ОБРАТНАЯ СТОРОНА ПРИВИЛЕГИЙ

ПРОБЛЕМЫ КОНТРОЛЯ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ В КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ И ПУТИ ИХ РЕШЕНИЯ

Виктор СЕРДЮК
генеральный директор
АО «ДиалогНаука»

Михаил РОМАНОВ
директор по развитию бизнеса ООО «Новые технологии безопасности»

На сегодняшний день информационные системы кредитно-финансовых учреждений стали достаточно сложными и многокомпонентными. Создание и вывод на рынок различных банковских продуктов, как правило, требуют разработки новых информационных систем. Эти системы виртуализируются, консолидируются в специальных вычислительных центрах (ЦОДах), а определенные системы мигрируют в «Облака». И, если раньше было достаточно иметь одного-двух администраторов для управления банковскими приложениями, которые успешно обслуживали все информационные системы организации, то сейчас это невозможно ввиду сложности и многообразия современных ИТ-систем.

Сегодня на первый план выходят риски, связанные с неконтролируемым административным доступом к информационным системам и ИТ-инфраструктуре компаний. По данным ведущих аналитиков, более 70% нарушений ИБ происходят именно по вине привилегированных пользователей. Хакеры или злоумышленники также сначала ищут возможность повысить свои привилегии в системах, а затем, имея хороший контроль над целевой системой, делают несанкционированные действия по краже, изменению, удалению платежной и другой информации в финансовой организации. Обычные пользователи, как правило, контролируются достаточно серьезно — применяются средства аутентификации, механизмы разделения полномочий, системы регистрации событий безопасности и другие решения. Однако вопросы контроля того, что делают так называемые привилегированные пользователи, до сих пор остаются в стороне во многих организациях. А по сути эти пользователи по умолчанию имеют очень высокий уровень доступа в систему и к различным конфиденциальным данным.

Кроме того, для обеспечения работоспособности своих систем большинство кредитно-финансовых организаций предоставляют доступ к своим корпоративным ресурсам внешним специалистам в рамках контрактов по аутсорсингу или удаленной работе. К тому же количество внутренних администраторов в ряде банков может доходить до нескольких десятков. Кроме того, ряд задач ИТ-подразделений компании, например, задачи по настройке специализированного оборудования, часто осуществляются силами вендора. Данный подход экономически оправдан, однако он несет дополнительные риски информационной безопасности. Так, в частности, бывает невозможно определить, кто и что делал в системе, так как, например, учетная запись Суперпользователя (root, Administrator и др.) в системах часто одна, а доступ с её правами необходимо обеспечить и вендору, и администратору, и консультанту.

Рассмотрим простой пример — после новых настроек в ПО или применения очередного обновления «боевая» информационная система банка перестала работать. В данном случае для оперативного восстановления работоспособности системы необходимо понять, какие действия администраторов привели к сбою и кто именно допустил ошибку. Хорошо известно, что время простоя платежных и других систем банка является в прямом смысле «золотым». Журналы аудита, как правило, лишь в редких случаях помогают решить указанную проблему, так как протоколирование абсолютно всех действий в системе обычно не заложено в ПО. Даже если такие уровни журналирования и предусмотрены в ПО, то они не используются, так как их применение приведет к замедлению работы системы. Именно поэтому сейчас стали популярны системы контроля привилегированных пользователей (PIM, Privileged Identity Management). В настоящее время на российском рынке представлено большое количество систем данного класса. Рассмотрим задачи, которые можно решить с помощью таких систем, на примере отечественного решения SafeInspect:

1. Необходимо обеспечить строгую аутентификацию привилегированных пользователей. Здесь существует масса проблем, вызванная тем, что администраторы часто используют специализированные протоколы, которые имеют собственные системы аутентификации. В качестве примера можно привести использование протокола SSH, который предполагает использование ключей SSH для доступа (имя — пароль мы не будем рассматривать). А это совершенно отдельная система, ключи не имеют ничего общего с сертификатами x.509, которые часто используются для аутентификации обычных пользователей и клиентов.

2. Необходимо определить и применить политику, которая обеспечивает доступ администраторов в строго определенное время (особенно важно для доступа внешних администраторов).

3. Крайне необходимо обеспечить правильное разделение полномочий по доступу к информационным ресурсам. Решение данной задачи осложняется тем, что администраторы имеют крайне «глубокий» доступ в систему и высокие полномочия. Как правило, во многих организациях администраторы имеют доступ в рамках своей системы ко всей ИТ-инфраструктуре организации и крайне болезненно относятся к каким-либо ограничениям.

4. При работе с учетными записями типа Суперпользователя (root, Administrator и т.п.) важно обеспечить точный контроль над тем, кто именно и какие действия производил под этим аккаунтом, а это часто невозможно сделать штатными средствами.

5. Важно контролировать как пароли/ключи доступа, так и время доступа к разным системам и своевременно их менять или блокировать. В идеале стоит менять пароли или ключи сразу после завершения сеанса доступа.

6. Поскольку администратор может вводом неправильной команды случайно или преднамеренно нарушить работоспособность системы, крайне важно иметь возможность защиты от таких ошибок. Например, эту проблему можно решить путем запрета ввода определенных команд или системой быстрого оповещения, которая будет показывать, что определенные команды вводились в короткий промежуток несколько раз и имеется риск того, что в данном случае производились несанкционированные действия.

7. Кроме того, часто возникает необходимость проанализировать, что делалось в системе месяц назад с как можно наибольшей детализацией (как в случае исправления ошибок администрирования, так и в случае поиска несанкционированных действий). И тут такие системы являются незаменимыми.

8. Современные протоколы администрирования, даже самые базовые и популярные, сложны по своей природе, имеют т.н. субканалы, по которым передаются данные, и они зашифрованы. Контроль таких субканалов с точки зрения возможной утечки данных также является крайне важной задачей. В данном случае, например, решение SafeInspect позволяет полностью расшифровать данные и передать их в систему DLP или другую систему безопасности для последующего анализа.

9. Современные стандарты по безопасности, такие, как PCI DSS, СТО БР ИББС, в ряде случаев требуют наличия средств контроля привилегированных пользователей в финансовых организациях.

С учетом вышесказанного можно отметить, что внедрение системы контроля привилегированных пользователей позволит организации:

- выполнить соответствующие требования стандартов — СТО БР ИББС, PCI DSS, ISO 27001 и др.;
- снизить риск несанкционированного доступа привилегированных пользователей и утечки конфиденциальной информации;
- существенно снизить риск нарушения работоспособности и безопасности ИТ-инфраструктуры;
- создать архив записей сессий привилегированных пользователей для последующего проведения служебных расследований.

* * *

В настоящей статье были рассмотрены только основные возможности по применению систем контроля привилегированных пользователей. Как мы видим, затрагивается целый пласт проблем ИБ, которые в течение долгих лет не решались в полном объеме. Однако в современных условиях эти угрозы уже нельзя игнорировать, поскольку от безопасности в этой сфере может зависеть работоспособность ключевых бизнес-процессов финансовой организации. Использование решения класса SafeInspect позволит существенно повысить уровень безопасности кредитно-финансовой организации за счет снижения рисков, связанных с привилегированными пользователями.