Код безопасности
ГК «Информзащита»

# Защита ключевых ресурсов организации с помощью TrustAccess

сентябрь 2011

# Защита ключевых ресурсов организации с помощью TrustAccess

Неослабевающий интерес прессы к теме утечек данных ограниченного доступа неслучаен, ведь масштабы потенциального ущерба от утечек как для коммерческих, так и государственных организаций могут оказаться поистине ужасающими. Негативными последствиями утечки данных могут стать прямые убытки, такие как затраченные на разработку технологических решений, ставших известными конкурентам, средства или проигранные в результате утечек тендеры. К списку потенциальных неприятностей можно также добавить упущенную выгоду из-за испорченного имиджа компании или снижение котировок акций компании (для акционерных обществ), а в случае утечки персональных данных – еще и штрафы со стороны регуляторов и компенсации по судебным искам.

Как показывает практика, жертвами утечек информации становятся и крупные компании, имеющие в своем арсенале серьезные и дорогостоящие системы информационной безопасности. Почему же даже мощные оборонительные системы не всегда могут помочь?

В большинстве случаев внешний периметр корпоративной сети защищен межсетевым экраном, при этом внутренний периметр сети предприятия считается доверенной зоной и дополнительных мер по его защите, как правило, не предпринимается. Конечно, во многих организациях для защиты рабочих мест сотрудников дополнительно используются персональные межсетевые экраны, но они в основном сосредоточены на ограничении доступа сотрудников к интернет-ресурсам. А доступ к серверам контролируется в основном только организационными мерами.

Но достаточно ли для защиты ключевых ресурсов, где хранятся и обрабатываются наиболее ценные для организации данные (например, таких как серверы, рабочее место руководителя или главного бухгалтера), традиционных механизмов? А вы уверены, что ключевые ресурсы вашей организации надежно защищены от сетевых атак зло-умышленников или действий инсайдеров?

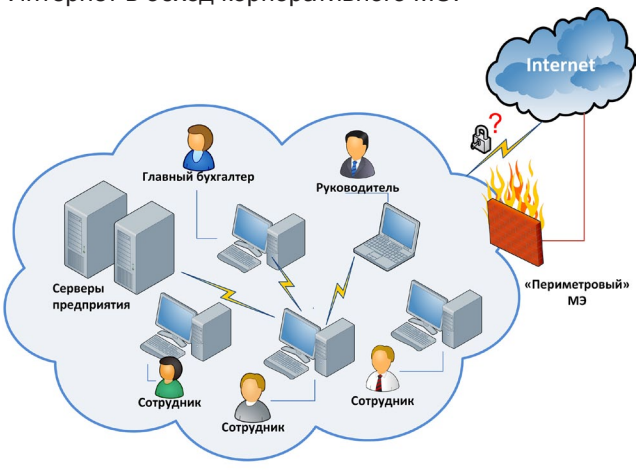
## Неэффективность традиционных межсетевых экранов для защиты ключевых ресурсов организации

Традиционный межсетевой экран, устанавливаемый на границе сети, не дает 100% гарантии защиты ключевых ресурсов организации.

Несомненно, «периметровый» МЭ – весьма эффективная преграда на пути потенци-ального злоумышленника. Но если оборона МЭ будет преодолена, внутренние ресурсы окажутся полностью беззащитны. В арсенале профессиональных хакеров есть масса способов обойти традиционные механизмы защиты, а с развитием современных технологий количество этих способов только возросло.

Одна из основных уязвимостей большинства межсетевых экранов заключена в неправильной конфигурации и настройке. Кроме явных ошибок, к уязвимости могут приводить и вполне осознанные действия персонала. Например, распространенной политикой безопасности является запрет на МЭ всех протоколов, за исключением действительно необходимых. Однако администратор МЭ по просьбе кого-либо из внутренних пользователей может на время разрешить доступ по некоторым протоколам (например, по ICQ). Этого может быть вполне достаточно для успешной атаки на МЭ со стороны злоумышленников.

Следует отметить, что успешная атака возможна и без преодоления механизмов защиты межсетевого экрана. Зачем пытаться проникнуть к ресурсам через защитные средства, когда можно попытаться их обойти? Например, простым техническим средством для обхода защиты МЭ может стать мобильный телефон, который применяется легальным пользователем (невольным сообщником) для доступа в Интернет в обход корпоративного МЭ.



Еще одним не менее важным недостатком «периметровых» межсетевых экранов является невозможность обеспечить защиту внутренних ключевых ресурсов предприятия от инсайдера. Традиционный МЭ позволяет только просматривать трафик на границах между внутренней и внешней сетями – если трафик не проходит через него, то никаких признаков атаки и не обнаруживается. В общем-то, ни один, даже самый эффективный и многофункциональный МЭ, не позволит обнаружить попытку обойти его со стороны легального пользователя изнутри сети. А именно внутренний нарушитель и является в большинстве случаев «злоумышленником», виновным в утечке конфиденциальной информации. При этом в большинстве случаев действия инсайдера не носят злоумышленный характер. Как правило, причиной утечки является халатность, невнимательность и необдуманные действия сотрудников организации.

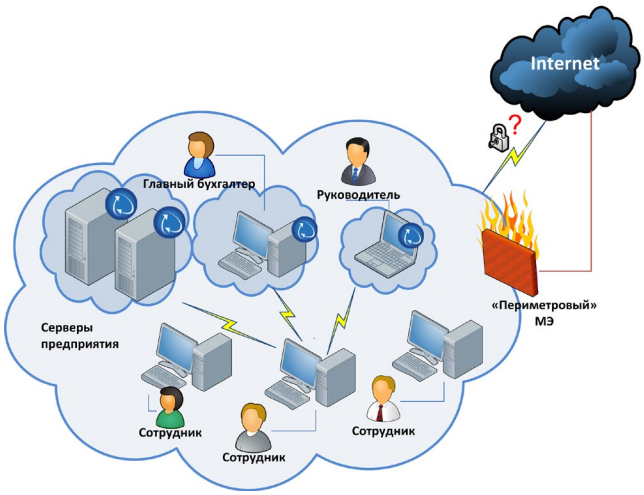
## Варианты защиты ключевых ресурсов организации

Но если традиционный «периметровый» МЭ не гарантирует 100% защиты ключевых ресурсов организации, каков же тогда выход?

Наиболее простым и наименее затратным способом защиты любых ресурсов являются организационные меры. Например, можно попросту ограничить физический доступ к ключевым ресурсам или выделить их в отдельный сегмент сети. К сожалению, такой подход не всегда эффективен или вообще применим. В частности, сервер БД выделить в отдельный сегмент сети вряд ли получится, поскольку клиентские приложения на рабочих местах пользователей должны иметь возможность обратиться к серверу БД за данными.

Внедрение криптографических методов, таких как ЭЦП или шифрование передаваемого по локальной сети предприятия трафика, хотя и эффективно, но сопряжено со значительными техническими трудностями и финансовыми расходами. К этому можно добавить неизбежное снижение скорости трафика в сети, а также необходимость периодического выпуска и замены сертификатов.

Применение распределенного межсетевого экрана TrustAccess, предназначенного именно для защиты ключевых ресурсов сети, позволит обеспечить эффективную защиту самых важных ресурсов организации от сетевых угроз без применения традиционных криптографических средств.




В отличие от «периметровых» межсетевых экранов, TrustAccess функционирует непосредственно на защищаемых объектах, обеспечивая их защиту от сетевых угроз как со стороны внешнего нарушителя, так и инсайдера. В качестве защищаемых объектов могут выступать: сервер баз данных, сервер бухгалтерии, компьютер руководителя или главного бухгалтера,– одним словом, ключевые ресурсы организации. Помимо традиционного для межсетевых экранов механизма фильтрации сетевых соединений, TrustAccess также обеспечивает аутентификацию, позволяющую разграничить сетевой доступ к защищаемым информационным системам.

## Шесть аргументов в пользу TrustAccess

### 1. Сертифицированная защита

TrustAccess сертифицирован во ФСТЭК России по уровню МЭ2 и НДВ4[1], что позволяет использовать его для защиты информационных систем персональных данных до класса К1 включительно. Продукт позволит выполнить требования к системе защиты персональных данных (в соответствии с требованиями приказа ФСТЭК России №58) не только в части обеспечения безопасного межсетевого взаимодействия, но и закроет требования к некоторым другим подсистемам (например, подсистемам управления доступом, регистрации и учета[2], контроля целостности[3]).

### 2. Мощные защитные механизмы

TrustAccess – межсетевой экран второго класса[4] с широким набором защитных механизмов.

- Аутентификация сетевых соединений

Механизм аутентификации, реализованный в TrustAccess, основан на протоколе Kerberos, нечувстви-тельном к попыткам перехвата паролей и атакам типа Man in the Middle. Аутентификации подле-

1 Имеется также усиленная версия продукта для защиты государственной тайны.
2 Выполняются с некоторыми ограничениями.
3 Частично выполняются.
4 Согласно классификации РД Гостехкоммиссии при Президенте РФ «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации».

жат не только субъекты доступа, но и защищаемые объекты, там самым, обеспечивается защита от подмены защищаемого объекта. Возможна двухфакторная аутентификация с использованием персональных идентификаторов eToken и iButton.

- Фильтрация сетевых соединений

Правила фильтрации TrustAccess обладают широким диапазоном настроек. Сетевые соединения можно ограничить на уровне сетевых протоколов, портов, пользователей, групп пользователей, параметров прикладных протоколов, временных интервалов. Возможна настройка реакции на срабатывание правил фильтрации.

- Защита от replay-атак

Для защиты от replay-атак применяется ISAKMP-ассоциация.

- Защита сетевого взаимодействия

Защита сетевого взаимодействия достигается посредством использования протоколов семейства IPsec:

- AH (Authentication Header) – позволяет гарантировать аутентичность и целостность передаваемых данных каждого IP-пакета и, как следствие, обеспечивает защиту от атак типа Man in the Middle;
- ISAKMP – предназначен для обмена ключами и согласования параметров соединения.

- Ограничение работы по некоторым сетевым протоколам

Можно разрешить или запретить сетевые соединения по протоколам согласно RFC 1700, а также по IPv4, IPv6 или Novell IPX.

- ICMP-защита

Гибкая настройка организации обмена сообщениями по межсетевому протоколу ICMP позволит обеспечить защиту от большинства атак отказа в обслуживании.

## 3. Защита от сетевых атак

TrustAccess – эффективная защита от большинства известных сетевых угроз:

| | |
|---|---|
| Man in the Middle | √ |
| Подмена защищаемого объекта | √ |
| Replay-атака | √ |
| IP-спуфинг | √ |
| Перехват сетевых пакетов | √ |
| Прослушивание сети | √ |
| Подмена сетевых пакетов | √ |
| Отказ в обслуживании | √ |

## 4. Прозрачность для приложений

Защитные механизмы TrustAccess абсолютно прозрачны для приложений: нет необходимости вносить изменения в логику работы информационных систем, дорабатывать приложения или менять протоколы сетевого взаимодействия компонентов информационной системы. Следует также отметить, что внедрение TrustAccess не требует реконфигурации сети или приобретения дополнительного оборудования.

## 5. Подтвержденная сместимость с ОС Windows

Компоненты TrustAccess могут функционировать на компьютере под управлением практически любой операционной системы семейства Windows.

Важным преимуществом TrustAccess является наличие статусов совместимости Microsoft Works with Windows Server 2008 R2 и Microsoft Works with Windows 7. Драйверы TrustAccess протестированы в соответствии с методикой Microsoft и подписаны сертификатом WHQL (Windows Hardware Quality Lab).

Совместимо с Windows 7

Works with Windows Server 2008 R2

## 6. Разнообразные сценарии использования

TrustAccess позволяет максимально ограничить доступ к серверу БД в многозвенных ИСПДн или разграничить доступ к серверам разных отделов предприятия на основе должностей пользователей. Кроме того, TrustAccess позволяет решить важную практическую задачу – снижение класса ИСПДн путем сегментирования сети с целью сэкономить затраты. TrustAccess может применяться для разграничения доступа пользователей к файл-серверу на уровне общих папок. Защитные механизмы TrustAccess эффективны в современных конфигурациях информационных систем (при терминальных соединениях и на виртуальных машинах).

Следует отметить, что TrustAccess имеет статус VMware Ready и внесен в каталог партнерских продуктов VMware.

vmware READY

Код безопасности
ГК «Информзащита»

Почтовый адрес: 127018, Россия, Москва, а/я 55.
Адрес офиса в Москве: ул. Образцова, д. 38.
Адрес офиса в Санкт-Петербурге: Свердловская наб., д. 44.
Тел.: +7 (495) 980-2345 (многоканальный).
Факс: +7 (495) 980-2345.
E-mail: info@securitycode.ru
Запрос дополнительной информации о продуктах: info@securitycode.ru
По вопросам стоимости и покупки продуктов sales@securitycode.ru
По вопросам партнерства и сотрудничества info@securitycode.ru

Вы можете узнать подробную информацию о продуктах на сайте
www.securitycode.ru

**О компании «Код Безопасности»**

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, коммерческой и государственной тайны, а также среды виртуализации. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

«Код Безопасности» входит в группу компаний «Информзащита», которая уже около 15 лет является лидером российского рынка информационной безопасности.

ООО «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России и ФСБ России.