Код безопасности
ГК «Информзащита»

Эффективная система защиты — главное оружие против компьютерных преступлений

Юлия Смирнова
Менеджер по развитию направления компании «Код Безопасности»

Статистика такова, что в России большинство уголовных дел по компьютерным преступлениям остаются нераскрытыми. Действующие нормы уголовного, уголовно-процессуального и административного законодательства в области компьютерных преступлений показывает отсталость, неточность и противоречивость нормативной базы. Можно сказать, что практически единственной преградой для преступников является очередное техническое решение, а не перспектива попасть на судебную скамью.

Как показывает практика, жертвами компьютерных преступлений становятся и крупные компании, имеющие в своем арсенале серьезные и дорогостоящие системы информационной безопасности. Почему же даже мощные оборонительные системы не всегда могут предотвратить компьютерное преступление?

Почему дорогостоящие системы защиты не панацея от компьютерных преступлений

Давайте заглянем внутрь инфраструктуры любого предприятия. Что же мы увидим? Обычно защита внутренней сети предприятия ограничивается обеспечением защиты от внешних сетевых угроз. Для этого используется межсетевое экранирование, организация VPN, шифрование и другие механизмы. Внутренний же периметр сети предприятия считается доверенной зоной и, как правило, дополнительных мер по его защите не предпринимается. С развитием современных технологий создание доверенного периметра уже не столь эффективно — злоумышленник может получить доступ внутрь корпоративной сети, например, по Wi-Fi, минуя маршрутизатор с системой защиты.

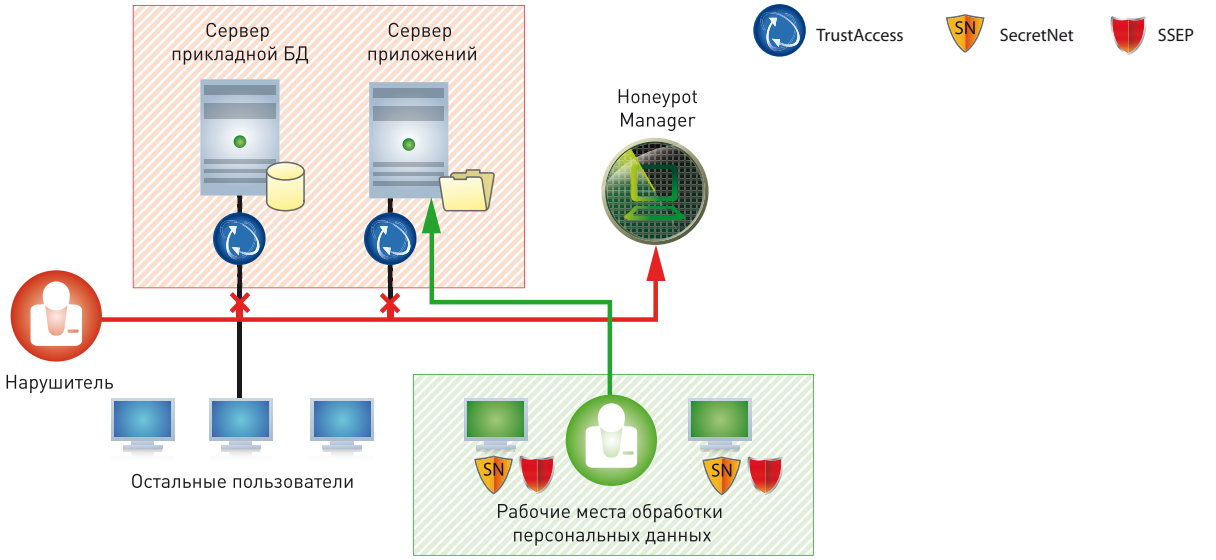
Большинство современных информационных систем, где обрабатываются данные ограниченного доступа, имеют клиент-серверную или многозвенную архитектуру. Традиционные средства защиты от несанкционированного доступа сконцентрированы на защите локальных файловых ресурсов, но даже если таковые используются, они не гарантируют защиту информации при ее передаче по сети. Выходом может стать применение распределенного межсетевого экрана с функцией аутентификации сетевых соединений.

Согласно статистике, большинство утечек конфиденциальной информации происходит по вине инсайдера. Нередко сотрудники предприятия использует легко подбираемые пароли, теряют «флешки» с важной информацией, страдают от вирусов и спама из Интернета — порой персоналу компании просто не хватает грамотности в вопросах обеспечения информационной безопасности. В связи с этим построение эффективной системы защиты информации невозможно без полноценной защиты рабочих мест пользователей.

Пример построения эффективной системы защиты информации

На схеме продемонстрирован сценарий защиты внутренней сети организации. Конфиденциальная информация обрабатывается в информационной системе, имеющей трехзвенную архитектуру (конфиденциальная информация обрабатывается на рабочих местах пользователей, сервере приложений и сервере БД).

Средство защиты от НСД Secret Net и Security Studio Endpoint Protection обеспечат все необходимые защитные механизмы отдельного компьютера. Распределенный межсетевой экран TrustAccess, в свою очередь, обеспечит разграничение доступа и сетевую защиту серверов. Доступ к серверу приложений получат только пользователи системы, доступ к серверу БД — только сервер приложений. Для всех остальных пользователей локальной сети доступ к серверам будет запрещен. Honeypot Manager позволит зафиксировать попытки неавторизованных пользователей получить доступ к системе с конфиденциальной информацией.



Пару слов в заключение

Построение эффективной системы защиты может стать главным оружием против компьютерных преступлений. А использование систем обнаружения несанкционированного доступа и вторжений на базе имитации данных позволит отследить попытки совершения компьютерных преступлений и вовремя на них среагировать.

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. «Код Безопасности» входит в группу компаний «Информзащита» – признанного лидера в сфере информационной безопасности – и является преемником её многолетних наработок в области создания средств защиты информации для государственных и коммерческих заказчиков.