



Код безопасности
ГК «Информзащита»

Предотвращение мошенничества и утечек информации в информационных структурах банков с использованием технологий сенсоров-ловушек

Проблематика

Для бизнеса любого банка критичной информацией, нуждающейся в качественной защите, являются в первую очередь данные о собственной операционной деятельности (счета, проводки, финансовые отчеты). Кроме того, любой банк также имеет дело с персональными данными своих клиентов (идентификационные данные, номера счетов, финансовые показатели и т.д.). Но вот вопрос: как эффективно защитить данные, которые могут храниться и обрабатываться практически в любом сегменте, узле, приложении или компьютере сети организации?

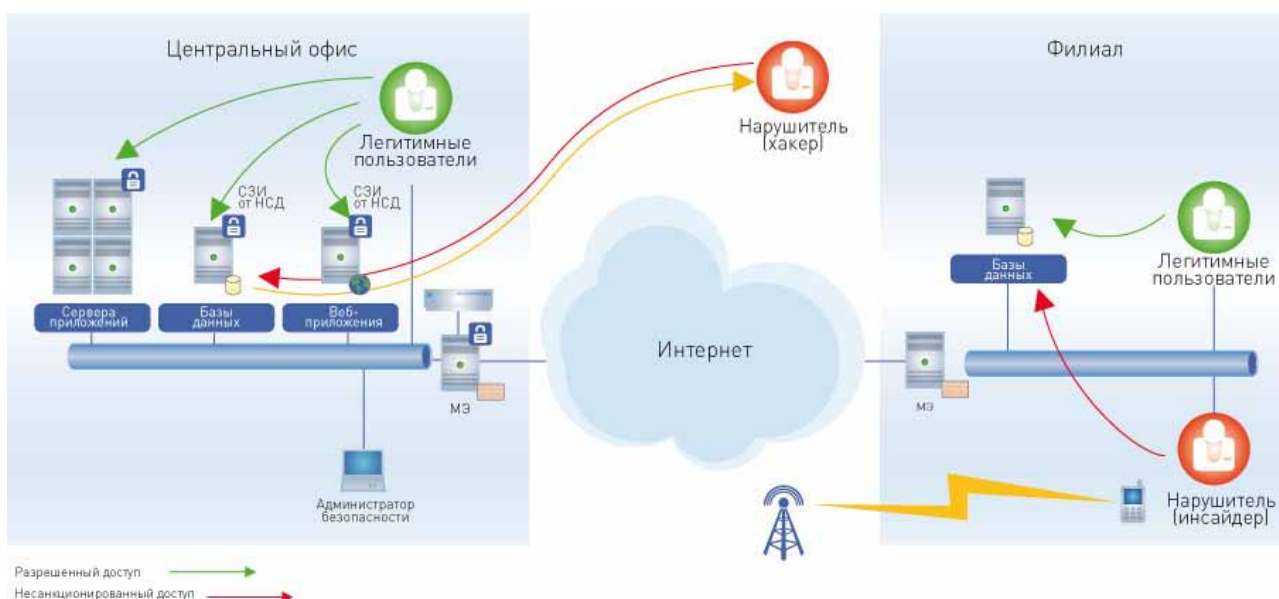
А ведь помимо этого еще необходимо удовлетворять требованиям стандартов (PCI DSS, СТО БР) и регуляторов (БР, ФСТЭК), предъявляемым к банкам. Это особенно актуально ввиду того, что не так давно правительством РФ были законодательно закреплены статус персональных данных и требования по их защите со стороны обрабатывающих их организаций.

Традиционные подходы к безопасности работают далеко не всегда. Как известно, ни одно средство не гарантирует 100%-ной защиты данных, поэтому для обеспечения сетевой безопасности используются различные типы средств: брандмауэры и прокси-серверы – для защиты периметра, серверные и персональные средства безопасности – для защиты компьютеров, специальные средства используются также для обнаружения атак и утечек данных, для защиты виртуальных сетей. Также, как правило, в любой сети используются политики безопасности для управления учетными записями пользователей и компьютеров.

Однако даже при наличии всех традиционных средств защиты все равно существуют угрозы, от которых сеть не застрахована и которые реализуются вследствие недостатков или особенностей проектирования тех или иных традиционных средств защиты. Например, межсетевой экран может надежно защищать от проникновения внутрь сети, но не препятствует передаче данных во внешнюю сеть. Кроме того, он не препятствует работе во внутренней сети всевозможных мобильных устройств, так как трафик этих устройств не проходит через шлюзы – наблюдается так называемое исчезновение периметра сети. Антивирус является средством «реактивной защиты», зависящим от частоты обновлений баз сигнатур вредоносного ПО. Персональные СЗИ от НСД не всегда блокируют съемные носители и сетевые USB-устройства. Что касается COB, то зачастую среди всей регистрируемой ими информации бывает сложно выделить критичные события и они не всегда понимают атаки на прикладные программы. К тому же сложные IDS- и DLP- системы требуют наличия специально обученного персонала и больших материальных затрат на поддержание их работы и анализ их деятельности.

Кроме того, всегда существует вероятность кражи информации со стороны сотрудников организации – инсайдеров.

Таким образом, возможность получения нежелательного доступа к внутренней сети предприятия злоумышленником, который ищет доступные ресурсы компании, существует даже при использовании комплексного подхода к безопасности. А ведь цена утечки конфиденциальной информации может быть очень высока – как финансовая, так и репутационная.



Именно поэтому в различных организациях все большей популярностью пользуются системы раннего обнаружения и предотвращения атак, работающие на основе косвенных признаков (поведение систем и пользователей), такие как системы обнаружения вторжений и корреляции событий. Преимущество таких систем в том, что они способны противостоять не только известным, но и новым угрозам.

Как раз одним из таких средств, позволяющих значительно повысить безопасность информационной сети, являются honeypot-системы.

Что такое honeypot?

Идея honeypot проста и известна с незапамятных времен – нарушителя ловят на приманку. В локальной сети размещается легкодоступная и привлекательная для нарушителя цель, внешне неотличимая от реальных ресурсов, единственное предназначение которой – попасться на глаза нарушителю, спровоцировать его на неправомерные действия и сообщить «куда следует» о факте «контакта».

Другими словами, honeypot – это система обнаружения попыток несанкционированного доступа к информационным ресурсам. Honeypot имитирует работу реальной системы, являющейся потенциальной целью атак и несанкционированного доступа, отвлекает на себя внимание и ресурсы нарушителя, фиксирует все его действия и информирует службу безопасности о фактах нарушений. При этом, в зависимости от типа honeypot, имитироваться могут любые системы, служащие потенциальными объектами для атак: серверы, базы данных, сетевые сервисы, файловые ресурсы и т.д.

Преимущества использования honeypot-систем

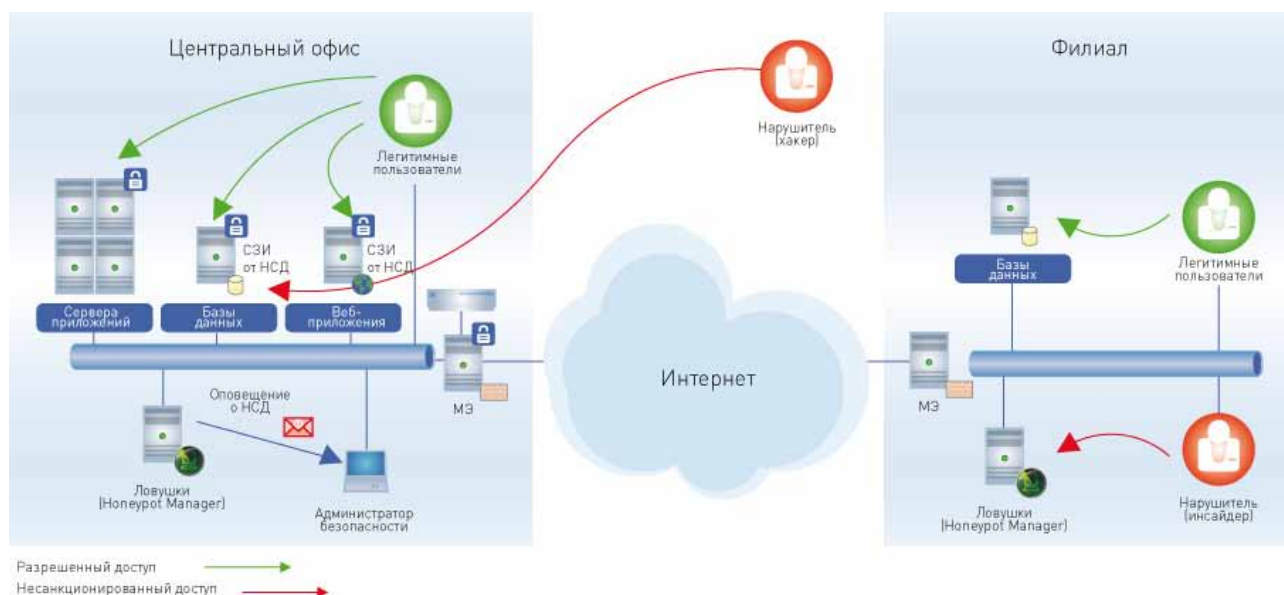
Технология honeypot является одним из наиболее эффективных и доступных средств раннего предупреждения, обнаружения и противодействия атакам на сетевые ресурсы.

Преимущества honeypot-систем определяются самим принципом их работы. Прежде всего, это практически полное отсутствие ложных срабатываний. Поскольку honeypot лишь имитирует реальную систему и к нему не обращаются ни реальные пользователи сети, ни легальные сетевые приложения, то любая активность на honeypot и любая попытка обращения к нему является несанкционированной и свидетельствует либо об атаке, либо об исследовании сети с целью найти уязвимые места в ее защите.

Отсюда следует и еще одно преимущество – обнаружение новых типов атак, так как активность на ловушке регистрируется независимо от типа атаки.

Предупрежден – значит вооружен

Honeypot позволяет снизить риск сетевых атак на реальные системы, предупреждая, обнаруживая и протоколируя деятельность нарушителя. Установленный и грамотно настроенный honeypot отвлекает внимание и ресурсы нарушителя от реальных систем, позволит выявить попытку атаки, предоставит информацию для ее изучения и даст дополнительное время для принятия адекватных мер защиты.



Возможность понять цели, методы и средства нарушителя

Определение факта атаки является важнейшим моментом для администраторов, так как позволяет оперативно принять меры противодействия. Но помимо этого honeypot позволяет также получить информацию, необходимую для изучения поведения, методов и инструментария нарушителя. Дело в том, что honeypot позволяет сохранить следы воздействия для дальнейшего расследования. Атакующую honeypot-систему можно спокойно отключить и передать для анализа собственным или внешним специалистам по информационной безопасности, что обычно невозможно для реального сервера корпоративных приложений.

По оставленным нарушителем следам можно узнать об используемых им методах и средствах атаки, а также сделать выводы о ее целях. При этом важной особенностью honeypot-систем является сравнительно небольшое количество информации, которую нужно изучать при расследовании инцидента. Реальные системы сети протоколируют огромное количество информации, в связи с чем расследование инцидентов ИБ на основе логов многочисленных сетевых приложений и систем является довольно трудоемкой задачей. Honeypot, напротив, содержит только нужную информацию, связанную с фактами нарушений. Так как никакой легальной активности на нем не происходит.

Security Studio Honeypot Manager

Security Studio Honeypot Manager (далее – Honeypot Manager) – новый продукт компании «Код Безопасности» – представляет собой готовую к использованию honeypot-систему, имитирующую сетевые бизнес-приложения с подставными данными. Honeypot Manager позволяет обнаруживать вторжения нарушителей в локальную вычислительную сеть предприятия и анализировать их действия без снижения производительности реальных систем хранения и обработки данных, а также без непосредственной угрозы потери ценной информации.

Honeypot Manager регистрирует любые действия в контролируемом приложении, которое фактически является специальным сенсором-ловушкой, проводит регулярный аудит собранных данных и анализирует их на соответствие настроенным правилам уведомлений. Результаты анализа активности регистрируются в журнале в виде сообщений о фактах НСД с указанием информации о компьютере и учетной записи потенциального нарушителя, времени и характере доступа, а также могут отправляться по электронной почте для уведомления заинтересован-

ных лиц.

Все записи аудита хранятся в отдельной базе данных и доступны для последующего анализа даже в случае порчи сенсора нарушителем или краха системы. Настраиваемая система отчетов на основе Microsoft SQL Server Reporting Services позволяет производить анализ активности и видеть статистику работы системы.

Продукт позволяет имитировать работу приложений, используемых в т.ч. для обработки и хранения персональных данных и конфиденциальной информации – баз данных и файловых серверов. Поддерживается имитация как двух-, так и трехзвенных приложений баз данных.

Honeypot Manager не избавляет от возможности получения нежелательного доступа к внутренней сети предприятия, но снижает риск и позволяет использовать полученную с его помощью информацию для построения более эффективных и надежных систем защиты реальных приложений и сетей.

Требования стандартов и регуляторов

Honeypot Manager обладает сертификатом ФСТЭК России, подтверждающим его соответствие требованиям по 4 уровню контроля отсутствия НДВ. Кроме того, ФСТЭК России официально подтвердил возможность использования Honeypot Manager в ИСПДн до первого класса (К1) включительно.

Что особенно ценно для банков, продукт помогает выполнить требования, предъявляемые Международным стандартом безопасности данных индустрии платежных карт PCI DSS и стандартом Банка России СТО БР.

Выводы – нужно ли использовать Honeypot Manager в информационной структуре банка?

Коротко говоря – да, по следующим причинам:

1. Honeypot Manager позволит своевременно выявить попытки несанкционированного доступа к критичным для банка ресурсам (базам данных и файловым серверам) и принять необходимые меры по устранению либо снижению рисков потери или кражи конфиденциальной информации или выведения из строя бизнес-приложений.
2. Honeypot Manager даст возможность компенсировать слабые стороны и недостатки классических СЗИ, таких как межсетевой экран, IDS и СЗИ от НСД.
3. Применение Honeypot Manager позволит снизить финансовые и репутационные риски, возникающие в виде штрафов и/или остановки деятельности компании по результатам проверок уполномоченных органов, в том числе в части защиты персональных данных.



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.