А.СЫЧЕВ: НЕ ОЦЕНИВ ПОТЕНЦИАЛЬНЫЙ УЩЕРБ И РЕАЛЬНО СУЩЕСТВУЮЩИЕ РИСКИ, НИ ОДИН УВАЖАЮЩИЙ СЕБЯ РУКОВОДИТЕЛЬ БАНКА НЕ НАЧНЕТ ТРАТИТЬ ДЕНЬГИ.

забываются «ключи». Как с этим борются? Путем мотивации персонала. Но мотивация зачастую играет против банка: никто из специалистов не признается в нарушении правил из страха быть оштрафованным, лишиться премии и т.д.

Что делать? На мой взгляд, применять подход, при котором необходимо «поставить» системы так, чтобы правила нельзя было не выполнить. А для этого необходимо объединять уже существующие в банках системы информационной безопасности и системы физической безопасности. В частности, нужно четко идентифицировать объект, применять биометрическую идентификацию. Необходимо иметь информационный «след» – что делает конкретный специалист на протяжении всей его работы. Это достигается с помощью видеонаблюдения, систем контроля доступа, бюро пропусков, наконец, – и вся эта структура должна определять информационный «след». Необходимо также определить ряд регламентов, которые мы должны отслеживать с помощью систем информационной и физической безопасности.

Резюмируя свое выступление, хочу сказать: возникает некий новый «пласт», который очень жестко связан с «человеческим фактором». Крайнее выражение этого фактора – инсайд. А борьба с ним – это не подключение имеющихся средств, а дополнение их специальными системами, объединяющими информационные и физические средства безопасности. И интегрирующая система, которая стоит над этими системами и заставляет всех сотрудников без исключения выполнять административные правила.

А. СЫЧЕВ: Вы говорите абсолютно верные вещи, но верные только в одной части – когда мы касаемся деятельности банка в части миддл- и бэк-офиса. Когда же мы говорим о бизнес-деятельности банка, то вопрос обеспечения информационной безопасности надо понимать гораздо шире. Потому что речь, в первую очередь, идет о клиентах, а клиенты, к сожалению, – потенциальная угроза. Так, например, наш опыт показывает, что очень часто, осуществляя обмен информацией с клиентами в электронном виде, мы фиксируем на стороне клиента заражения вредоносным программным обеспечением. Естественно, это представляет потенциальную угрозу информационным системам банка. И эту проблему невозможно решить путем различных интеграций, написания регламентов и т.д.

На самом деле проблему надо рассматривать в более широком смысле. Информационная безопасность банков должна обеспечиваться отработкой неких сервисов безопасности, которые предоставляются как внутри банка, так и его клиентам. Потому что риски, которые «несут» в банк наши клиенты, не менее серьезны, чем риски, возникающие в результате инсайда. Кроме этого, есть понимание, что даже внутренние бэк-офисные технологии тоже могут быть небезопасными – не потому что кто-то потерял пароль или кто-то работает не в здании банка, а в удаленном режиме, а потому что технологии сами по себе построены без учета требований безопасности и не могут обеспечить адекватный уровень информационной безопасности. Поэтому вопрос, по моему убеждению, надо рассматривать комплексно, не «завязываясь» только на его технических аспектах.

Д. ГОРЕЛОВ: 100-процентно защищенная система – это система, которая не работает. Мы никогда не знаем, что будет в дальнейшем с технологиями, со злоумышленниками, поэтому всегда будет иметь место борьба между мечом и щитом. И самая большая проблема, что в идеальных 100% самыми дорогими для банка становятся последние два-три – 98-99%. Поэтому не всегда стоит стремиться к безопасности на уровне 99,99%, разумнее остановиться на уровне 97% – но это будет как раз та степень защищенности, которая необходима банку. И финансово-кредитной организации не придется тратить на системы безопасности столько денег, что ее деятельность просто станет невыгодной.

С. ПАВЛОВСКИЙ: По моему убеждению, те, кто говорит о 100-процентной информационной безопасности в своих банках, просто занимаются самолюбованием или самоуспокоением. И то и другое – самый короткий путь к краху. Мы же понимаем, что ситуация постоянно меняется и, следовательно, постоянно возникают новые вызовы и риски.

Здесь уже говорилось о «человеческом факторе» в разрезе инсайда. Этот фактор, с моей точки зрения, важен и когда речь идет о клиентах. Клиенты, к сожалению, не всегда в состоянии понять и оценить уровни рисков. Поэтому с каждым из них необходимо разговаривать на понятном ему языке. Необходимо донести до него, какие риски возможны и какие потери он лично может понести в случае реализации этих рисков. Чтобы достичь этого, в свою очередь, необходим контакт с клиентом. Если он налажен, то это путь к обеспечению комфортного для банка уровня информационной безопасности.

Е. АКИМОВ: Мне приходилось сталкиваться с прямо противоположным мнением: спасение утопающих – дело рук самих утопающих. Если у клиента нарушена конфиденциальность ключей шифрования и ЭЦП, то некоторые банки склонны воспринимать это исключительно как проблему самого клиента, что, конечно, не так.

Причем наиболее эффективно эта задача решается не только разъяснительными мерами и даже не обязательствами по защите клиентского места (AV, HIPS и пр.), прописанными в договоре, а более комплексно. Прежде всего, из мер, существенно снижающих возможности для мошенников, надо отметить создание fraud machine, осуществляющих в том числе мониторинг банковских транзакций, интеллектуально проверяя их на возможность мошенничества.

Наша дискуссия о возможности или невозможности стопроцентной безопас-

МНЕНИЕ ЭКСПЕРТА

Владимир КОБЫЛЯНСКИЙ, советник исполнительного директора по информационной безопасности компании BSS

Специфика текущего положения дел такова, что внешними угрозами для банков, по сути, являются только DOS-атаки. Злоумышленники в подавляющем большинстве случаев не тратят силы на преодоление системы защиты информации банков (которые обычно находятся все же на достаточно приличном уровне). А вот внутренние (инсайдерские) атаки представляют действительно серьезную угрозу. Как правило, к защите от внутреннего нарушителя банки относятся достаточно небрежно. А зря, поскольку инсайдер может нанести весьма существенный урон.

Методы борьбы с инсайдом существуют.

Использование технических средств:

- строгая аутентификация сотрудников (например, с помощью USB-ключа или биометрии);
- аудит всех действий всех пользователей (включая администраторов) в сети;
- использование средств защиты конфиденциальной информации от инсайдеров;
- шифрование конфиденциальных данных.

Использование организационных мер:

- обучение сотрудников, отвечающих за информационную безопасность;
- повышение личной ответственности сотрудников;
- постоянная работа с персоналом, имеющим доступ к конфиденциальной информации (инструктаж, обучение, проверка знания правил и обязанностей по соблюдению информационной безопасности и т.д.).

Пожалуй, в числе самых распространенных остаются инциденты, связанные с использованием системы дистанционного банковского обслуживания.

Существует несколько основных типов атак:

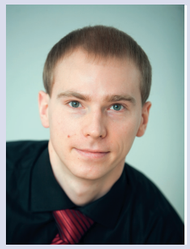
- атака типа «человек посередине»;
- кража ключевого контейнера;
- атака удаленного управления.

Против всех эти типов атак уже разработаны и активно применяются меры противодействия, а именно:

- шифрование передаваемых данных;
- использование технологии ЭЦП;
- использование отторгаемых носителей (токенов), в том числе и с неизвлекаемыми ключами;
- использование одноразовых паролей;
- использование виртуальных клавиатур;
- использование систем оповещения;
- использование систем фрод-анализа.

Новым типом атак является «атака подмены документа». В процессе данной атаки злоумышленник с помощью вредоносного программного обеспечения подменяет реквизиты платежного поручения перед его отправкой банку. Причем для пользователя подмена реквизитов происходит совершенно незаметно, а потому он, ни о чем не подозревая, подписывает поддельный документ с помощью своей ЭЦП, вводит одноразовый пароль и отправляет поручение в банк. Методом противодействия таким атакам является использование средств визуализации подписываемых данных, которые сейчас активно внедряются разработчиками систем ДБО.

SIEM КАК «ЧЕРНЫЙ ЯЩИК»



Александр КУЗНЕЦОВ, руководитель отдела безопасности информационных систем НТЦ «Вулкан»

Не случайно на «круглом столе», посвященном информационной безопасности в банках, был поднят вопрос об «информационном следе»: методичная фиксация действий конкретных специалистов в течение рабочего дня – действительно важная мера в борьбе с инсайдом. Хотел бы, однако, добавить, что данных видеонаблюдения, СКУД, бюро пропусков может оказаться недостаточно для выявления и расследования инцидента, связанного с «внутренним человеческим фактором». Все чаще ставится вопрос о максимально широкой регистрации действий пользователей не только на уровне «физики», но и в информационной среде. А в большой ИТ-инфраструктуре штатных средств приложений, ОС и СУБД для этого может оказаться недостаточно. Во всяком случае, вопрос типа «Кто входил в домен с 11.00 до 11.30 шесть месяцев назад?» очень часто остается без ответа: как правило, «логи» так долго не хранят, а если хранят, то возможности по их обработке ограничены.

Эта проблема может эффективно решаться путем применения систем управления событиями и информацией о безопасности (SIEM) – решений, обеспечивающих централизованный сбор и анализ регистрационной информации со всей ИТ-инфраструктуры. В рассматриваемом аспекте эти системы становятся своего рода аналогом «черного ящика» – авиационного бортового регистратора, фиксирующего параметры полета и использующегося при расследовании летных происшествий. Сегодня SIEM представлены на рынке такими продуктами, как RSA enVision, ArcSight, QRadar. Банки имеют возможность выбрать наиболее подходящее решение и реализовать у себя комплексную систему регистрации и анализа событий.

Важно отметить и тот факт, что осознание гарантированной и беспристрастной регистрации ключевых действий в информационной системе хорошо дисциплинирует персонал и является неплохой профилактической мерой.