6. Защита на компютърните мрежи. Правила за поведение в Интернет

В уроци от предишни години вече сме се спирали на въпросите за защита на компютрите, и особено тези работещи в мрежа, от злонамерени действия, с помощта на средствата на ОС и антивирусните програми. В този урок ще посочим и някои други възможности. Много е важно да се разбере, че предлаганите възможности защитават компютърните системи не само от злонамерени действия, но и от такива, предизвикани от небрежност, незнание или невнимание – в този случай могат да бъдат нанесени не по-малки щети. Ще припомним и правилата на поведение при работа в Интернет, които са предназначени да ни предпазят от злонамерени действия, насочени срещу самите нас, тъй като глобалната мрежа предоставя много възможности за такива действия.

Потребителско име и парола

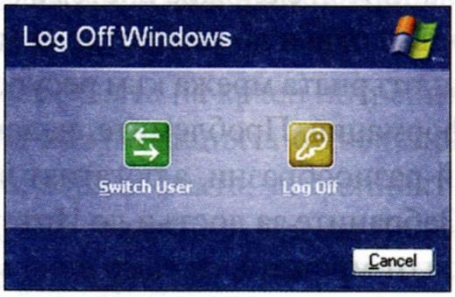
Основното средство за защита на компютърните системи, както от злонамерени действия, така и от небрежност или невнимание, е системата за регистриране на потребителите. За всеки потребител на един компютър, особено когато потребителите са много, ОС позволява да бъде създадено лично пространство в компютъра, наричано ***ъкаунт*** (англ. account, сметка – терминът е въведен още по времето, когато достъпът до компютри е бил силно ограничен и всеки потребител е трябвало да заплаща използвания от него компютърен ресурс). Всеки собственик на ъкаунт си има потребителско име (login), парола (password) и определени за него ресурси – например, дисково пространство, където да разполага файловете си.

Компютър, потребителите на който имат лични ъкаунти, при стартиране не отваря автоматично работното поле на ОС, а започва процес по ***идентификация*** на потребителя. По време на идентификацията той трябва да въведе потребителското си име и паролата, за да може да започне работа с компютъра. Ако потребителят въведе валидно потребителско име и свързаната с него парола, тогава компютърът започва ***сесия*** с потребителя, като го поставя в обичайните за работа условия и освобождава достъпа само до тези ресурси, на които потребителят има право. На *Фиг. 1* е показан диалогов прозорец на ОС Windows за започване на сесия.

Фиг. 1. Начало на сесия

Когато потребителят завърши работа с компютъра, той трябва да прекрати сесията по определения в ОС начин. В ОС Windows потребителят трябва да изпълни командата Log Off от менюто ***start*** и в диалоговия прозорец да избере Log Off (прекрати сесията), ако няма потребител, който е готов да използва компютъра веднага, или Switch User (смени потребителя), ако има такъв потребител (*Фиг. 2*).

Фактът, че по време на сесия потребителят може да използва само разрешените за неговия ъкаунт ресурси означава, например, че той няма как да изтрие чужди файлове и по този начин да навреди на работата на колегите си, не може да запълни целия диск с любимите си звукозаписи и филми, нито пък да използва направеното от друг, за да завърши без много да се труди възложения му проект по ИТ.



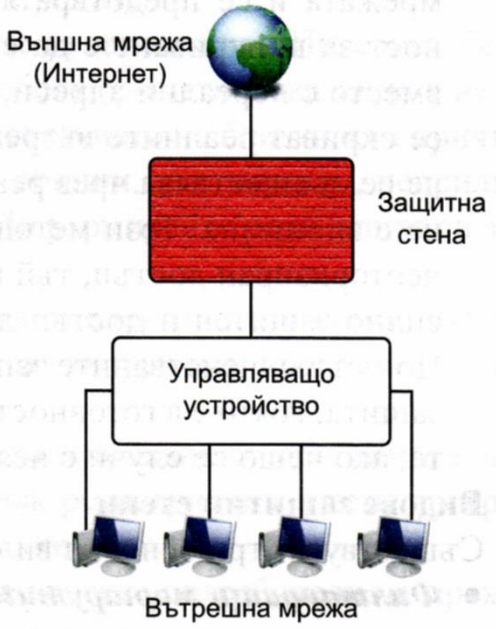
Фиг. 2. Край на сесия

Каква е практиката в момента? В много локални мрежи, всеки потребител може да влезе на всеки компютър с едно и също потребителско име и парола, например Login: one; Password: 1 – и бързо, и лесно. При това, той може да ползва целия ресурс, да изтрива безразборно файлове, да пълни диска с каквото реши, а след напускане на работното място не е нужно дори да затваря сесията – и без това следващият потребител ще използва същия ъкаунт. С такава организация на достъпа не е трудно злонамерен човек да научи използвания от твърде много потребители ъкаунт и не само да нанесе вреди на локалната мрежа, но и да влезе от нея в Интернет и безнаказано да предприеме действия, имащи дори престъпен характер.

Използването на лични ъкаунти не решава автоматично проблема. Ако потребителят не си направи парола по правилата – достатъчно дълга, с използване както на букви, така и на цифри и специални знаци, тогава паролата му лесно може да бъде разгадана. Ползата от личен ъкаунт е малка и когато потребителят напуска работното място, без да прекрати започнатата от него сесия и оставя ъкаунта си неизвестно на кого.

Защитна стена (файъруол)

Изграждането на защита от неоторизиран достъп до компютърните мрежи е свързано с редица проблеми. Необходимо е създаването на специални правила за достъп и ползване на ресурсите в нея, както и избор на защитна система, осигуряваща възможности за строг контрол. Файъруол (англ. firewall, защитна стена) е система за защита от вредители на ОС Windows XP. Този тип защита е най-разпространеният в компютърните мрежи. Тя успешно работи заедно с управляващите устройства на мрежата (рутери, сървъри и др.). Буквалният превод от английски „огнена стена“ не е лишен от смисъл, но ние ще използваме понятието ***защитна стена*** (*Фиг. 3*).



Фиг. 3. Защитна стена

Файъруол е сложна система от програми, проектирана да не допуска неоторизиран достъп отвън до компютърна мрежа (всички нейни компютри и ресурси), както и от компютърната мрежа към ресурси извън нея, чрез следене на целия мрежови поток от информация. Проблемите, налагащи използването на защитна стена, могат да бъдат най-разнообразни, а богатият ѝ инструментариум позволява ефективно справяне с тях. Забраните за достъп до Интернет сайтове, както и за използването на различни ресурси от мрежата, са само една малка част от възможностите на файъруол.

Основни функции на защитната стена

В компютърните мрежи, всяка комуникация между две отделни компютърни устройства се осъществява посредством пренос на данни. Прието е този процес да се нарича ***трафик***. Защитните стени проследяват трафика и тяхна задача е да пропускат само тази информация, която е разрешена и безопасна. Функциите на защитната стена, най-общо казано, са две:

- ***Блокираща***. Когато се направи опит за осъществяване на комуникация между устройство от мрежата и нашия компютър, защитната стена проверява внимателно данните, достигащи до нея. Ако те не отговарят на правилата за сигурност, зададени от администратора на мрежата, защитната стена прекратява комуникацията. По този начин данните, изпратени от едното комуникиращо устройство, никога не достигат до другото. Освен входящите данни, защитната стена може да блокира и изходящите, предпазвайки по този начин чуждото устройство от вредител, намиращ се на нашия компютър. Това рязко намалява опасността от разпространяване в мрежата на потенциално опасни услуги, зловреден софтуер и некласифицирана информация.
- ***Прикриваща***. Тази функция се състои в замяната на адресна информация с нереална, като прави мрежата ни да изглежда анонимна. Така се скриват важни вътрешни мрежови характеристики от останалата част на мрежата и се предотвратяват евентуални бъдещи атаки. Друга възможност за прикриване е да се замества адресът на защитавания компютър вместо с нереални адреси, с адреса на самата стена. По този начин също се скриват реалните вътрешни адреси на мрежата, но комуникацията вече се осъществява чрез реалния мрежов адрес на самата защитна стена и не е анонимна. Този метод на защита носи значително по-малък риск от неоторизиран достъп, тъй като стената е обектът от мрежата, който е най-силно защитен и достъп до нея има само администраторът на мрежата. По-усъвършенстваните защитни стени разполагат с вторична програма за защита, която е в готовност да поеме изцяло функционалността на главната, ако нещо се случи с нея.

Видове защитни стени

Съществуват три основни вида защитни стени:

- ***Филтриращи маршрутизатори***. Разглеждат всеки един пренос на данни поотделно и не се интересуват от това дали има разрешена комуникираща връзка между двете компютърни устройства.

- ***Нефилтриращи маршрутизатори***. Разглеждат всеки един пакет от данни само при установена и разрешена комуникация.
- ***Прокси***. Това са програми, които изпълняват ролята на краен потребител, защитавайки истинския краен потребител на комуникацията от външни опасности. Имат много силни защитни свойства, поради факта, че крайният потребители никога не осъществява директна връзка с външни мрежи (Internet).

Правила за сигурност при работа в Интернет

Когато работите, общувате или просто се забавлявате в Интернет, трябва да се замисляте не само за безопасността на своя компютър, а и за своята собствена безопасност. В Интернет пространството се намират хора с недобри намерения и за това трябва да се спазват определени правила:

- Не посещавайте сайтове, които не са ви препоръчани от възрастен и съдържат непонятна или смущаваща информация. Много от тях могат да застрашат домашния компютър с вируси и други вредни програми.
- Не се регистрирайте без знанието на родителите или учителите си в сайтове, които изискват предоставяне на лични данни.
- Не се представяйте за някой, който не сте и не посещавайте сайтове за възрастни.
- Внимавайте, когато някой ви предлага нещо безплатно или ви кани да се включите в дейност, обещаваща лесна и голяма печалба. Това вероятно е опит за измама.
- Не предоставяйте в мрежата лична информация като име, парола, адрес, домашен телефон, месторабота и служебен телефон на родителите си или училището, в което учите, без разрешение от родители.
- Не изпращайте в мрежата свои снимки или снимки на свои близки, преди да сте обсъдили решението си със своите родители.
- Не приемайте среща с някой, с когото сте се запознали в Интернет, без съгласието на своите родители. Ако те одобрят срещата, нека тя да е на публично място и по възможност да е в присъствието на близки или приятели.
- Не отговаряйте на съобщения, които са обидни, заплашващи, неприлични или ви карат да се чувствате неудобно. Информирайте родителите си за такива съобщения.
- Не отваряйте прикачени файлове в писма от електронната поща, получени от непознат подател. Те могат да съдържат вируси или програми, които да увредят компютъра ви.
- Внимавайте, когато разговаряте с непознати в някоя от програмите за общуване в реално време. Помнете, че хора, регистрирани в тези програми, могат да се представят за такива, каквито не са.
- Бъдете вежливи и уважавайте правата на другите потребители на мрежата.