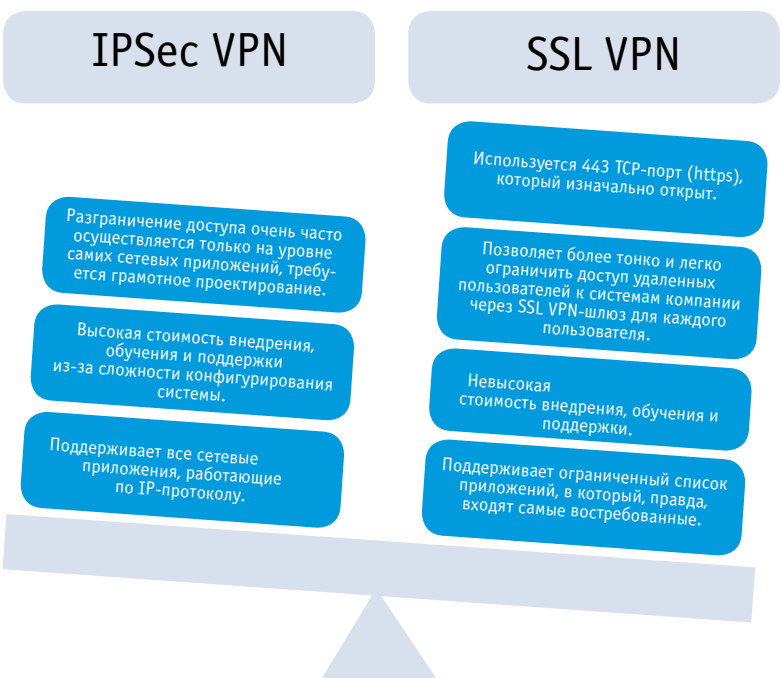
Безопасный удаленный доступ
к корпоративным ресурсам – существующие концепции и решения

Александр ДОРОФЕЕВ,
CISSP, CISA, директор,
АНО «Учебный центр «Эшелон»

Многие из нас уже не представляют, как можно эффективно работать без удаленного доступа к корпоративной сети. Мы подключаемся к сети компании из дома, из гостиницы, даже во время отпуска у нас может возникнуть необходимость получить доступ к своему корпоративному почтовому ящику, и мы пойдем искать ближайшее интернет-кафе. Раньше наибольший интерес к технологиям удаленного доступа проявляли компании, деятельность которых связана с удаленной работой сотрудников на территории клиентов (аудиторы, консультанты, интеграторы), теперь же вследствие финансового кризиса уже многие организации рассматривают возможность сократить свои затраты за счет использования сотрудников, работающих удаленно от офиса – в своем доме. Удобствами удаленного доступа могут воспользоваться и злоумышленники, и необходимо четко понимать, как они будут действовать, чтобы применять соответствующие меры защиты.

Организация удаленного доступа к корпоративным информационным ресурсам, как правило, связана с использованием виртуальных частных сетей (Virtual Private Network – VPN) на основе протоколов IPSec и SSL.

При использовании IPSec VPN у пользователя складывается ощущение, что он находится у себя на работе: он работает с теми же сетевыми программами, что и у себя в офисе, а в случае SSL VPN ему требуется web-браузер, через который и предоставляется доступ к системам компании. В первом случае, как правило, сотруднику необходимо воспользоваться своим корпоративным ноутбуком и сетью, которая позволяет обращаться к портам VPN-шлюза, а во втором – найти лишь устройство с выходом в Интернет. Обе технологии больше дополняют



друг друга, чем конкурируют, и во многих компаниях используются совместно.

С точки зрения информационной безопасности, появление сервиса удаленного доступа (вне зависимости от используемой VPN-технологии) влечет за собой возникновение новых рисков, которые нужно минимизировать внедрением как технических, так и организационных мер.

Рассмотрим наиболее распространенные сценарии атак на корпоративные ресурсы посредством удаленного доступа, которые условно можно разделить на две группы:

- нацеленные на пользователя системы удаленного доступа для дальнейшего проникновения в корпоративную сеть;
- нацеленные непосредственно на корпоративную сеть компании.

Взлом VPN-шлюза внешним злоумышленником

Данный сценарий применим для IPSec VPN и SSL VPN, так как всегда есть «дверь» в виде специального устройства/сервера, через которое удаленные пользователи попадают в корпоративную сеть. При реализации подобного сценария атака будет проходить по следующим этапам:

1) идентификация цели. Злоумышленнику необходимо определить сетевой адрес VPN-шлюза, через который удаленные пользователи входят в сеть. Для этого он будет искать доменное имя шлюза с помощью поисковых ресурсов (Google, Yandex и т. п.), перебирать всевозможные домены третьего уровня (наподобие vpn.ваш_домен.ru), сканировать диапазоны IP-адресов, выделенных вашей организации, с помощью сканера портов;

2) определение используемого VPN-решения. Обнаружив VPN-шлюз, злоумышленник постарается определить версию используемого программного обеспечения и запущенные сетевые сервисы;

3) подбор паролей. Первое, что сделает злоумышленник, – проверит наличие учетных записей с паролями по умолчанию;

мнение специалиста

Михаил ГРУНТОВИЧ,
руководитель обособленного подразделения в городе Пенза, ЗАО «ОКБ САПР»

Заниматься обеспечением безопасности, основываясь только на собственной интуиции, по меньшей мере, недальновидно. Стоит воспользоваться технологиями оценки защищенности, коих сейчас достаточно много. При этом, конечно, следует реально оценивать свой бюджет и свои риски. А значит, надо понять, против какого злоумышленника следует защищаться: самоутверждающийся хакер, или организованная группа хакеров, или конкурирующая компания... От этого будут зависеть не только используемые механизмы, но и все построение эшелонов защиты. Может оказаться, что интернет-кафе как точка доступа отпадает в принципе, а помимо чисто программных средств защиты может потребоваться и аппаратная поддержка в виде средств аутентификации, безопасного хранения данных, ограничения доступа.

Если ситуация серьезная, при реализации нужно не пожалеть денег на консультацию со специалистами. Решения безопасности могут потребовать учета не только современного состояния технологий атак, но и перспектив, для оценки которых и выработки адекватных решений защиты не достаточно отрывочных публикаций в Интернете. Может оказаться, что изменения нужны и внутри компании: все взаимосвязано, а комплексное решение может сэкономить ресурсы.

Ростислав РЫЖКОВ,
руководитель отдела развития, ОАО «ЭЛВИС-ПЛЮС»

Для организации эффективной защиты удаленного доступа помимо понимания общих контуров проблемы необходимо учитывать ряд важных факторов. Средств организации VPN и межсетевого экранирования много, и эффективность их разная. Бывают они некоммерческие (свободно распространяемые), и коммерческие. Свободно распространяемые средства пригодны там, где ущерб от вторжения злоумышленника невелик. Коммерческие стоят заметных денег, и пользователь должен решить, как эти деньги эффективно вложить. При выборе следует обратить внимание на некоторые свойства приобретаемых средств организации VPN и межсетевого экранирования, которые заметно влияют на эффективность системы защиты. Среди таких свойств – использование стандартных протоколов SSL и IPSec (некоторые средства защиты строятся на модифицированных, либо оригинальных протоколах), а также наличие средств централизованного управления доступом пользователей к ресурсам корпоративной ИС. Отдельно необходимо отметить важность использования в средствах VPN «правильных» криптоалгоритмов. С одной стороны, их использование в нашей стране регламентируется нормативно, и для многих пользователей (госструктуры, операторы персональных данных) критически важно использовать именно отечественную, ГОСТ-овскую криптографию. С другой – надо помнить, что встроенная в VPN-средства «западная» криптография DES, 3DES, AES может оказаться недостаточно стойкой.

Кирилл СЛУЧАНКО,
ведущий инженер отдела системной интеграции, компания «Поликом Про»

Следует отметить, что клиентская часть современных решений в области SSL VPN уже может обеспечить клиентам «прозрачность» доступа к корпоративной сети, сравнимую с IPSec VPN – при этом браузер явно используется только на этапе установления соединения. Наблюдается тенденция сдвига области применения IPSec в сторону магистральных каналов с полной заменой систем клиентского удаленного доступа на SSL VPN. Это вполне объяснимо, так как технология SSL VPN обеспечивает большую универсальность с точки зрения получения удаленного доступа, так как меньше зависит от NAT, прокси-серверов и МСЭ на транзите между клиентом и сервером удаленного доступа.

Позволю себе не согласиться с утверждением, что проектирование, развертывание и настройка систем IPSec VPN сложнее, чем систем SSL VPN. С учетом возможных вариантов доступа по SSL VPN (бесклиентский, с тонким или полнофункциональным клиентом), многообразия браузеров и других факторов, зачастую настройка SSL VPN становится более сложной, чем настройка IPSec VPN – однако результат стоит того.

С точки зрения защиты подключений удаленного доступа можно дополнительно упомянуть технологии контроля доступа к сети (NAC), использование терминальных серверов с ограничением функциональности клиента или специальных «песочниц», изолирующих запускаемые корпоративные приложения от ПО клиента удаленного доступа.

4) поиск и эксплуатация уязвимостей. На данном этапе злоумышленник, зная версию используемого ПО, попытается найти известные уязвимости и использовать их для получения доступа.

Для защиты от подобного лобового воздействия специалисты по защите информации:

- выбирают такое доменное имя для VPN-шлюза, чтобы его нельзя было легко угадать (в названии избегают слов «VPN», «remote»);
- осуществляют мониторинг появления имени шлюза в индексах поисковиков (например, с помощью сервиса Google Alerts);
- используют для VPN-шлюза IP-адрес провайдера, а не собственный;
- настраивают межсетевой экран таким образом, чтобы блокировать попытки сканирования портов и определять попытки вторжений;
- регулярно устанавливают выпускаемые вендором обновления;
- проводят тестирование на проникновение, стараясь обнаружить бреши в защите раньше, чем это сделают злоумышленники.

Нужно понимать, что злоумышленник не всегда будет действовать «в лоб» и атаковать наши внешние ресурсы, он может проникнуть в сеть с помощью наших пользователей.

Кража ноутбука пользователя для удаленного доступа в сеть

Злоумышленники могут похитить ноутбук сотрудника с целью проникнуть в корпоративную сеть компании через систему удаленного доступа. Такой сценарий применим для технологий удаленного доступа на основе IPSec VPN, поскольку в данном случае ноутбук содержит все настройки для доступа в сеть и, как часто бывает, пароли пользователя.

Для защиты от подобной угрозы компании:

- внедряют политику безопасности мобильных устройств, предусматривающую отсутствие логотипов компании на устройствах и чехлах, использование кабеля безопасности, с помощью которого ноутбук пристегивается, если владельцу необходимо оставить его без присмотра и т. п.;
- проводят обучение сотрудников, уделяя особое внимание безопасному обращению с мобильными устройствами в общественных местах;
- устанавливают системы шифрования жестких дисков ноутбуков;

мнение специалиста

Евгений БЛОХИН,
руководитель практики комплексных решений компании «Verysell Проекты»

Чтобы обеспечить высокий уровень защиты мобильных устройств сотрудников, ИТ-специалисты должны следовать нескольким простым правилам.

Для защиты доступного из сети VPN или web-сервиса необходимо использовать лучшую практику ведущих производителей решения.

Чтобы обезопасить данные непосредственно на носителе – достаточно использования политик безопасности и системы шифрования.

Кроме того, при подключении в корпоративную сеть устройств, работающих во внешней среде, необходимо использовать режим карантина. В карантинной зоне происходит проверка устройства на все возможные вирусы, производится обновление антивирусных программ и т. д. При этом ноутбук или смартфон, не соответствующий политикам безопасности, в корпоративную сеть не допускается.

И, наконец, известно, что наибольшая часть утечек информации с мобильных устройств происходит по вине самих сотрудников, поэтому разговор о технических средствах защиты не имеет никакого смысла без создания совершенно новой модели поведения. Нельзя допускать, чтобы сотрудники халатно подходили к вопросу защиты используемых в работе устройств, ссылаясь на нехватку времени, неудобство и на то, что вся ответственность за безопасную работу лежит на ИТ-службе. Чтобы «привить» новую культуру ответственности за безопасную удаленную работу, должно регулярно проводиться обучение персонала с объяснением, какие угрозы несет беспечное обращение с мобильными устройствами и как этих угроз избежать.

Михаил РОМАНОВ,
директор по развитию бизнеса Stonesoft в России, СНГ и странах Балтии

Технологии IPSec VPN и SSL VPN больше дополняют друг друга, чем конкурируют. С одной стороны, технология SSL не требует установки клиентского ПО, что по идее дешевле. Однако, как правило, традиционные технологии IPSec VPN на стороне узла требуют значительно меньше ресурсов для обработки такого же количества одновременных соединений, кластеризуются для отказоустойчивости проще, в то время как SSL устройства большинства вендоров требуют применения для этой цели внешних балансировщиков, что значительно удорожает решение. Кроме того, у технологии SSL в реализации большинства вендоров имеются принципиальные ограничения по максимальному количеству одновременных соединений.

С точки зрения безопасности технология SSL менее надежна. Шлюз IPSec VPN часто вообще не регистрируют в DNS и взломать его намного сложнее. Например, тут http://www.kb.cert.org/vuls/id/261869 описана уязвимость, продиктованная самой природой или концепцией SSL. Исключить ее совсем, кроме как очень аккуратным администрированием, разграничением доступа и т. п., вряд ли получиться.

Таким образом, если идет речь о доступе с ноутбука, то, несомненно, проще и надежнее использовать IPsec VPN. Клиенты у некоторых вендоров уже давно могут использовать порт 80, 443 и др. Если в доступности только коммуникатор или интернет-киоск, не обойтись без SSL VPN. Таким образом, говорить о перевесе технологии SSL пока рано, гораздо удобнее использовать обе технологии, получая преимущества обеих, как мы и делаем, например, в своей компании.

• используют средства двухфакторной аутентификации, что делает компрометацию пароля не критичной, так как он состоит из постоянной части – пин-кода и переменной, которая регулярно меняется произвольным образом (например, каждую минуту).

Перехват паролей пользователей

Для получения доступа к сети в большинстве случаев пользователь должен ввести имя своей учетной записи и пароль. Именно эти данные становятся самой желанной добычей при применении технологии SSL VPN.

Наиболее простыми и доступными способами получения подобной информации являются использование программ типа «keylogger», перехватывающих все строки, введенные пользователями, а также проведение фишинг-атак на пользователей.

В первом случае имя учетной записи и пароль вашего сотрудника могут быть похищены, например, в интернет-кафе, где он воспользовался общественным компьютером для доступа в корпоративную сеть.

Во втором случае злоумышленники запускают web-сервер со страницей «Смена пароля», дизайн которой идентичен страницам вашего VPN-шлюза. Сотрудникам рассылается письмо от имени ИТ-отдела с просьбой пройти по ссылке и сменить пароль. Пользователи сами «сдают» свои пароли, вводя их на странице подставного ресурса. Как правило, мало кто обращает внимание на необычное имя сервера в адресной строке web-браузера и звонит в службу информационной безопасности.

> Как правило, мало кто обращает внимание на необычное имя сервера в адресной строке web-браузера.

Для защиты от реализации подобного сценария компании:

- внедряют уже упоминавшуюся двухфакторную аутентификацию для того, чтобы перехваченным паролем злоумышленник уже не смог воспользоваться через короткий промежуток времени;
- внедряют виртуальную клавиатуру на странице аутентификации SSL VPN-шлюза;
- настраивают VPN-шлюзы таким обра-

мнение специалиста

Сергей ХАЛЯПИН,
руководитель системных инженеров,
компания Citrix Systems

Защита удаленного доступа к корпоративным ресурсам совершенно справедливо делится на две части: доступ во внутреннюю сеть за счет создания туннеля IPSec VPN и доступ к самим ресурсам, защищенный с помощью SSL VPN.

При построении решений необходимо провести тщательный анализ имеющейся инфраструктуры и потенциальных атак злоумышленников. В результате такого анализа, который должен осуществляться совместно ИТ-службой, отвечающей за эксплуатацию, и службой ИТ-безопасности будет выбрано решение, наиболее полно соответствующее выдвигаемым организацией требованиям. В добавление ко второй схеме, хочется отметить, что такое решение очень хорошо совмещается с решениями терминального доступа. В этом случае список приложений, доступный удаленным пользователям, становится практически не ограниченным.

С точки зрения использования решений по двухфакторной аутентификации наиболее интересное, на мой взгляд, решение One-Time Password, делающее бессмысленным перехват паролей.

Шлюзы SSL VPN действительно можно настроить на проверку конечной точки на соответствие политикам организации. В этой области существуют решения, которые позволяют не только включать/выключать доступ, но и предоставлять его более гранулярно в зависимости от состояния конечной точки, места подключения сотрудника. При работе из наименее защищенных сред, сотрудник, например, получит доступ только на чтение данных, запрет на сохранение информации на локальное устройство и на печать информации на локальных принтерах. В случае подключения этого же сотрудника, с теми же самыми учетными данными из филиала организации с корпоративного ноутбука, он получит максимально разрешенный ему доступ.

мнение специалиста

Николай РОМАНОВ,
технический консультант,
Trend Micro в России и СНГ

Хотелось бы отметить ряд нюансов, связанных с безопасностью на уровне подключения удаленного узла.

Как показали последние несколько лет, основной упор злоумышленники делают именно на широкий спектр возможностей глобальной сети. Распространение получили механизмы подмены DNS-запросов (например, путем заражения удаленного узла вредоносным кодом). Защиту от этого можно реализовать преимущественно на глобальном уровне – например, репутационные сервисы, содержащие информацию об источниках заражения. Подобная защита может дать больший результат, нежели обычное антивирусное ПО, т. к. попадание кода на машину далеко не всегда может быть замечено локально. Если говорить о подделках страниц, через которые производится аутентификация пользователя, то SSL требует наличия сертификата, а подменный сайт, как правило, его не имеет, и в браузере сразу будет выводиться предупреждение.

Как показывает практика, нередко корпоративный ноутбук обладает базовой защитой и далеко не всегда организации прибегают к использованию дополнительных систем. Одним из важнейших аспектов в обеспечении защиты в настоящее время является защита от использования уязвимостей.

В связи с этим, в дополнение к инфраструктурным системам управления обновлениями, очень желательно использовать дополнительные средства: на клиентских машинах, равно как и в системах, через которые производится удаленный доступ, стоит установить HIPS, а также систему контроля критических событий как на уровне приложений, так и на уровне доступа.

Антон КРЯЧКОВ,
директор по продуктам, Aladdin

Обеспечение безопасного доступа к корпоративным информационным ресурсам из любой точки мира – актуальная потребность для бизнеса в современных условиях. Основным барьером для проникновения злоумышленника в корпоративную сеть организации при удаленном доступе была и остается двухфакторная аутентификация на основе аппаратных средств – токенов (смарт-карт, USB-ключей). И на этом аспекте хотелось бы остановиться подробнее.

Основными проблемами, сдерживающими применение токенов на базе смарт-карт, были отсутствие драйверов и ПО промежуточного слоя (криптопровайдера, библиотеки PKCS#11) на удаленных рабочих станциях, например, того же интернет-кафе. И если эта проблема была решена после появления CCID-совместимых USB-ключей (драйвера CCID есть в составе ОС начиная с Windows Vista), то проблема отсутствия на компьютере криптопровайдера, «знающего» как работать с данным токеном, своей актуальности не потеряла. Для ее решения разработчики средств аутентификации предложили многофункциональные USB-ключи на базе смарт-карт, работающие в нескольких режимах. Сразу после подсоединения такого ключа к порту USB, он находится в режиме эмуляции устройства хранения данных и часть памяти смарт-карты представляется операционной системе как содержимое USB CD-ROM диска. С этого диска запускается компактное приложение, которое по протоколу HTTPS соединяется с сервером удаленного доступа (адрес сервера хранится в памяти смарт-карты). Приложение скачивает и проверяет целостность пакета ПО промежуточного слоя (например, криптопровайдера), переводит USB-ключ в режим HID-устройства и «туннелирует» запросы к смарт-карте через HID-драйвер. Самое замечательное, что для реализации описанного сценария работы не требуются права администратора и не изменяется конфигурация ПО на рабочей станции. Браузер прозрачно для себя работает с клиентскими сертификатами на USB-ключе, например для SSL-аутентификации клиента. Такие технологии позволяют существенно повысить надежность защиты доступа в удаленном режиме работы.

зом, чтобы они предъявляли браузеру пользователя электронные сертификаты, подтверждая свою подлинность;

- проводят регулярное обучение сотрудников, которые должны уметь распознавать попытки обмана и угрозы информационной безопасности.

Вирусная атака через ноутбук пользователя

В случае применения технологий IPSec VPN специалистам по информационной безопасности приходится всерьез рассматривать и возможность проникновения вирусов в сеть через систему удаленного доступа. Ведь пользователь не всегда использует свой корпоративный ноутбук для работы. Он выходит в Интернет, загружает файлы, просматривает видео и т. п. Такой компьютер, находящийся какое-то время вне зоны контроля, уязвим для вирусных атак. При подключении зараженного компьютера к корпоративной сети вирус может осуществить атаку на информационные ресурсы компании.

Для защиты от такой угрозы очень часто используют клиентское ПО для удаленного VPN-доступа, которое не позволяет подключиться к корпоративной сети, например, если отключен персональный межсетевой экран или антивирус (что, как правило, является характерным признаком активности компьютерного вируса). В подобных случаях пользователю на помощь приходит SSL VPN, который позволяет ему получить доступ, например, к электронной почте через web-сервис, но в то же время существенно затруднит распространение вируса. Стоит отметить, что и шлюзы SSL VPN можно сконфигурировать таким образом, что специальный Java-апплет (или ActiveX-компонент) будет загружаться в браузер клиента и выполнять проверки безопасности, но этой функцией не всегда пользуются, поскольку она создает ограничения, которые могут быть не приемлемы для бизнеса (например, существует бизнес-требование, что сотрудник должен иметь возможность подключиться к корпоративной сети из любого интернет-кафе).

Кража данных/ мошеннические действия сотрудников компании

Внутренний сотрудник или внешнее лицо, которое каким-то образом смогло получить доступ к корпоративной сети через систему удаленного доступа, может нанести серьезный ущерб своими действиями. Для минимизации подобного риска необходимо разграничение уровней доступа для удаленных пользователей. Каждая группа пользователей должна иметь доступ только к тем ресурсам, которые реально требуются для удаленной работы (принцип «минимальных привилегий»). Компании обычно закрепляют такие правила предоставления удаленного доступа в формализованной процедуре. Ну и конечно, защитой от такого сценария должен стать весь набор мер информационной безопасности, принятых в компании.

Рассмотрев возможные сценарии атак на систему удаленного доступа и меры по защите, можно прийти к справедливому выводу, что обеспечение безопасности удаленного доступа заключается не только во внедрении и грамотной настройке какого-либо современного VPN-решения, но и в реализации компанией необходимых процедур и регулярном обучении сотрудников, причем как технических специалистов, так и обычных пользователей. ■

мнение специалиста

Михаил ОРЕШИН,
директор по развитию, компания «Амрита Групп»

Во-первых, думаю, что в ближайшее время мы отойдем от слова «удаленный» доступ к ресурсам, и останется просто доступ к корпоративным ресурсам. Так как сценариев доступа можно написать бесчисленное множество. По моему мнению, SSL VPN несмотря на более гибкие настройки и политики, более подвержен риску атаки «man in the middle», а точнее «man in the browser», от которой не поможет ни виртуальная клавиатура, ни двухфакторная аутентификация, ни OTP. Соглашусь, что вероятность целевой атаки на данный момент пока не велика, но вопрос уже не стоит как чисто теоретический. Кроме доступа к ресурсам, стоит вопрос управления рабочими станциями, кто за них будет отвечать? Если сам пользователь, то идеально идти в концепции «а-ля SSL VPN» (мы предоставляем в браузере или терминале доступ, что там вокруг – нас мало волнует), если все-таки компания, то смотреть в сторону IPSec VPN (рабочая станция полностью нам подконтрольна). Так что с точки зрения степени применимости SSL VPN больше подходит для контрактных работников, чем для тех, кому нужен доступ к большому количеству ресурсов. Есть еще технология, предложенная Microsoft DirectAccess, которая продолжает идею IPSec VPN, но более прозрачна как для пользователя, так и для ИТ-отдела, и технология виртуализации приложений, отдельных или remote desktop (RDT), тоже решающая задачу доступа к ресурсам компании, и, в конце концов, virtual desktop (VDI).

Алексей ПЛЕШКОВ, начальник отдела защиты информационных технологий, ГПБ (ОАО)

Рассмотренная концепция демонстрирует объединение классических подходов: «secure remote access» и «end-point security». Важным аспектом при принятии решения о внедрении в организации решения, реализующего концепцию удаленного доступа к ресурсам, является юридическая сторона вопроса. В связи с вступлением в силу Федерального закона от 27.07.2006 № 152 «О персональных данных» и постановлений правительства, в которых определены жесткие требования к наличию комплекса организационно-правовых ограничений и к реализации технических мер по защите обрабатываемой информации, сокращается количество аргументов «за» применение удаленного доступа к ресурсам крупной организации. Это усугубляется тем обстоятельством, что на российском рынке промышленных технических решений в настоящее время отсутствуют «коробочные» продукты, в полной мере реализующие предложенную автором концепцию и имеющие при этом необходимый и достаточный набор сертификатов на применяемые технические средства защиты для прохождения организацией проверки уполномоченными органами. Аттестационные и испытательные лаборатории не берутся за аттестацию технических средств и систем, предоставляющих доступ из неконтролируемой зоны к конфиденциальной информации, обрабатываемой внутри защищаемого периметра.

Однако, благодаря очевидному удобству для конечного пользователя, в угоду стремительному развитию бизнеса, зависящего все чаще от оперативного круглосуточного доступа ключевых участников процесса к внутренним информационным ресурсам организации, появляются новые концепции безопасного удаленного доступа.

«Комкор» – привлекательный работодатель

Компания «Комкор», оператор московской мультисервисной сети «Акадо Телеком», признана «Привлекательным работодателем-2009» по итогам исследования, проведенного порталом SuperJob.ru. Исследование проводилось среди 165 тыс. российских работодателей. Цель исследования – определение наиболее востребованных из них с точки зрения соискателей. Звания «Привлекательный работодатель» удостоились компании, которые отвечали нескольким заданным критериям. Компания, претендующая на получение статуса «Привлекательный работодатель», должна была в течение всех четырех кварталов 2009 г. активно подбирать персонал, размещая вакансии на портале SuperJob. Учитывалось среднее количество просмотров вакансий соискателями – этот показатель должен был составлять не менее 500. Основным критерием оценки, влияющим на присуждение звания, стал средний отклик на вакансии – не менее 30 резюме. По результатам исследования, звание «Привлекательный работодатель-2009» получили ведущие предприятия различных отраслевых сегментов экономики, такие как: «Патэрсон», «Мосмарт», Центр внедрения «Протек», «Кока-Кола ЭйчБиСи Евразия» (Москва), «Ингосстрах», «Банк ВТБ 24», «АКБ Росбанк», «Альфа-Банк», ГМК «Норильский никель», World Class, Colliers International FM, Capital Group и др.

www.akado-telecom.ru