РАЗРАБОТКА КОМПЛЕКСА ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ МЕР ДЛЯ ПРОТИВОДЕЙСТВИЯ ИНСАЙДЕРАМ

Поляничко Марк Александрович
К.т.н., доцент, ФГБОУ ВО ПГУПС (г. Санкт-Петербург)
polyanichko@pgups.ru

Аннотация. Инсайдерские угрозы информационной безопасности — это угрозы, исходящие от работников организации. В статье рассматриваются организационные меры по обнаружению инсайдеров и предотвращению их действий. Обнаружение инсайдеров и противодействие им, как внутренней угрозе информационной безопасности, может быть реализовано за счет внедрения в работу комплекса организационных мер, снижающих вероятность успешной реализации инсайдерской угрозы.

Ключевые слова: внутренние угрозы информационной безопасности, инсайдер, классификация инсайдеров, обнаружение и противодействие инсайдерам.

DEVELOPMENT OF ORGANIZATIONAL AND TECHNICAL MEASURES COMPLEX FOR COUNTERING INSIDERS

M. Polyanichko

Summary. Insider threats to information security are threats posed by employees of the organization. The article examines the organizational measures for the detection of insiders and preventing their actions. Detection of insiders and counteraction to them as an internal threat to information security can be implemented through the introduction of a set of organizational measures that reduce the likelihood of insider's success.

Keywords: internal threats to information security, insider, classification of insiders, detection and counteraction to insiders.

Инсайдерская деятельность представляет собой значительный риск для организаций. Действия инсайдеров могут потенциально привести к инцидентам, угрожающим репутации, бренду или финансовому положению компании [1]. Международные аналитические обзоры и отчеты показывают, что в последние годы организации расширяют финансирование мероприятий по обеспечению информационной безопасности и активно работают в области противодействия атакам и все больше организаций уходят в сторону реализации принципа Security-by-design [6]. Тем не менее, результаты опросов показывают, что этого недостаточно. 87% опрошенных компаний отмечают, что средств, выделяемых для обеспечения желаемого уровня информационной безопасности и устойчивости к угрозам не хватает, применяемые средства защиты неоднородны и работают изолированно. На данный момент, число организаций, использующих передовые решения, относительно невелико [2].

При этом надо принимать во внимание, что курс, взятый на цифровую трансформацию экономики [7], толкает организации к быстрому освоению и внедрению новых технологий и бизнес-моделей, что повышает значение информационной безопасности и, со временем, может поставить ее в ряд ключевых факторов, обеспечивающих стабильность и непрерывность работы.

Несмотря на это, статистика показывает, что 77% организаций находятся на начальном этапе построения системы защиты информации, а многие организации даже не обладают полным пониманием того, какая информация и активы имеют для них принципиально важное значение и где они хранятся [3]. Тем не менее, глобальные

кибератаки, проводимые в последние годы дали понимание, что защита информации необходима не только для сохранения конфиденциальности данных, но и для обеспечения непрерывности деятельности организации.

Несмотря на риски, вызванные инсайдерскими угрозами, организации должны обеспечивать сотрудников доступом к корпоративной информации для выполнения своих рабочих обязанностей. Реализовать систему, способную обнаруживать и снижать риски инсайдерской угрозы очень сложно [4]. Тем не менее, существуют организационные меры, которые при использовании стандартных программных средств защиты информации и небольшой стоимости могут снизить вероятность успешной реализации инсайдерской угрозы.

Как говорилось ранее, инсайдерскую активность сложно засечь, тем не менее, определенные управленческие действия могут повысить шансы на обнаружение инсайдерской деятельности:

- Идентификация критичных информационных активов и выдача минимально необходимого уровня доступа к данным для сотрудников для увеличения шансов быстрого обнаружения инсайдерского поведения;
- Обеспечение соблюдения рабочего распорядка;
- Проведение регулярных инструктажей по информационной безопасности, в том числе доводящих до работников важность вопросов противодействия инсайдерским угрозам;
- Проведение обучения по использованию программных средств защиты информации, использования корпоративной почты и ее фильтрации, обучение правильной последовательности действий в случае обнаружения программ шифровальщиков;
- Мониторинг сетевого трафика, выявление необычных действий, таких как подключение к неизвестным внешним ресурсам, подключение в нерабочее время, передача большого объема данным и т.п.

Предотвращение реализации инсайдерской угрозы может быть таким же сложным как и обнаружение вредоносных действий инсайдеров, так как работники имеют легитимный доступ к информационным активам компании. Тем не менее, определенные управленческие действия могут снизить вероятность нарушения конфиденциальности, целостности или доступности данных:

- Использование принципа выдачи наименьшего количества прав, исключение доступа сотрудников к информации, которая им не требуется для выполнения их служебных обязанностей.
- Реализация мер, предотвращающих возможность распространения данный, таких как запрет на использование съемных носителей информации
- Внедрение системы, сканирующей и анализирующей почтовые отправления. Блокировка подозрительных исходящих сообщений снижает вероятность передачи корпоративных данных через интернет.
- Мониторинг исходящего трафика и анализ шифрованных потоков данных.
- Использование сегментирования сетей для отделения подсетей с конфиденциальной информацией и анализа фактов копирования информации из этих подсетей.
- Проведение регулярных инструктажей по работе с корпоративной почтой и выработки навыков проверки всех приложений к письмам перед их открытием.

Вместе с тем, организации должны рассматривать возможность проверки новых сотрудников до того, как они приступили к работе, и вводить контрактные положения об аналогичной проверке бизнес-партнёров. В первую очередь это касается тех лиц, которым будет предоставлен доступ к важной информации. Под проверкой понимается процедура скрининга. Скрининг — процедура верификации данных представленных кандидатом на трудоустройство в своем резюме и заявлении, выполняемая работодателем (или сторонней организацией). Данная процедура может позволить выявить слабые стороны характера подчиненного и наклонности к нелегальной деятельности, которые могут нанести ущерб организации и ее репутации или служить ограничением для эффективного выполнения своих обязанностей. Скрининг часто выполняется для того, чтобы определить, можно ли доверять работнику доступ к финансовым ресурсам и конфиденциальной информации. Также скрининг часто требуется для кандидатов на должности, требующие высокого уровня доверия, такие как работа в сфере образования, судах, медицинских учреждениях, аэропортах или правительстве. Данная проверка может выполняться частной компанией и быть дорогостоящей. В результате скрининга проверяются данные по прежним местам работы, кредитной истории и записях о судимостях. Цель такой проверки — обеспечение безопасности и защиты сотрудников организации [5].

Обнаружение и предотвращение инсайдерских угроз — сложная задача, но, если организации смогут определить наиболее критичные данные и обеспечить наблюдение за действиями, выполняемыми с этими данными, вероятность обнаружения неавторизованных действий значительно вырастет и снизит возможности инсайдера по реализации успешной атаки.

ЛИТЕРАТУРА

1. Insider Threat Report: 2018 — CA Technologies // CA Technologies URL: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf (дата обращения: 18.07.2018).
2. Поляничко М. А. Использование технических индикаторов для выявления инсайдерских угроз // Кибернетика и программирование. — 2018. — № 6. — С. 40–47. DOI: 10.25136/2306–4196.2018.6.27970. URL: http://e-notabene.ru/kp/article_27970.html.
3. Поляничко М. А. Модель зрелости процессов противодействия внутренним угрозам // Естественные и технические науки. 2018. — № 11., Выпуск (125). — 2018 — с. 452–456.
4. Поляничко М. А. Моделирование действий инсайдеров на основе аппарата информатики поведения // Естественные и технические науки. 2018. — № 12., Выпуск (126). — 2018 — с. 446–449.
5. Холодный Ю. И. Применение полиграфа при профилактике, раскрытии и расследовании преступлений (генезис и правовые аспекты). Монография, — М., 2000.
6. Kessel P. Van Is cybersecurity about more than protection? // // EY Global Information Security Survey 2018–19 [Электронный ресурс]. — Режим доступа: https://www.ey.com/Publication/vwLUAssets/ey-la-cybersecurite-est-elle-seulement-une-affaire-de-protection-en/$FILE/ey-giss-2018-en.pdf.
7. Распоряжение Правительства РФ от 28.07.2017 N1632-р «Об утверждении программы „Цифровая экономика Российской Федерации“».

Журнал «Современная наука: актуальные проблемы теории и практики»

ПГУПС