Steps to Success
Пътят към успеха

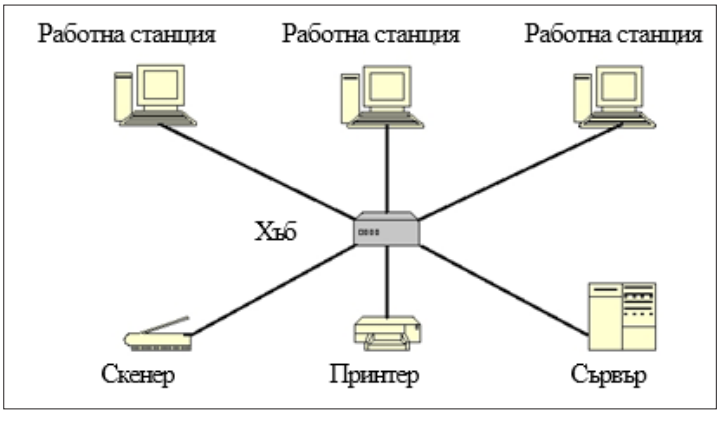
ЗАЩИТА НА ИНФОРМАЦИЯТА НА КОМУНИКАЦИОННИ И КОМПЮТЪРНИ МРЕЖИ

Живко Милов[1)]
Висше училище по телекомуникации и пощи – България

Резюме. В темата ще разгледаме следните класификации за защита на комуникационните и компютърните мрежи:
– класификация според физическия обхват;
– класификация според класификация на мрежите според топологията им;
– класификация според мрежовата архитектура и метода на администриране;
– класификация според мрежовата операционна система;
– класификация според мрежовия протокол.
Keywords: network architecture; network operating system; computer networks; protection service

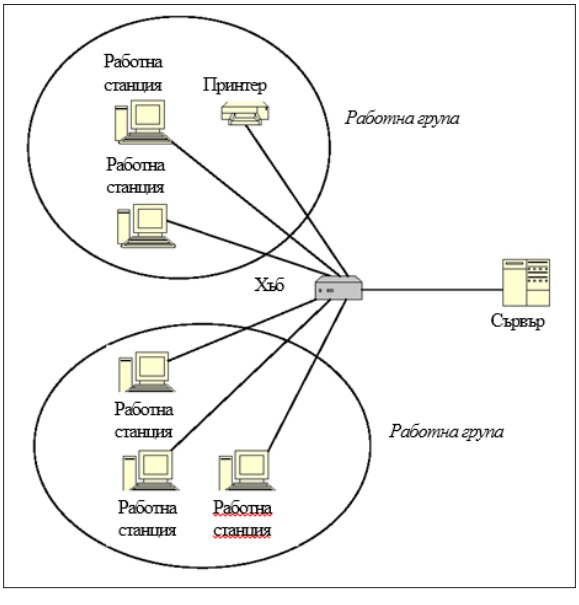
За по-лесното им управление големите LAN биват разбивани на свързани помежду си работни групи. Под работна група следва да се разбира група от персонални компютри (потребители), които споделят общи ресурси, като например: файлове, приложения, принтери и/или др. Например компютрите в различните отдели (личен състав, счетоводство, продажби и др.) на едно предприятие могат да бъдат обособявани в отделни работни групи и последните – свързани помежду си, образувайки една обща LAN. Когато в LAN мрежа се използват протоколите и технологиите на интернет, мрежата може да бъде определяна още и като интранет.

Под физически обхват следва да се разбира размерът на географската област, в която е разположена мрежата, и на второ място – броят на компютрите в нея. Според физическия си обхват мрежите биват:
– локални мрежи (LAN – Local Area Network);
– градски мрежи (MAN – Metropolitan Area Network);
– глобални мрежи (WAN – Wide Area Network).



Източник: Учебник компютърни мрежи

LAN мрежата обхваща ограничена географска област, като например: стая, етаж или сграда. Броят на компютрите в различните LAN би могъл да се различава съществено, като се започне от един два компютъра у дома или в офиса и се достигне до десетки дори стотици компютри в една сграда или в множество такива, намиращи се в близост една до друга. Терминът работна станция (workstation) означава, че компютърът работи под управление на своя разположена собствена операционна система. Работните станции изпълняват ролята на клиенти, т.е. на компютри, които използват споделяни в мрежата ресурси, осигурявани най-често от компютър, наричан сървър. Сървър е ком-



Източник: Учебник-компютърни-мрежи

пютър, който споделя своите ресурси с останалите участници в мрежата, а хъбът ги свързва физически в мрежа.

За по-лесното им управление големите LAN биват разбивани на свързани помежду си *работни групи*. Под работна група следва да се разбира група от персонални компютри (потребители), които споделят общи ресурси, като файлове, приложения, принтери и/или др. Например компютрите в различните отдели (личен състав, счетоводство, продажби и др.) на едно предприятие могат да бъдат обособявани в отделни работни групи и последните – свързани помежду си, образувайки една обща LAN. Когато в LAN мрежа се използват протоколите и технологиите на интернет, мрежата може да бъде определяна още и като *интранет*.

MAN мрежите биват изграждани от две или повече LAN, разположени в границите на един град (в област с радиус не по-голям от 50 до 80 км). По обхват те заемат междинно положение между LAN и WAN и често пъти вместо MAN биват квалифицирани като LAN или WAN. Затова определението MAN се среща рядко.

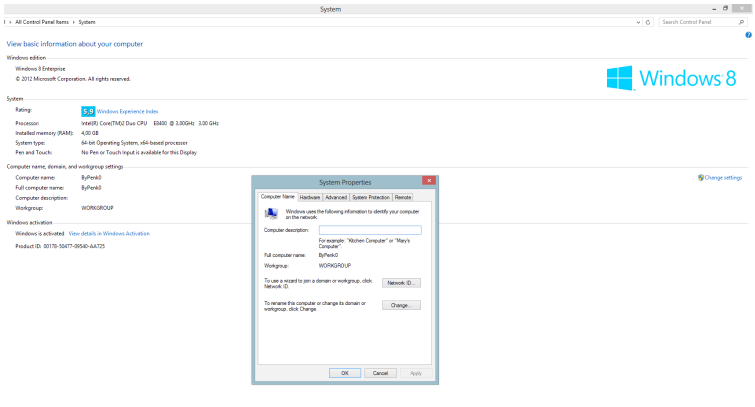
Класификация според метода на администриране

Една мрежа може да бъде организирана по два начина:

– като равноправна (peer to peer) работна група, в която всеки компютър може да изпълнява ролята на клиент или на сървър, при което всеки един от потребителите самостоятелно администрира ресурсите на своя компютър;

– като сървърнобазирана мрежа, администрирането на която е съсредоточено в един централен компютър, наричан сървър.

На фиг. 1 е разгледана компютърна мрежа от обща работна група с 10 компютъра.



Фигура 1.

Защита на мрежите

Важен въпрос, касаещ мрежите, е защитата на данните от загуба и/или от злоупотреба. Той бива разглеждан в два аспекта – *мрежова сигурност* и *предпазване от случайни сривове*. Под мрежова сигурност следва да се разбират мерките за защита от преднамерен или случаен достъп до информацията, съхранявана в мрежата. Пълна (100-процентова) гаранция за мрежова сигурност никога не може да има. Мрежовата сигурност е горещ проблем в света на информационните технологии. Бизнесът става все по-зависим от компютърните мрежи и информацията, съхранявана в тях. Но заедно с това той става все по-уязвим от пробиви в мрежовата сигурност. Често ставаме свидетели на съобщения в медиите за проникване в мрежите на правителствени и бизнес организации, както и за поражения, нанасяни от компютърни вируси.

Външните и вътрешните нарушители на мрежовата сигурност не са единствената заплаха за мрежите. Възможни са и случайни сривове, предизвикани от хардуерни повреди, природни бедствия или технически грешки в експлоатацията. Всички те водят до загуба на файлове, съдържащи в редица случаи ценна информация.

Видове заплахи

Когато започва изграждане на компютърна мрежа, винаги се поставя и въпросът за нейната сигурност. Анализира се степента на конфиденциалност на данните и се определят нуждите от защита. На тази база се съставя план за мерките, които трябва да се предприемат за осигуряване на нужната мрежова сигурност.

Заплахите за сигурността биват *вътрешни* и *външни*.

Вътрешни заплахи. Вътрешните пробиви на сигурността се осъществяват от служители на организацията, експлоатираща мрежата. Мотивите за това могат да бъдат най-различни.

Корпоративен шпионаж, свързан с кражба на търговски, технически или други тайни. Осъществява се в полза на конкурентни компании от подкупни служители. Този вид шпионаж спада към най-интелигентните, тъй като се извършва от хора с висок професионален опит. Мерките за сигурност, предназначени за осуетяване на корпоративен шпионаж, се осъществяват на най-високо управленско ниво с помощта на специалисти, посветени в защитата от шпионаж на корпоративните мрежи.

Саботаж. Понякога кариеристично настроени служители, за да покажат, че се справят в работата по-добре от свои колеги, прибягват до саботаж на дейността на последните. Формите на саботаж могат да бъдат най-различни, като се започне от претърсване на чужда електронна поща и на файлове за добиване на някаква уличаваща информация и се стигне до съзнателно унищожаване на важни данни. Особено опасни са служители, недоволни от политиката (понижение, уволнение и прочие), провеждана спрямо тях от страна на организацията, в която работят. Те са в състояние да повредят съзнателно

даден хардуер, да изтрият информация от твърдите дискове или да разпространят вируси в мрежата.

Случайни пробиви. Причиняват се несъзнателно от служители на организацията поради техническа некомпетентност или липса на подготовка. В старанието си да „поправят" възникнал дребен проблем, те биха могли да затрият ценна информация. Чрез въвеждане на позволения за работа само с определени файлове тази опасност може да бъде сведена до някакъв минимум, но не може да бъде избегната напълно.

Външни заплахи. Към външните заплахи могат да бъдат отнесени неоторизирано използване на пароли и ключове; DoS атаки; IP спуфинг; компютърни вируси и червеи; троянски коне.

Атаки от типа DoS. Атаките от типа DoS (Denial of Service – отказ от услуга) биват наричани още *нюк (nuke)* атаки. Те не предизвикват срив на атакуваната машина, а нарушават нейното нормално функциониране. Най-често използвани форми на DoS атаки са наводнението на протокола Ping/Internet Control Message Protocol (ICMP); смърф атаката; Ping на смъртта; SYN атаки.

Ping/ICMP наводнение. ICMP е протокол за съобщения и проверки за грешки, използван в интернет за предаване на информация. Командата **ping** е използвана за проверка дали даден компютър в мрежата се обажда. За целта тя използва ICMP пакети. Командата изпраща съобщение, наричано ICMP Echo Request, и чака да получи отговор, наричан ICMP Echo Replay. ICMP наводнението се състои в „наводнение" на протокола ICMP с пакети, предизвикващо „задавяне" на системата, към която е било извършено обръщане чрез командата **ping**. На IP адреса се изпращат непрекъснато пакети, в резултат на което той започва да забавя своята работа, след което се изключва поради таймаута на командата **ping**.

Смърф атаката е вид ICMP наводнение, което влияе на целия мрежов сегмент. Изпраща се съобщение до бродкастен адрес, което достига до всички компютри в мрежата, заставяйки ги да отговорят. Това натоварва мрежата и всички комуникации се забавят, в резултат на което всички потребители в един момент загубват връзката с мрежата.

Ping на смъртта е атака, която използва ограниченията, налагани от *максималната единица за предаване* (MTU – maximum transmission unit) на информация в мрежата. MTU се определя от пропускателната способност на преносната среда и от архитектурата на мрежата. Ако бъде изпратен пакет, който надхвърля MTU, той бива разделян на по-малки парчета и след това сглобяван отново, след като достигне до крайното си местоназначение. IP пакетът, в който е капсулирана заявката за ICMP ехо, е ограничен до 65 535 октета (един октет съдържа 8 бита). Ако бъде изпратен пакет с размер, надхвърлящ максималния брой октети, компютърът получател няма да бъде в състояние да сглоби разбития на части пакет и ще срине своята работа.

SYN атаката използва синхронизиращата последователност на TCP, за да осъществи прекъсване на комуникациите. За изграждане на сесия TCP използва процес на тристранно ръкостискане. Клиентът предава сегмент със заявка SYN за синхронизация, представляваща число. Сървърът изпраща на клиента отговор (потвърждението ACK), който включва числото, изпратено от клиента, увеличено с единица, заедно с друго SYN число, генерирано от сървъра. Клиентът добавя единица към числото на сървъра и го връща обратно на сървъра под формата на ACK. Ако процедурата протече нормално, двата компютъра установяват комуникационна връзка помежду си. Атаката се състои в изпращане на голям брой SYN заявки посредством подправен (спуфнат) IP адрес (виж следващия абзац). Приемащият компютър поставя заявките в опашка и започва да ги обслужва. Чрез непрекъснато запълване на опашката със заявки и поддържането ѝ в това състояние се пречи на компютъра да обслужва други заявки. По този начин потребителите не могат да получат връзка към сървъра.

IP спуфингът представлява подправяне на IP адрес. Изпращат се отвън съобщения, на които пакетите, по-конкретно техните хедъри, са така променени, че да изглеждат, сякаш идват от компютър, принадлежащ на мрежата. С придобития по този начин достъп до мрежата може да започне атака за кражба или унищожаване на данни.

Компютърните вируси са програми, които могат да нанасят най-различни поражения – от смущаване на визуализацията до изтриване на файлове на операционната система. Те притежават способността да се репликират и да се разпространяват от един компютър на друг без знанието на потребителите.

Червеят (worm) е вирус, който притежава способността да се *самореплицира* и да унищожава файлове в компютрите. Червеите се разпространяват най-често като прикрепени към електронната поща или като документи, съдържащи макроси. Те могат да попаднат в мрежата и с HTML страници, съдържащи червеи под формата на скриптове.

Троянските коне са зловредни програми, които биват представяни пред потребителите като програми, предназначени за извършване на някаква определена полезна дейност. Стартирането на една такава програма довежда до неочаквани вредни последствия. В много от случаите това са уебсайтове, които изискват от потребителите въвеждане на личните им данни, които след това биват ползвани за пъклени цели.

Мерки за сигурност

Сигурност на паролите. Важна част от плана за сигурност на мрежата е осигуряване на по-неразгадаеми пароли. На потребителите на мрежата трябва да бъдат препоръчани следните правила за създаване на пароли. Паролите не трябва да бъдат думи или числа, имащи някаква връзка с потребителя, като например рождена дата, име на член от семейството, име на куче и т.н. Паро-

лите не трябва да бъдат думи от речника, тъй като при отгатване на пароли с помощта на програми последните използват думите от речника. Парола, която съдържа главни букви на случайно подбрани позиции е трудно разгадаема. Паролата трябва да бъде такава, че да може да се помни от потребителя, а не да се записва на хартия, откъдето друго лице би могло да я прочете. Колкото е по-голяма дължината на паролата, толкова по-трудно се разгадава, но и по-трудно се помни. Паролата трябва периодически да се променя, но не много често, за да може да се помни.

Повечето мрежови операционни системи позволяват на администраторите да задават минималната дължина на паролите, да проследяват тяхната история (съхранява се списък с предишните пароли, като не се допуска тяхното повторно използване) и да задават срокове на валидност на паролите (заставят потребителите да променат паролите си през зададен интервал от време). Установяването на самоличността на потребителите е важен фактор за сигурността. В последно време се обръща внимание на технологии, които гарантират висока степен на сигурност при идентифициране на потребителите. Към тях могат да бъдат отнесени смарт картите и технологиите, проверяващи биометричните данни на потребителите, като разпознаване на пръстови отпечатъци, сканиране на ретината и разпознаване на ириса на окото, както и верификация на гласа.

Паралелно с нарастване на популярността на безжичните комуникации и бързото им навлизане в дейността на хората се засили и интересът за осъществяване на пробиви в тях. Рисковете нараснаха значително. Нещо повече, в интернет се появиха безплатни програми за Windows и Linux, предназначени за кракване на безжични мрежи.

Появи се и друга опасност – жичните мрежи биват краквани по безжичен път. Това става посредством преносим компютър, включен чрез кабел към жична LAN, например от служител на фирма, включил персоналния си компютър към мрежата на фирмата си. Тъй като вече, като правило, всеки преносим компютър е снабден с вградена карта за безжична връзка (интерфейс 802.11b/802.11g), един кракер, намиращ се някъде в близост, например отвън на паркинга на фирмата, може да влезе през безжичния интерфейс в преносимия компютър и от там – в жичната LAN.

Непозволен достъп до мрежа на дадена компания може да се получи и случайно. Включвате своя преносим компютър и без да искате, се свързвате с точка за достъп от безжичната мрежа на съседната компания, чийто обхват на действие припокрива действието на вашата безжична мрежа. През точката бихте могли да влезете в локалната мрежа на чуждата компания и да получите достъп до секретна информация или от там да се свържете по интернет непозволено с някаква друга компания. Злонамерени атаки кракерите могат да извършват посредством своя лаптоп. С помощта на специален софтуер те пре-

връщат безжичната карта на лаптопа в легитимна точка за достъп, с помощта на която влизат в локалната мрежа на компанията, вместо да използват легитимна точка за достъп, принадлежаща на мрежата. Такива лаптопи биват наричани „софт-точки“ (soft APs). Атаката се извършва на MAC ниво, поради което средствата за защита, използвани на ниво 3 (автентикация и VPN), не могат да послужат като бариера. MAC измама (кражба на идентификация) се осъществява, когато кракерът подслуша трафика и от него извлече MAC идентификатора (MAC адреса) на някой от компютрите в мрежата и присвоените му права на достъп. В безжичните мрежи е реализиран механизъм за MAC филтрация на адресите, който ограничава участието в мрежата, допускайки само устройства, които са били предварително регистрирани посредством своите MAC адреси. Съществуват обаче програми (например програмата SMAC), които, подслушвайки трафика, разузнават мрежата и могат да регистрират в нея допълнителен MAC адрес, посредством който след това може да се влезе нелегитимно в мрежата. Съществува и друг начин да бъде „прескочена оградата“. Става чрез използване на „посредник“. Кракерът, превърнал компютъра си в „софт-точка“ (soft APs), подмамва някой от легитимните участници в мрежата да се свърже с него. Веднъж осъществил това, кракерът прави връзка с реална точка за достъп (AP) от мрежата посредством другата безжична карта на компютъра си, създавайки нелегитимен трафик през хакнатия компютър. Атаки чрез използване на „посредник“ се осъществяват с програми като LANjack и AirJack[5)].

В настоящия текст разгледахме най-общо мрежите и използването им в една работна група. От работната страна и колегите в едно работно място се забелязват опити до саботаж, за да се навреди на друго лице. Колкото повече се разрастват технологиите, се забелязва развитие и в разбиване на компютърните и телекомуникационните системи с цел да се навреди на реномето на някой служител или да се източи важна и ценна информация.

NOTES/БЕЛЕЖКИ

1. Авторът е студент във Висше училище по телекомуникации и пощи.

Консултант при разработване на настоящия текст е проф. д.т.н. инж.-мат. Антонио Андонов, катедра „Телекомуникации“, Факултет по телекомуникации и мениджмънт, Висше училище по телекомуникации и пощи.

2. http://www.scribd.com/doc/73679720/41/%D0%97%D0%B0%D1%89%D0%B8%D1%82%D0%B0-%D0%BD%D0%B0-%D0%BC%D1%80%D0%B5%D0%B6%D0%B8%D1%82%D0%B5

3. http://techs-mobile.blogspot.com/2010/06/lan.html

4. http://www.vpntutorials.com/tutorials/l2tp-ipsec-vpn-etup-tutorial-for-windows-8/

5. https://technet.microsoft.com/en-us/library/jj613767.aspx
6. http://bg.wikipedia.org/wiki/OSI_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB

REFERENCES/ЛИТЕРАТУРА

Shindar, D. (2015). *Kompyutarni mrezhi*. Sofia: SoftPres. [Шиндър, Д. (2015). *Компютърни мрежи*. София: СофтПрес.]
Nortan, P. (2014). Palno rakovodstvo za rabota s mrezhi. Sofia: Infodar. [Нортън, П. (2014). *Пълно ръководство за работа с мрежи.* София: Инфодар.]
Kolektiv. (2015). Kompyutarni mrezhi v lesni stapki. [Колектив. (2015). *Компютърни мрежи в лесни стъпки*.]
Bakardzhieva, T. (2013). Elektronni biznes-tehnologii i mrezhi. Varna: VSU „Chernorizets Hrabar". [Бакърджиева, Т. (2013). *Електронни бизнес-технологии и мрежи.* Варна: ВСУ „Черноризец Храбър".]
Kaeo, Merike. (2015). Proektirane na mrezhova sigurnost. Sofiya: SoftPres [Каео, Мерике. (2015). *Проектиране на мрежова сигурност*. София: СофтПрес.]

PROTECTION OF INFORMATION OF COMMUNICATION AND COMPUTER NETWORKS

Abstract. In the text we will discuss the following classifications for protection of communication and computer networks:
– classification according to physical range;
– classification according to the method of administration;
– classification based network operating system;
– classification according to network protocol;
– classification of the networks according to their topology;
– classification according to network architecture.

✉ **Mr. Zhivko Milov**
University of Telecommunications and Post
Sofia, Bulgaria
E-mail: zhivko88@abv.bg