ПРОБЛЕМИ НА СИГУРНОСТТА ПРИ ОТДАЛЕЧЕН ДОСТЪП ДО КОРПОРАТИВНИТЕ МРЕЖИ

Нели Лилова

В света на съвременния бизнес, в научните среди и академичните институции нараства популярността на отдалечения достъп. Съвременните решенията за отдалечен достъп позволяват на потребителите да установят връзка към мрежата и да изпълняват задачи по такъв начин, както ако са свързани директно по кабел към останалата част на мрежата, дори ако са отдалечени на хиляди километри. В резултат на това отдалечения компютър става член на локалната мрежа, макар и временно.

Типичната мрежова връзка за отдалечен достъп се осъществява с модем. Отдалечен достъп до мрежата може да бъде реализиран и чрез безжични връзки. Той позволява да се разшири мрежата отвъд физическите и граници до почти всяка точка на света, необходим е само сървър за отдалечен достъп.

В днешно време безжичните технологии стават все по-необходими и в академичните институции и научните среди. Тази нужда доведе до национални и международни инициативи за осъществяване на национален и международен роуминг. Роуминг се нарича осигуряването на преход на мобилна работна станция от един административен домейн към друг, без прекъсване в услугата или загуба в свързаността.

TERENA faskforce on Mobility формулира изискванията за развитие на международен роуминг, чрез който потребителите на Националните изследователски и образователни мрежи (НИОМ) ще имат възможност за достъп до академичните институции по света. EDUROAM е научно-изследователски проект, благодарение на който учените имат мобилна интернет свързаност с всички членуващи организации.

Отдалеченият достъп става все по-важен с нарастването на мобилността на потребителите на мрежите и с разрастването на бизнеса на организациите до множество места, или отварянето на техните ресурси за избрани външни партньори без поставяне на тези ресурси в интернет.

Тук съм изложила проучванията си, относно публикуваната информация за проблемите на сигурността при отдалечения достъп до корпоратвните мрежи, визирала съм най-популярните решения за отдалечен достъп и съм анализирала най-често прилаганите мерки за сигурност при този вид достъп. Един такъв анализ и обобщение има своята стойност, защото е важно да се разбере с какво услугите за отдалечен достъп могат да помогнат на организацията, при избор на едно от приложенията му и особено при избора на решение за мерките за сигурност за постигане на сигурна среда и осигуряване на потребителите удобството на отдалечения достъп.

Изследванията показват, че едни от най-популярните съвременни приложения на отдалечения достъп биха могли да се обединят в пет основни групи:

- свързване на офиси и филиали;
- възможност за връзка към мрежата след фиксирано работно време;

- ♦ телекомютинг;
- ♦ мобилни потребители;
- ♦ осигуряване на достъп за клиенти и партньори.

Първото приложение – свързване на офиси и филиали е обусловано от факта, че дори малките бизнес организации отварят офиси на различни места и това предполага наличието на връзка към мрежата в централния офис. Dial-up връзката е достатъчна, когато не е нужен чест или постоянен достъп, или когато той се извършва от няколко компютъра. В централния офис един компютър в мрежата може да бъде настроен като dial-up сървър. Потребителите от филиалните офиси могат да избират и установяват връзка към мрежата, когато е необходимо.

Второто приложение касае служителите, чито работен ден продължава в часовете след работа. За тях може да бъде полезно и необходимо да имат връзка до корпоративната мрежа след фиксираното работно време.

Третото приложение – предоставяне на програмистите на софтуер, творческия персонал, търговци и административни служители възможност за телекомуникации (телекомютинг) – т.с. възможност да работят вкъщи в част от работното време или на пълно работно време. Тези служители се наричат **телекомютъри**, защото се свързват отдалеч с офиса и остават във връзка през деня чрез e-mail, чат на живо и дори аудио и видео конферииране. Dial-up достъпът е най-често срещания начин за свързване на телекомютърите към LAN на организацията, макар че в някои случаи може би е по-добре да се използват специално предназначена за целта връзка. Ако организацията има много служители телекомютъри, сървърът за отдалечен достъп ще изисква включването на множество модеми (банка от модеми), за да могат да се осъществят множество връзки едновременно. При това всеки модем изисква собствена телефонна линия.

Четвъртото приложение дава възможност на служителите, които са на път (търговци, предприемачи, инструктори, мениджъри от висок клас, ръководители на бизнес обиколки и др.) да се свързват към корпоративната мрежа. Невъзможно или трудно може да се съхранят всички необходими файлове на лаптопа или нотбук компютъра. Освен това съществува и заплаха за сигурността, защото те могат да бъдат откраднати физически. По-добро решение може да бъде мобилният потребител да избира (dial-up) LAN мрежата на организацията, където се автентифицира неговия потребителски акаунт и след това да осъществява достъп до данните в мрежата, вместо да ги копира на собствения си диск.

Петото приложение е осигуряване на достъп до избрани мрежови ресурси за клиентите на компанията или за нейните партньори. При тази концепция, от съображения за сигурност трябва да се реши дали „потребителите гости“ да имат достъп до мрежата посредством обиковен акаунт (guest акаунт) или чрез уникално потребителско име и парола. Предоставянето на анонимен достъп е опция, подходяща за среда с ниска сигурност или за такава, в която сървърът за отдалечен достъп е отделен от останалата мрежа посредством защитна стена (firewall). Другата опция – уникален ID и парола за клиента, увеличават работата на администраторите, но позволява да се следи кой осъществява достъп до мрежовите ресурси и кога и как става това.

Съществуват няколко вида форми на връзка за отдалечен достъп:

- ♦ Dial-up връзка по аналогова или цифрова телефонна линия;
- ♦ VPN (Virtual Private Network) – виртуална частна мрежа, която използва интернет като преносна среда за изграждане на връзка.

Предимствата и недостатъците на VPN решенията, сравнени с Dial-up решенията са обощени в следващата таблица:

Предимства на VPN	Недостатъци на VPN
Избягват се таксите за междуградски разговори. Необходими са по-малко телефонни линии и по-малко модеми. Ако VPN е базирана на ISP, се съкращават разходите за администриране и обучение.	И в двата края на връзката трябва да има надеждна интернет връзка. Производителността често е по-ниска, отколкото при dial-up връзката.

Повечето често използвани VPN мрежи са реализирани за една от следните цели:

♦ да осигурят отдалечен достъп до мобилните служители или такива работещи вкъщи;

♦ за осигуряване на екстранет мрежа, до която имат достъп служители, клиенти и партньори;

♦ за осъществяване на контакт между два офиса в различни местоположения, без да се изгражда специална връзка.

Независимо от формата на връзка за отдалечен достъп, връзката към външния свят ви излага на определени рискове по отношение на сигурността. Можете да повишите сигурността по няколко начина, като едновременно с това разрешите на вашите потребители отдалечения достъп, който им е необходим. С помощта на мерки за сигурност в комбинация с позволения за достъп до файлове и споделени ресурси за контрол на достъпа, можете да постигнете сигурна среда и в същото време да осигурите на потребителите удобството на отдалечения достъп.

Изследванията на водещи фирми за одитиране на сигурността показват, че най-често прилаганите **мерки за сигурност** са:

♦ сигурност чрез обратно избиране;

♦ методът RADIUS – Remote Authentication Dial-up User Service;

♦ политики за отдалечен достъп;

♦ заключване на акаунти;

♦ сигурни хостове.

Сигурността чрез обратно набиране е възможност на сървъра за отдалечен достъп, която може да разшири сигурността чрез ограничаване на dial-up връзките само до тези на одобрени телефонни номера. При включена сигурност с обратно набиране сървърът не вярва на акредитивите (потребителски имена и парола), въведени от потребителя. Той се изключва или прекъсва връзката и веднага след това набира клиента с номера, който е записан на сървъра и разрешава нормален достъп.

RADIUS е протокол, който стана индустриален стандарт за автентификация на dial-up потребители и осигурява услуги за управление на акаунти за dial-up сървъри, използвани от ISP доставчиците. Dial-up сървърът се конфигурира като RADIUS клиент, а информацията за потребителско име и парола се изпращат от dial-up сървъра до RADIUS сървъра. Именно RADIUS сървърът осигурява централизирано автентификация с помощта на определени протоколи:

♦ CHAP (Challenge Handshake Authetication Protokol) и MS-CHAP – протоколи за автентификация с предварително съгласуване на повикването;

♦ DNIS (Dialed Number Identification Services);

♦ ANI (Automatic Number Identification) Service.

DNIS е базиран на номера, набиран от потребителя, а ANI е базиран на номера от който се обажда потребителят.

Съхраняването на информацията за осигуряване на контрол на достъпа в RADIUS сървъра е по-сигурно, от съхранението ѝ в конфигурацията на мрежовите устройства, където тя би била достъпна на всички потребители с равни права, където нивото на криптиране не винаги може да осигури защита дори при производители на оборудване от висок клас. RADIUS е удобен протокол за услуги, изискващи автентификация и оторизация при достъп до мрежов или изчислителен ресурс, с възможност за конфигуриране на различни услуги на мобилни и стационарни потребители с по-високи изисквания по отношение на сигурността и централизирана тарификация. Въпрос на бъдеще е заменянето на RADIUS протокола с аналогични протоколи, които са базирани на TCP или други протоколи от транспортния слой, свързани с изграждането на потребителска сесия за надежден транспорт на данни при едновременно криптиран пренос на информацията. В момента RADIUS се използва и за осигуряване на достъп и тарификация при всички VoiP услуги. При това, освен информацията, свързана с тарифирането на услугите, в RADIUS сървърите се акумулира и много специфична информация, свързана с обмена на телефонен трафик, имащ отношение както към информационната сигурност, така и информация, полезна за оптимизиране на услугите и повишаване на качеството им. От гледна точка на защита на личните данни би било добре потребителите на VoiP услуги да се доверят на легитимни лицензирани оператори.

В научноизследователския проект EDUROAM, в който са включени българските университети и институти на

БАН, като членове на Националната изследователка и образователна мрежа, централизирана автентификация се осъществява именно чрез RADIUS сървър, който у нас се поддържа от фондация „Технологии на информационното общество“ – НИОМ на България.

Политиките за отдалечен достъп са възможност за контрол на достъпа в зависимост от използваната операционна система. Те предоставят или забраняват достъпа на базата на следните критерии:

- част от деня (примерно ограничаване на отдалечения достъп от 8 часа сутрин до 6 часа следобед);
- ден от седмицата (примерно от понеделник до събота, но не и в неделя);
- членство в група (примерно забранява се достъпът на всички членове на групата CTNBnew);
- тип на отдалечената връзка (примерно разрешаване на VPN връзка и забраняване на dial-up връзка и обратно).

Политиките могат също да ограничават количеството време, което потребителят може да бъде свързан, или методите на автентификация, които могат да бъдат използвани.

Заключването на акаунт може да бъде приложено към връзка за отдалечен достъп, за да попречи на неоторизирани потребители да познаят валидната парола, чрез използване на различни пароли в последователен ред, ръчно или чрез софтуерни атаки с груба сила. При заключването на акаунта, след определен брой неуспешни опита за логване, акаунтът се заключва и системата не приема повече опити. Конфигурирането на тази възможност става като се зададе стойността на следните параметри:

- брой на неуспешните опити, които са разрешени преди включване – потребителят може да сбърка паролата един или два пъти, но малко вероятно е да повтаря грешката си непрекъснато, затова може тази стойност да бъде 3;
- интервал от време или период, след който акаунтът ще бъде освободен или ще остане заключен, докато администраторът не го отключи – например приемлив интервал от време е 2 часа. При това положение, ако легитимният потребител се опитва да се логне, след като акаунтът е бил заключен вследствие атака на нарушител, потребителят ще може да направи това без проблеми;

Хостовете за сигурност представляват устройство, използвано за автентификация на входящи потребители. То се използва в допълнение към собствените мерки за сигурност на сървъра за отдалечен достъп. Хостът представлява хардуерно устройство, което се инсталира между клиента за отдалечен достъп и сървъра за отдалечен достъп. Съществуват няколко типа хостове за сигурност. В някои случаи хостът изисква от dial-up потребителя да зададе потребителско име и парола, които са отделни и независими от името на акаунта и паролата за логване в сървъра за отдалечен достъп. Например компанията Security Dynamics предлага модема Secur ID, представляващ модем от типа PC card, който включва автоматизирана автентификация за мобилни потребители. Потребителите въвеждат PIN номер, който се изпраща автоматично от модема до хоста за верификация.

Известно е, че сигурността на VPN има три компонента: автентификация, авторизация и криптиране.

Автентификацията на VPN клиента включва проверка за истинност на самоличността на машината и на потребителя, който инициира VPN връзката.

Авторизацията означава зададените ограничения, на базата на които на едни потребители се предоставя достъп до VPN, а на други се отказва. За защита на данните във VPN мрежа могат да бъдат използвани най-различни технологии за **криптиране**, без които те биха могли лесно да бъдат прихванати, докато се движат по обществената мрежа.

ИЗТОЧНИЦИ

1. www.eduroam.org
2. www.corecom.com/html/vpn.html
3. www.list.gmu.edu/links.htm
4. www.shiva.com/images/
5. www.ietf.org/html.charters/
6. www.func.com/radius
7. **Шиндър, Д.** Компютърни мрежи. София, Софтпрес, 2003.
8. **Притам, В.** Защитни стени и сигурност в Интернет, София: Дуо дизаийн, 2005.