риск в сигурността, примерно изпълними файлове, скриптове и други.

NAT

Преобразуването на мрежови адреси (Network Address Translation – NAT) е метод на споделяне на една интернет връзка за компютрите в локална мрежа. Компютрите използват като DNS сървър и gateway компютъра (или устройството) осигуряващо NAT. В локалната мрежа се използват IP адреси от частното адресно пространство. Тъй като компютрите в локалната мрежа не притежават реални IP адреси, то те са практически недостъпни от Интернет. По този начин NAT работи и като защитна стена.

Windows предлага NAT чрез функцията Internet Connection Sharing (ICS). Компютърът - ‘сървър’ има два мрежови интерфейса – един за интернет връзката и един за локалната мрежа. ICS се активира чрез свойствата на мрежовата (интернет) връзка. В страницата Internet Connection Sharing се поставя отметка на ‘Allow other user to connect through this computer’s Internet connection’.

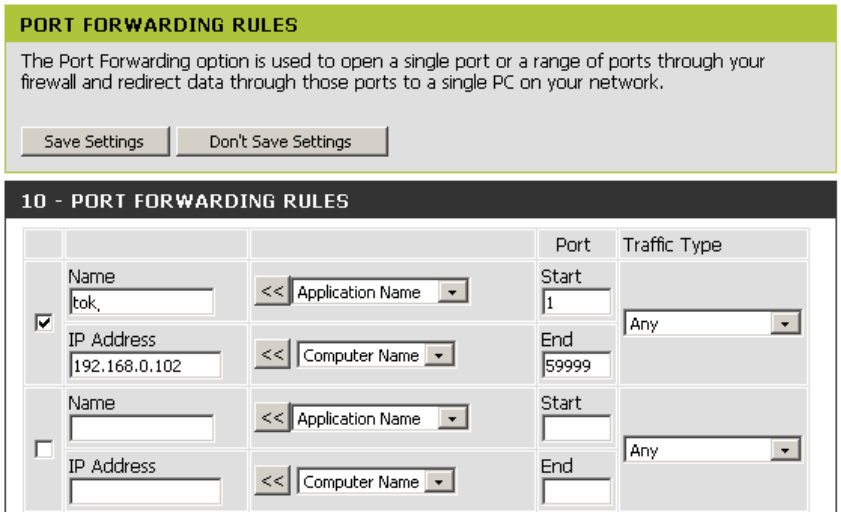


Фиг. 20-9. Конфигуриране на Internet Connection Sharing

За втория мрежов адаптер ICS назначава IP адрес, активира DNS и DHCP сървъри, които се задават чрез автоматично конфигуриране на компютрите-станции.

Използване на компютър за ‘сървър’ на споделената интернет връзка има много недостатъци. Първо, ако компютърът се използва като работно място, на неговия потребител ще се наложи да го рестартира поради някаква причина, което ще доведе до прекратяване на достъпа на останалите потребители към Интернет. Програмен или апаратен срив на компютърната система на ‘сървъра’ ще спре достъпа на потребителите в локалната мрежа. Обикновено такъв компютър се оставя включен денонощно – при това дори разходите за електрическа енергия не бива да се подценяват.

Значително по-добро решение е закупуването и инсталирането на устройство – Broadband Router – рутер за споделяне на интернет връзка. Той е самостоятелно устройство, обикновено включва 4 портов 10/100Mbps суич, в много от моделите и безжична мрежа 802.11. Рутерът е надеждно устройство, конфигурира се лесно – през WEB интерфейс. Рутерът осъществява NAT за компютрите в локалната мрежа, предлага им DNS и DHCP сървър за автоматично конфигуриране – аналогично на ICS. За разлика от него той позволява използване на произволно частно адресно пространство, а не само 192.168.0.0/24. Съществуват случаи, в които е необходимо услуга, предлагана от компютър в локалната мрежа да бъде достъпна и за интернет потребителите. Тази възможност обикновено се нарича ‘Virtual Servers’, ‘Mapped Links’ и др.



Фиг. 20-10. Конфигуриране на Broadband Router – пренасочване на портовете към локален компютър

Антивирусна защита

Интернет е рискова среда. Инсталирането на софтуер – антивирусни и анти-спам (ad-ware) програми, тяхното непрекъснато актуализиране и проверка за функционирането им е важно условие за осигуряване на информационна сигурност на работното място. Антивирусните програми спират всеки опит за стартиране на известен за тях злонамерен софтуер. В допълнение на това, анти-спам програмите спират изпълнението на много програми, които сами по себе си не са категоризирани като злонамерен софтуер. Програмите-спам не са вируси, но те генерират нежелани рекламни съобщения, например в електронната поща.

Работоспособността на тези програми трябва да се проверява. Не трябва да се забравя, че те могат да опазят компютъра само от известните им програми. Рискът от заразяване остава. Най-чести са атаките от програми от типа “троянски кон”. Те разпознават и елиминират антивирусната програма. Липсата или невъзможността за инсталиране на антивирусна програма почти винаги е доказателство за наличието на вирус.

Един от основните канали за разпространение на злонамерен софтуер е електронната поща. Най-често достъпа до служебната кореспонденция се осъществява с програмата Outlook Express. Съществуват много пропуски в програмата, открити от кракерите и използвани за инсталиране на програми тип червеи, без намесата на потребителя. Актуализирането на Windows чрез инсталация на всички service pack-ове и кръпки (patch) намалява рисковете. Много често нежеланите програми се маскират като zip архиви, картинки и други, като представят името си примерно ‘message.zip’, следвано от много интервали и накрая разширението ‘.exe’. Тъй като разширението за изпълним файл не се вижда, доверчивият потребител го стартира, отговаря на всички въпроси от Windows за неговата безопасност и се заразява.

Ако във фирма/организация има проблеми с получаване на заразени писма, е необходимо да се вземат мерки срещу това. Ако се използва собствен сървър, е необходимо да се инсталира антивирусна програма на сървъра за електронна поща. Съществуват и анти-спам програми за сървърите за електронна поща. Те използват евристични алгоритми за разпознаване на нежеланата поща. Добра идея е да се забрани категорично получаването като прикачени файлове на всички изпълними програми и скриптове.

Основни правила за антивирусна защита:

- *Не стартирайте програми, получени от несигурни източници. Проверката с антивирусна програма на всеки чужд дисков носител е задължителна*!
- *При инсталацията на пиратски софтуер винаги се подлагате на риска от заразяване!*
- *Не стартирайте .EXE файлове, получени по електронна поща, без потвърждение от изпращача!*
- *Не оставяйте дискети във флопидисковото устройство!*
- *Използвайте актуализирани антивирусни програми!*.

Физическа сигурност

При планиране на политиката за мрежова сигурност трябва да се има предвид и ограничаване на физическия достъп на външни лица до данните в мрежата. Мероприятията могат да бъдат насочени в следните направления:

Защита на кабелите срещу директен физически достъп

Мрежовите кабели трябва да бъдат положени така, че да няма възможност за физически достъп до тях. При изграждане на локална компютърна мрежа е необходимо да бъде направено т.н. структурно окабеляване. Мрежовите кабели трябва да бъдат положени в специални канали или да бъдат скрити в окачени тавани или подови настилки. Кабелите с усукани двойки проводници са особено лесни за подслушване. При оптичните кабели това е възможно, но е значително по-трудно.

Защита на компютърната система

Важен момент от сигурността на мрежата е ограничаване на физическия достъп за външни лица до компютрите и другите мрежови компоненти. Дейностите в тази насока могат да бъдат следните:

- всяко устройство да се маркира с инвентарен номер;
- да се изисква легитимиране на външните посетители, преди да бъдат допуснати до оборудването;
- работните станции и сървърите да се държат в заключващи се помещения;
- там където това не е възможно, да се въведе софтуерна защита.

Използване на технически средства за защита

- система за видеонаблюдение;
- алармена система (СОТ);
- кодови брави;
- система с персонални магнитни карти.

Въпроси

1. Кои основни действия трябва да присъстват в плана за мрежовата сигурност в една фирма?
2. Кои операционни системи допускат въвеждането на нива на сигурност за потребителски и групов акаунт?
3. Кои правила трябва да включва политиката за сигурност на паролите?
4. По какъв начин „защитната стена” защитава вътрешната мрежа?
5. Кои са основните правила за осигуряване на антивирусна защита?
6. Кои са основните моменти за осигуряване на физическа защита?