ОПРЕДЕЛЕНИЕ ОСНОВНЫХ ХАРАКТЕРИСТИК ИНСАЙДЕРОВ

Аллахвердиева Эльнара Асад кызы

магистрант, Бакинский Государственный Университет, Азербайджан, г. Баку

DEFINITION OF THE MAIN CHARACTERISTICS OF INSIDERS

Allahverdiyeva Elnara Asad kizi

Master's student, Baku State University, Azerbaijan, Baku

Аннотация. На долю инсайдеров приходится значительная часть нарушений безопасности и других видов потерь организаций, и они привлекают внимание как ученых, так и практиков. Хотя были разработаны методы и механизмы для отслеживания потенциальных инсайдеров с помощью электронного мониторинга данных, лишь немногие исследования посвящены прогнозированию потенциальных вредоносных инсайдеров. Используя метод интеллектуального анализа текстов для анализа различных медиаконтентов существующих инсайдерских дел, мы разработали метод выявления важнейших и общих признаков того, что человек может быть злонамеренным инсайдером.

Ключевые слова: инсайдер, инсайдерская угроза, теория планируемого поведения, текстовый анализ

Постановка проблемы и анализ последних исследований. В области информационной безопасности тема "инсайдерской угрозы" привлекает к себе большое внимание, но до сих пор не получила серьезного эмпирического исследования. Тем не менее, существует множество фактов о инсайдерской угрозы. В одном из отчетов 2010 года ФБР отметило 10 примеров инсайдерских атак, зарегистрированных за последние годы, включая кражу коммерческих секретов, корпоративный шпионаж и несанкционированное раскрытие информации). Эти инциденты привели к крупным финансовым потерям. Некоторые исследователи считают, что инсайдерскую угрозу, в отличие от атак со стороны, легче реализовать, поскольку инсайдеры лучше знакомы со структурой безопасности организаций, в которых они работают [1,2]. Инсайдеры организации либо имеют законный доступ к ресурсам организации [3], либо обладают знаниями о деятельности организации [4] Обладая знаниями и легитимным доступом, они могут обойти протоколы безопасности и воспользоваться доверием, которое организация оказала им [5]

Информационная эпоха привела к новым последствиям инсайдерской угрозы. Последствия атак инсайдеров имеют многомерный характер, включая финансовые потери, нарушение работы организации, потерю репутации и долгосрочное воздействие на организационную культуру. По сравнению с последствиями сторонних атак, инсайдерские атаки приводят к инцидентам с более высокими последствиями поскольку инсайдеры знакомы с контрмерами и знают, как найти свои цели.

В информационную эпоху темам инсайдерства и инсайдерских угроз уделяется значительное внимание как со стороны практиков, так и со стороны научных кругов. С одной стороны, инсайдерская угроза считается одной из самых серьезных проблем безопасности , что подтверждается результатами опроса 2008 года CSI Computer Crime and Security Survey, в котором "инсайдерская угроза" была названа второй после компьютерных вирусов проблемой безопасности. Тем не менее, инсайдерская угроза получила относительно низкий уровень научных исследований. Одна из важных причин такого недостатка внимания связана с трудностями в борьбе с инсайдерской угрозой. Некоторые из причин, способствующих этому пробелу в исследованиях, включают недостаток данных для анализа и малое количество полезных методов для изучения этой темы. В связи с этим организации используют технические средства контроля, такие как брандмауэры, и ограничивают доступ пользователей, чтобы предотвратить возможные нарушения безопасности со стороны инсайдеров.

К сожалению, технические средства контроля мало что делают для того, чтобы изолировать подозрительные и вредоносные действия инсайдеров без недопустимых ложных срабатываний. Например, контроль доступа, основанный на аутентификации и авторизации, предполагает, что инсайдеры всегда будут использовать законные привилегии для выполнения вредоносных действий и таким образом будут пойманы, но как только это предположение будет нарушено, контроль доступа потеряет свою силу.

Мониторинг, еще одна распространенная техника борьбы с инсайдерской угрозой, основана на предположении, что аномальное использование системы указывает на подозрительных инсайдеров. Однако мониторинг - это скорее метод подтверждения post-hoc для подтверждения уже подозрительных инсайдеров и поэтому возникает вопрос, может ли он служить в качестве сдерживающего фактора[5].

Технические подходы к борьбе с инсайдерскими угрозами страдают двумя основными недостатками: Во-первых, злонамеренные намерения инсайдеров могут быть ненаблюдаемыми, а поведенческие модели инсайдеров существенно различаются. Однако все инсайдерские атаки имеют одну общую черту: они совершаются инсайдерами, имеющими мотивацию. В исследовании 2005 года, посвященном инцидентам с участием инсайдеров в Randazzo et al. обнаружили, что в 23 инцидентах, произошедших с 1996 по 2003 год, в 81 % случаев преступниками двигала финансовая выгода, в 23 % - месть, в 15 % - неудовлетворенность и в 15 % - желание добиться уважения. Другие исследования предполагают, что гнев, обида или чувство мести могут быть первопричинами инсайдерских атак. В существующих исследованиях также предпринимаются попытки определить психологические индикаторы мотивации злоумышленников-инсайдеров. Грейтцер и Фринке [6] разработали 12 индикаторов подозрительных злонамеренных инсайдеров, три из которых возглавляют недовольство, принятие обратной связи и проблемы с управлением гневом. Они также сообщили, что эти показатели являются достаточно хорошими предсказателями. Однако все эти индикаторы - факторы, которые можно наблюдать на рабочем месте, и предполагается, что потенциальный или действующий злонамеренный инсайдер выявит их на работе. Это может быть не всегда так, поскольку дисциплинированные инсайдеры могут оставаться "под радаром" и не проявлять таких признаков. Кроме того, эти индикаторы еще не получили эмпирического подтверждения.

Современное состояние феномена инсайдерской угрозы в большей степени ориентировано на предотвращение возможных преступников и в меньшей степени на их идентификацию и поимку. Данное исследование направлено на развитие существующих исследований по выявлению вредоносных инсайдеров путем использования информационных технологий для подтверждения индикаторов инсайдерской угрозы эмпирическими данными.

2. Методология. В исследованиях часто сосредоточены на предотвращении инцидентов с участием инсайдеров, а не на выявлении вредоносных инсайдеров. Кроме того, хотя были предложены некоторые характеристики вредоносных инсайдеров, многие из них не выдержали тщательного эмпирического исследования. Мы стремимся устранить эти пробелы, используя текстовый анализ и классификацию для изучения данных третьих лиц, а именно прошлых отчетов о пойманных злонамеренных инсайдерах, и эмпирически изучить их характеристики. Затем мы намерены использовать эти эмпирически подтвержденные

характеристики в попытке лучше предсказать и идентифицировать потенциальных злонамеренных инсайдеров.

Данные, используемые в данном исследовании, в основном получены из двух источников: публичных отчетов и предыдущих исследований. Мы начнем с текстового анализа публичных отчетов для поиска ключевых слов имени (инсайдера), вовлеченного в обнаруженные инциденты с инсайдерами. После того как мы выявим достаточное количество случаев, мы проведем текстовый анализ на предмет выявления признаков, характерных для предыдущих исследований.

Метод, который мы использовали в данном исследовании, основан на процедуре, представленной Грейтцером и Фринке [6] . В этом процессе собранные данные сначала преобразуются в наблюдения, а затем эти наблюдения группируются в различные показатели. В подходе Грайтцера и Фринке данные собираются в виде текстовых отчетов. Данные представляют собой прямую доступную информацию о деятельности отдельных лиц, такую как табель учета рабочего времени, записи о входе в VPN и т. д. записи, записи входа в VPN и так далее. Когда эти данные собраны, для вычисления наблюдений используются алгоритмы.

После того как данные собраны и классифицированы, можно приступать к наблюдениям. Наблюдения-это выводы из данных, отражающие определенное состояние. В для расчета времени работы (наблюдения) можно использовать записи табеля учета рабочего времени (данные) и вход в VPN. На основе наблюдений можно получить показатели. Индикаторами называются действия или события, которые являются предвестниками определенного поведения.

В данном исследовании мы рассматривали более широкую перспективу, включая, но не ограничиваясь психологическими индикаторами злонамеренных инсайдеров, как это сделали Грейцер и Фринке . Поэтому мы расширяли рамки исследования с точки зрения данных, наблюдений и индикаторов, но при этом в рамках метода.

В качестве исходных данных в нашем исследовании использовали прямые описания существующих злонамеренных инсайдеров из публичных отчетов, национальных или местных СМИ, а также предыдущих исследований. Эти неструктурированные данные перерабатываются в структурные наблюдения с помощью текстового майнинга с извлечением информации. В этом процессе используются эвристические методы: мы добываем и извлекаем описания злонамеренных инсайдеров и преобразуем их в наблюдения (отражение определенной характеристики или состояния инсайдера), после чего обрабатывается следующий фрагмент данных. Если извлеченное из данных наблюдение уже существует (т. е. уже было идентифицировано), то к остальным добавляется новая запись об этом наблюдении. Однако если объект еще не был замечен, то создается и записывается новое наблюдение.

Основное отличие нашего метода от метода Грейтцера заключается в том, что индикаторы в нашем исследовании не уточняются и не извлекаются из наблюдений, а предопределяются предыдущими исследованиями. Поэтому наблюдения кластеризуются по индикаторам, с помощью методов кластеризации текста. Тем не менее, мы отмечаем, что наличие заранее определенных наблюдений не помешает выявить потенциальные новые наблюдения, и мы ожидаем, что они будут найдены. Современные методы интеллектуального анализа текста и классификации достаточно мощные и могут дать результаты, которые не могут быть обнаружены человеком.

Список литературы:

1. Insider Threat: Prevention, Detection, Mitigation, and Deterrence" by Eric Cole - 2018

2. "Managing the Insider Threat: No Dark Corners" by Nick Catrantzos - 2012

3. "Insider Threats in Cyber Security" by Sushil Jajodia, Paul C. van Oorschot, and Vipin Swarup -

2008

4. "Insider Threats in Cybersecurity" (article) by Dawn M. Cappelli, Andrew P. Moore, and Randall F. Trzeciak - 2009

5. "Insider Threats: Reducing the Risk with Open Source Intelligence" (article) by Mike James - Нет конкретной информации о годе издания.

6. Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data:towards predictive modeling for insider threat mitigation Insider Threats in Cyber Security (pp. 85-113): Springer.