УДК 004

ПОЛЯНЧИКО МАРК АЛЕКСАНДРОВИЧ

БАЗОВАЯ МЕТОДИКА ВЫЯВЛЕНИЯ ИНСАЙДЕРСКИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АННОТАЦИЯ

В работе представлена проблема выявления инсайдерских угроз информационной безопасности. Приведен анализ современного состояния методов и инструментальных средств защиты от инсайдерских угроз. Сформулирована базовая методика защиты от инсайдерских угроз.

Ключевые слова: кибербезопасность; информационная безопасность; инсайдер; выявление инсайдеров.

POLYANICHKO M.A.,

THE BASIC APPROACH TO IDENTIFYING INFORMATION SECURITY INSIDER THREATS

ABSTRACT

The paper presents the problem of identifying insider threats to information security. The analysis of the current state of methods and tools to protect against insider threats. The basic technique of protection against insider threats is formulated.

Keywords: cybersecurity; information security; insider; insider detection.

Инсайдерская угроза является одной из самых больших проблем информационной защиты. «Традиционная» защита и более совершенная защита от стойких продвинутых угроз (APT) на основе сбора данных неэффективны против инсайдеров-злоумышленников [7, 9]. Выявление инсайдерских угроз и злонамеренных инсайдеров – комплексная задача, которую решают аналитики и администраторы информационной безопасности как в коммерческом секторе, так и в государственных организациях. Действия инсайдера сложно отличить от действий легитимных пользователей по причине того, что инсайдер имеет легитимные права на авторизацию и использование информационных ресурсов организации. Инсайдерская активность (до 75%) [4, 5] до сих пор, как правило, обнаруживается в ручном режиме и только 19% действий выявляются с помощью сочетания автоматизированных программных средств и ручных процедур [11]. К информации, которую можно использовать для обнаружения инсайдеров можно отнести журналы операционных систем и логи информационных систем, телефонные записи и данные по активности учетной запись пользователя. Проведенные исследования показали, что для раскрытия почти трети инцидентов были использованы различные журналы. Большинство этих инцидентов были раскрыты персоналом, который не имеет отношение к информационной безопасности, так как инсайдеры тщательно скрывали свои действия и личность.

Тем не менее, для обнаружения и локализации инсайдерской угрозы недостаточно рассматривать решения только из технической области. Это вызвано тем, что эта проблема включает в себя разнообразные проблемы, включая психологические,

социальные и организационные вопросы. Большинство существующих подходов предлагают подходы выявления инсайдерской угрозы [2], ориентированные на выявление фактов неавторизованных действий и подходы, ориентированные на выявление аномального поведения, которое может являться проявлением злонамеренных действий.

Многие исследования, направленные на выявление инсайдерских угроз, развиваются под влиянием подходов, которые ранее использовались для обнаружения внешних угроз. Используются системы обнаружения вторжений (IDS) для выявления атак в реальном времени, используя базу данных шаблонов атак, которые проводились ранее. В IDS используется два подхода: выявление аномальной активности и сигнатурный анализ. К последним разработкам в области совершенствования IDS можно отнести Data mining, использование статистических моделей, нейронных сетей, генетические алгоритмы, экспертные системы и др. Это междисциплинарные подходы, относящиеся к математике и статистике, машинному обучению, моделированию, искусственному интеллекту и т.д. Многие подходы хорошо зарекомендовали себя при решении задачи обнаружения внешних угроз [8]. Эти подходы не эффективны при обнаружении внутренних угроз и дают большое количество ложно положительных результатов. Таким образом, эти подходы имеют ограниченное применение при обнаружении инсайдерских угроз. В том числе, системы обнаружения вторжений используют сигнатуры атак и не могут обнаружить действия, которые не оставляют записи в системах журналирования [6, 8].

Проведенный анализ исследований в области обнаружения инсайдерских угроз позволил определить основные проблемы, затрудняющие обнаружение инсайдеров [1, 3]:

– Обнаружение инсайдерской угрозы – явление, связанное с параметром времени. Таким образом, признаки инсайдерской угрозы располагаются в частотной и временной плоскости. Тем не менее, для этой конкретной проблемы, любое внезапное изменение в поведении отслеживается, так как внезапные изменения в поведении и действиях может быть сигналом, что инсайдер участвует во вредоносной атаке.
– Информация об инсайдерской угрозе представляет собой нестационар-ные многомерные временные ряды. Наличие постоянного глобального технологического прогресса приводит к нестационарности данных, так как внезапный технологический прорыв может сделать текущую ИТ-инфраструктуру и процессы устаревшими в очень короткий промежуток времени. Кроме того, роли сотрудников, бизнес-процессы, системы и организационные структуры постоянно меняются.
– Два или более инсайдеров могут объединиться, чтобы совершить злона-меренный акт и при этом не вызвать никаких подозрений. Например, большая группа инсайдеров может внести несколько небольших изменений в файл с ограниченным доступом, чтобы испортить данные.

Внедрение методики для эффективного устранения угроз злоумышленных инсайдеров может быть сложным, дорогостоящим и длительным процессом. Ниже описывается базовая методика, внедрение которой увеличивает защищенность организации от инсайдерских угроз.

1. Выявление угрозы. В первую очередь, в организации должен быть назначен работник, ответственный за выявление угроз со стороны злоумышленных инсайдеров, ответственный за отчетность перед руководством организации и ответственный за разработку и реализацию перечня мероприятий по снижению риска. В работе организации руководство должно демонстрировать поддержку политик, процедур и средств управления информационной безопасностью.

2. Базовый уровень безопасности. Предпосылкой для программы снижения риска от инсайдерских угроз является хорошо функционирующая традиционная система управления информационной безопасностью (ISMS), которая обеспечивает базовый уровень контроля безопасности в организации. Она защищает организацию от широкого спектра угроз и поможет снизить риск со стороны злоумышленных и неумышленных инсайдеров.

3. Реагирование на инциденты. Необходимо расширить существующие процессы реагирования на инциденты, чтобы должным образом решить проблему, созданную злоумышленными инсай-

дерами, и реагировать на нарастание напряжения среди работников, у которых есть подозрения в неправильных действиях со стороны других лиц. Еще одним сильным инструментом, позволяющим сдерживать потенциальные внутренние угрозы выступают дисциплинарные меры. Данные меры могут быть применены после подтверждения факта нарушения информационной безопасности. Применяемые дисциплинарные меры должны быть корректными и справедливыми по отношению к работникам, участвовавшим в нарушении информационной безопасности. Дисциплинарные меры принимаются как ответное действие, учитывающее характер и серьезность нарушения, влияние на работу организации, наличие периодических нарушений, зафиксированного факта прохождения соответствующего обучения и других факторов. Дисциплинарные меры также могут применяться профилактически в целях предотвращения нарушений работниками. В случае, если нарушение допущено намеренно, то данная ситуация требует немедленных ответных действий. Дисциплинарные меры могут предусматривать поощрительные меры в случае образцового поведения в части информационной безопасности и выступать в качестве дополнительного фактора мотивации.

4. Информационно-коммуникационная работа. Следует установить и соблюдать приемлемые правила, в которых достаточно ясно изложено, что ожидается и требуется от сотрудников организации в области информационной и системной безопасности. Следует информировать об инсайдерских угрозах и организовывать программы для обучения персонала, выявлению угроз и реагирования на них. Штатные работники и, в случае необходимости, работники организации, работающие по договору, должны быть соответствующим образом информированы и обучены, а также регулярно извещаться об изменениях в политиках и процедурах организации, в той мере, насколько это важно для исполнения их рабочих обязанностей. В случае, если работники не были осведомлены о лежащей на них ответственности в сфере информационной безопасности, может быть нанесен урон организации. Мотивированный персонал будет, вероятно, более надежным и вызывать меньше инцидентов информационной безопасности. Некорректное руководство может привести к негативному влиянию на информационную безопасность организации, провоцировать появление инсайдерских угроз и неправильное использование активов организации.

5. Определение ключевых объектов (ресурсов). Хорошо зарекомендовавшая себя традиционная ISMS должна установить важные объекты (ресурсы) организации, и это должно стать отправной точкой для определения приоритетов повышенной защиты от угроз со стороны злоумышленных инсайдеров. В частности, следует установить местоположение и поток конфиденциальных или ценных данных. Системы, обрабатывающие эти данные, должны рассматриваться как критически важные, в том числе любые системы, которые играют решающую роль в выполнении ключевых бизнес-процессов.

6. Контроль доступа. Необходимо обеспечить надёжное управление идентификацией и доступом. Это означает, что работникам предоставляются минимальные привилегии на доступ к системам; проверяется и соблюдается разграничение полномочий; и в случае появления новых работников, перемещения работников внутри организации или увольнения работника, процедуры доступа сразу же изменяются. Следует обращать особое внимание на пользователей, имеющих большие привилегии, а также, в сочетании с другими мерами, важно в первую очередь контролировать доступ к особо важной информации.

7. Проверка. Необходимо организовывать проверку 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 [10].

8. Предотвращение потери данных. Следует рассмотреть возможности использования программы Предотвращения потери данных (DLP) и Управления правами на доступ к данным (IRM), особенно если утечка конфиденциальных данных является ключевым риском для организации. Возможно внедрение приманок и конфигурирования DLP для обнаружения и реагирования на утечки данных в неавторизованных местах.

9. Мониторинг. Необходимо обеспечить надлежащее функционирование протоколов регистрации и анализа событий и корреляции процессов (SIEM), а также установить исходные параметры нормального сетевого трафика и использования системы.

10. Анализ данных. Следует расширить масштабы мониторинга, регистрации и аудита, чтобы собрать больше данных вокруг инсайдерской угрозы, включая данные о поведении сотрудников и их личные события. Необходимо включить инструменты анализа данных для прогнозирования и диагностики инсайдерских угроз. Особенно важно использовать реальные ресурсы и следить, чтобы группы мониторинга не перегружались все большими объемами данных каждый день, и чтобы необходимые данные не потерялись в этом потоке.

Предложенная базовая методика позволит повысить эффективность работы администратора безопасности и уменьшить время, требуемое для выявления наличия инсайдерской угрозы.

Список литературы

1. *Cappelli D., Moore A. and Trzeciak R.* The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud), New York, New York: Pearson Education, Inc., 2014.

2. *Gabrielson B.* (2006). Solving the insider threat problem. University of Louisville Cyber Security Days, October, Louisville, KY.

3. *Gheyas I.A., Abdallah A.E.* Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis // Big Data Analytics. 2016. № 1 (1). С. 6.

4. Insider Threat Report: 2018 – CA Technologies [Электронный ресурс]. – Режим доступа: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf (дата обращения: 18.07.2018).

5. *Keeney M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T. and S. Rogers.* (2005, May). Insider threat study: Computer system sabotage in critical infrastructure sectors. CMU/SEI and U.S. Secret Service.

6. *Kumar S.* (1995). Classification and detection of computer intrusions. (Unpublished doctoral dissertation). Purdue University, West Lafayette, IN.

7. *Smith J.A., Holloway R.* Mitigating cyber threat from malicious insiders. 2014. С. 1–8.

8. *Zeadally S. and etc.* Detecting insider threats solutions and trends // Information Security Journal. 2012. No 21 (4). С. 183–192.

9. *Поляничко М.А.* Анализ современного состояния методов и инструментальных средств защиты от инсайдерских угроз информационной безопасности // Фундаментальные и прикладные научные исследования: сборник статей XIV Международной научно-практической конференции. – Пенза, 2018. – С. 135–138.

10. *Холодный Ю.И.* Применение полиграфа при профилактике, раскрытии и расследовании преступлений (генезис и правовые аспекты): монография. – М., 2000.

11. Advanced threat detection with the Interset platform [Электронный ресурс]. – Режим доступа: https://interset.com/behavioral-analytics-white-papers/ (дата обращения: 10.06.2018).

Статья поступила в редакцию 21 августа 2018 г.
Принята к публикации 8 октября 2018 г.