

ВОПРОСЫ ПРИМЕНЕНИЯ ЧЕЛОВЕКО-ОРИЕНТИРОВАННОГО ПОДХОДА К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

Поляничко Марк Александрович

кандидат технических наук, доцент

Петербургский государственный университет

путей сообщения Императора Александра I, г.Санкт-Петербург

Аннотация. В статье рассматривается человеко-ориентированный подход к обеспечению кибербезопасности и проблемы, связанные с его применением. Данный подход основан на анализе поведения работников и позволяет выявить подозрительные действия на основе поведения пользователей, независимо от наличия и полноты информации об имеющихся информационных активах организации.

Ключевые слова: кибербезопасность, инсайдер, обнаружение инсайдеров, анализ поведения.

В связи с распространением и ростом популярности социальных сетей, облачных систем хранения данных, мобильных приложений и личных учетных записей электронной почты на рабочем месте, использование которых часто сопровождается непоследовательными и слабыми средствами управления информационной безопасностью, злоумышленникам предоставляются множество каналов для осуществления атаки. В связи с этим возрастает количество случаев утечки данных организаций, также отмечается увеличение зафиксированных случаев саботажа со стороны сотрудников [3, 8]. На этом фоне задача обнаружения инсайдерских угроз приобретает все большую актуальность. Современные программные средства защиты информации, как правило, ориентированы на информационные активы. Альтернативой данному подходу выступает обнаружение аномалий в поведении сотрудников на основе пользовательских данных. Данный подход имеет ряд недостатков, которые необходимо решить перед внедрением подобной системы. Обнаружение поведенческих аномалий на основе пользовательских данных, требует интеграции с системой управления инцидентами в области безопасности организации, интеграции с организационными мерами обеспечения конфиденциальности данных организации и постоянного надзора со стороны руководства [6].

Организации должны адекватно реагировать на растущую угрозу, исходящую от внутренних нарушителей. Для снижения этих рисков доступен широкий спектр технологических решений. Большинство этих технологий по принципу действия можно подразделить на два вида: ориентированные на анализ действий с активами организации и ориентированные на анализ действий пользователей, то есть человеко-ориентированные. В то

время как меры контроля, ориентированные на активы, сосредоточены на защите активов организации (информации, приложений, систем и сетей) от несанкционированного раскрытия, модификации или уничтожения, средства контроля, ориентированные на пользователя, сосредоточены на предотвращении или обнаружении несанкционированных действий пользователей, связанных с этими активами.

Наиболее часто используемым современным технологическим решением для уменьшения и устранения рисков являются системы предотвращения потери данных (DLP). Большинство современных DLP-решений ориентированы на ресурсы и основаны на базе правил, которая контролирует и осуществляет мониторинг распространения информации за пределами организации. Основным недостатком решений DLP на основе правил является то, что они полагаются на полную инвентаризацию ценных активов организации и не могут обнаружить утечку информации, для которой отсутствуют специально настроенные правила.

Также существуют системы, ориентированные на выявление аномалий в поведении пользователей, что позволяет выявлять подозрительную активность на основе моделирования поведения. Основным преимуществом такой системы по сравнению с продуктами, ориентированными на активы, является способность обнаруживать подозрительные действия на основе поведения пользователей, независимо от наличия и полноты информации об имеющихся активах и наличия заранее определенных записей в базе правил. Этот подход также позволяет выявить новые вредоносные модели поведения.

Однако внедрение такого рода решений требует от организации всестороннего рассмотрения вопросов соблюдения этических принципов. Многие страны, включая Европейские [2, 5, 6], имеют законодательство, защищающее сотрудников от постоянного мониторинга.

Применение человеко-ориентированного подхода обеспечения информационной безопасности, связанного с анализом поведения поднимает несколько проблем.

Проблема доверия

Доверие в организации часто выступает связующим звеном, объединяющим усилия работников. Оно является неотъемлемой частью любой организации и важно для успешной работы. Как правило, организации имеют иерархическую структуру и принятие решения идет от руководителя. В этом случае доверие концептуально выражается в уверенности в том, что каждый отдельный работник действует из соображений общих интересов. Применение данной технологии подразумевает наличие доверия у работников и клиентов в то, что данные о пользователях собираются для строго определенных целей, и что в организации имеются организационные механизмы, способные обеспечить правильность использования данной технологии и гарантировать отсутствие неправомерного использования собранных данных.

Проблема конфиденциальности

Конфиденциальность является важным вопросом: помимо законодательных ограничений, есть и этические соображения. Следует учитывать культурные и социальные факторы, а также риски для самой организации и затрагиваемых лиц [4]. При развертывании системы обнаружения внутренних угроз, использующей машинное обучение для анализа поведения, будут отслеживаться различные действия человека, включая доступ к файлам и сетевым ресурсам, перерывы на обед и просмотр веб-страниц. Хотя функциональность контроля просмотра веб-страниц и доступа к файлам аудита уже является частью современных систем DLP, появление дополнительного шага, осуществляющего мониторинг личных привычек человека может поднимать этические вопросы. Эти вопросы приобретают актуальность в тех случаях, когда мониторинг приводит к принятию решения, оказывающее негативное воздействие на отдельных лиц или коллектив в целом, особенно когда принятое решение является неправильным. Однако в случае, если принятое решение позволило предотвратить вредоносное событие, этические вопросы могут быть оправданы, так как данная технология позволила защитить интересы организации и снизить потенциальные убытки и ущерб.

Проблема неправильного использования данных

Еще одной проблемой является неправильное использование данных. Проведенный опрос показал, что треть технического персонала злоупотребляла своими привилегиями и искала в корпоративной сети конфиденциальную информацию, включая информацию о зарплате, личную информацию, протоколы заседаний правления и личные электронные письма. Эта проблема усугубляется недостатком понимания потенциальной опасности информации, в первую очередь это касается данных о перемещениях человека. Также в контексте систем машинного обучения существует риск неправильного использования данных, получаемых или выводимых системами машинного обучения.

Проблема точности данных

При работе с технологией, которая может повлиять на жизнь людей, точность является очень важным фактором. Недостаток в точности данных может иметь как положительные, так и отрицательные последствия. Например, система машинного обучения может проанализировать поведенческие данные работника на наличие признаков вредоносного поведения и выдать ложный положительный результат. В этом случае, работник может получить дисциплинарное наказание или даже может быть уволен. В любом случае такой результат вызовет стресс у работника, который сам по себе является негативным последствием. Также возможен обратный случай, при котором система допустила ложный отрицательный результат. При таком сценарии

вредоносное событие останется незамеченным, и последствия этого события распространятся на организацию и других работников.

Таким образом, опираясь на собранные данные, человеко-ориентированные системы обеспечения кибербезопасности строят модель нормального поведения пользователя и его работы с информационными системами организации. Данная модель может быть построена как с использованием статистических алгоритмов, так и с применением технологии Machine Learning [7]. В случае, если действия пользователя отклоняются от построенной модели, система фиксирует аномальное поведение и выдает соответствующее информационное сообщение администратору безопасности. Преимущество систем, основанном на человеко-ориентированном принципе заключается в том, что они могут функционировать в режиме реального времени и по действиям пользователя предугадывать наступление инцидента, тем самым позволяя осуществлять проактивное управление кибербезопасностью [1]. Решение проблем, указанных в статье, может позволить эффективно применять человеко-ориентированные системы обеспечения кибербезопасности на практике.

Список литературы:

1. 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.
2. Gotterbarn D. [и др.]. ICT integrity: bringing the ACS code of ethics up-to-date // *Australasian Journal of Information Systems*. 2006. № 2 (13). С. 169–182.
3. IBM Security IBM 2015 Cyber Security Intelligence Index // *IBM Security Managing Security Services*. 2015. С. 24.
4. Schwartz P. M. (2011). Privacy, ethics and analytics. *IEEE Security & Privacy*, 3(9), 66-69.
5. Senarathna I. [и др.]. Security and Privacy Concerns for Australian SMEs Cloud Adoption 2014. (WISP 2014). С. 1–20.
6. Thomas Georg, Patrick D., Meier M. Ethical issues of user behavioral analysis through machine learning // *Journal of Information System Security*. 2017. № 1 (13). С. 3–17.
7. Tuor A. [и др.]. Deep Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams 2017. № 2012.
8. Verizon 2015 Data Breach Investigations Report // *Information Security*. 2015. С. 1–70.