УДК 004.056

ПРОФИЛИРОВАНИЕ АКТИВОВ КАК ЭТАП УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сечкина Н.А., Исаев А.С.
(Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)
Научный руководитель – к.т.н., доцент Исаев А.С.
(Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Аннотация. Традиционный аудит активов требует значительных ресурсов, но при этом не всегда гарантирует точность и эффективность при дальнейшем использовании полученных результатов в вопросах управления рисками. В статье рассматриваются потребности отрасли информационной безопасности, которые стимулируют организацию внедрять комплексные и целенаправленные меры профилирования активов, а также проблемы, с которыми они сталкиваются при достижении поставленной цели. Также анализируются способы решения этой задачи с помощью автоматизированных средств и даются рекомендации по дальнейшей разработке собственной методики профилирования активов в организации.

Введение. В современном мире перед организациями стоит задача препятствовать угрозам информационной безопасности, так как они наносят вред бизнесу. Организации сталкиваются с непростым выбором: либо осуществлять полноценный аудит информационной безопасности с целью выявления активов, уязвимостей и угроз (что влечет за собой большую потребность в ресурсах и неудобства), либо ограничиваться выборочными проверками (что влечет за собой возможность уменьшения эффективности полученных данных для анализа риска информационной безопасности). Существующие автоматизированные системы профилирования активов идентифицируют только информационные активы и, в основном, основаны на несложной классификации активов, поэтому предоставляют слишком общую и размытую информацию. При этом точное определение критериев актива, которые впоследствии будут использоваться в процессе анализа риска — очень нетривиальная задача. Для этого необходимы мощные инструменты, способные анализировать данные. Для точной идентификации рисков необходимы практические средства, ускоряющие анализ и обработку всех доступных данных, т.к. в настоящее время многие организации все интенсивнее ищут способы сокращения затрат, включая затраты на управление рисками.

Основная часть. Профилирование активов открывает новые возможности при решении множества задач. Одновременный анализ всех данных об активе при расчете показателя риска каждого из них позволяет не только повысить точность оценки, но и снизить уровень неэффективности от использования более поверхностных форм профилирования.

При использовании средств профилирования активов организации могут сократить временные затраты на оценку рисков и выделить оставшиеся ресурсы на более приоритетные направления, например, представляющие наиболее высокую степень угрозы информационной безопасности или незаконного доступа к конфиденциальной информации, обеспечивая таким образом одновременно сокращение затрат, повышение эффективности и ускорение процедур управления рисками. Таким образом, средства профилирования активов позволяют повысить защищенность системы и удобство управления рисками, то есть являются выгодными для организации.

Разработка подробного профиля актива предоставляет организациям четкую иллюстрацию угроз, которым подвержены эти активы, и позволяет им реализовать программу упреждающего управления инцидентами, которая фокусируется на элементах угроз, связанных с рисками.

Большинство рассмотренных методик содержат подробную классификацию категорий активов и описание действий, которые необходимо выполнить для составления профиля актива, не содержат в себе конкретных рекомендаций о том, как реализовывать эти действия. Поэтому стоит не полностью опираться на описанные методики, а рассмотреть разные варианты их компоновки для создания своей методики профилирования активов, которая позволит уменьшить временные затраты и трудовые затраты и автоматизировать процесс профилирования активов информационной безопасности.

Сравнение методик и средств профилирования активов проводилось по следующим параметрам:

1) Выделение сотрудников как актив организации;
2) Выделение критичных информационных ресурсов организации;
3) Выделение информации как отдельного актива организации;
4) Подробная классификация;
5) Информация о определении стоимости актива;
6) Информация о защитных мерах для профиля актива;
7) Информация об угрозах и уязвимостях для профиля актива;
8) Необходимость составления отчетов;
9) Автоматизация процесса профилирования активов.

Ни одна рассмотренная методика или ни одно рассмотренное средство не удовлетворяет всем критериям одновременно. Что является предпосылкой к созданию методики, которая будет содержать в себе все перечисленные критерии. Тогда можно будет говорить о теоретической эффективности методики профилирования активов.

Выводы. Внедрение методики профилирования активов — рабочая и крайне эффективная альтернатива традиционному аудиту. В частности, применение технологии для эффективного анализа и для совместного применения данных позволяет существенно повысить эффективность и переложить часть работы по принятию решений с людей на методику. Повышение эффективности управления рисками организации с помощью методик профилирования активов может способствовать упрощению ведения бизнеса с позиции риск-ориентированного мышления. Правильно составленные профили активов можно дальше использовать в комплексных алгоритмах и сложных средствах управления рисками для вероятностной оценки риска. Профилирование активов не только способствует упрощению управления рисками (поскольку снимает необходимость тщательной проверки каждого актива, позволяя использовать профили), но и существенно повысить уровень защиты.

Сечкина Н.А. (автор) Подпись

Исаев А.С. (научный руководитель) Подпись