DOI 10.37882/2223-2966.2024.10-2.28

АНАЛИЗ СТРАТЕГИЙ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ИНСАЙДЕРСКОЙ УГРОЗЫ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

ANALYSIS OF INFORMATION PROTECTION STRATEGIES AGAINST INSIDER ATTACKS IN CLOUD COMPUTING

V. Strizhkov

Summary. The subject of the research is the problem of the insider threat to information security in organizations using the cloud computing platform. The object of the study is security as one of the main problems when planning the implementation of the cloud. The author delves into the nature and manifestation of insider attacks, and considers various strategies to counter the malicious actions of insiders. Emphasis is placed on the dilemma of convenience and security of cloud environments, which, on the one hand, free organizations from the burden of data management and storage costs, but at the same time are more vulnerable to malicious impact. The main result of the study is the identification and formulation of relevant and priority vectors for the development of existing methods for ensuring the security of information from malicious actions of insiders in the cloud environment. A special contribution of the author is a fresh look at understanding the insider threat and a designated approach to countering this threat, which combines the detection of behavioral anomalies both on the basis of data from technical monitoring tools and from social and information networks, taking into account the psychological profiling of employees of the organization.

Keywords: insider threat, internal intruder, misuse of access, cloud computing, network activity monitoring, information security.

Стрижков Владислав Александрович
Аспирант, Федеральное государственное образовательное бюджетное учреждение высшего образования «Финансовый университет при Правительстве Российской Федерации» (г. Москва)
218668@edu.fa.ru

Аннотация. Предметом исследования является проблема инсайдерской угрозы информационной безопасности в организациях, использующих платформу облачных вычислений. Объектом исследования является безопасность как одна из главных проблем при планировании внедрения облака. Автор углубляется в характер и проявление инсайдерских атак, а также рассматривает различные стратегии противодействия злонамеренным действиям внутренних нарушителей. Акцент делается на дилемме удобства и безопасности облачных сред, которые, с одной стороны, освобождают организации от бремени затрат на управление данными и их хранение, но в то же время оказываются более уязвимы перед лицом вредоносного воздействия. Основным результатом проведённого исследования является выделение и формулировка актуальных и приоритетных векторов развития существующих методов обеспечения безопасности информации от злонамеренных действий внутренних нарушителей в облачной среде. Особым вкладом автора выступает свежий взгляд на понимание инсайдерской угрозы и обозначенный подход противодействия этой угрозе, сочетающий обнаружение аномалий поведения как на основе данных из технических средств мониторинга, так и из социальных и информационных сетей с учётом психологического профилирования сотрудников организации.

Ключевые слова: инсайдерская угроза, внутренний нарушитель, неправомерное использование доступа, облачные вычисления, мониторинг сетевой активности, безопасность информации.

Введение

Проблемы кибербезопасности часто освещаются для широкой публики в средствах массовой информации, при этом акцент на обыкновенно делается на внешние атаки хакерских группировок. И несмотря на то, что именно внутренняя угроза остается более насущной проблемой, с которой сталкиваются компании, ей, тем не менее, не уделяется того внимания, которого она заслуживает. Клейкомб и Николь [1], дали исчерпывающее определение злонамеренного инсайдера как «нынешнего или бывшего сотрудника, подрядчика или другого делового партнера, который имеет или имел санкционированный доступ к сети, системе или данным организации и умышленно превышал или злоупотреблял этим доступом таким образом, что это отрицательно повлияло на конфиденциальность, целостность или доступность информации или информационных систем организации».

Существует достаточно доказательств того, что внутренние угрозы реальны и достигают уровня внешней угрозы. Например, Роберт Ричардсон в ходе исследования компьютерных преступлений [2] указал, что около 44 % всех организаций так или иначе приходилось сталкиваться со злоупотреблением компьютерными системами, потерей ноутбуков и кражей данных клиентов. Сара Питерс сообщает, что до 60 % всех финансовых потерь компаний вызваны инсайдерами. В (табл. 1) показаны четыре основные категории угроз, исходящие от внутренних нарушителей, а также процент респондентов, посчитавших, что эти угрозы действительно могут быть реализованы при текущем уровне защиты в их компаниях, согласно отчету Computer Security Institute [2].

Как ни странно, умеренный уровень беспокойства по поводу злонамеренных инсайдеров противоречит количеству инцидентов, о которых фактически сообщают те же самые организации.

Таблица 1.

Оценка различных внутренних угроз

Размер организации	Несанкционированное действия с конфиденциальной информацией		Мошеннические транзакции	Саботаж системы
	Доступ	Разглашение		
Маленький	29 %	31 %	24 %	24 %
Средний/ Большой	30 %	38 %	30 %	26 %

В этой статье мы рассматриваем проблему внутренних угроз в области облачных вычислений, которые, благодаря экономическим и техническим преимуществам, в последнее время получили широкое признание. Организации могут передать свою ИТ-инфраструктуру в облако и получить выгоду, в том числе быстрое выделение ресурсов, масштабируемость и экономию средств. Хотя организации ценят гибкость, масштабируемость и управление ресурсами, предоставляемые платформами облачных вычислений, безопасность в целом и вредоносные внутренние угрозы в частности считаются одной из основных проблем при использовании облачных вычислений. Внутренние атаки всегда считаются серьезным риском, поскольку злонамеренные инсайдеры могут повлиять на безопасность многих пользователей. Кроме того, этот риск инсайдерских атак будет более серьезным и разрушительным при использовании облачных вычислений. Таким образом, защита облачных вычислений от внутренних угроз важна для завоевания доверия пользователей. В этой статье анализируется и различные инсайдерские угрозы, характерные для облака. На основании реальных случаев инсайдерских атак, демонстрируется, как встроенная облачная архитектура способствует их успешному проведению.

Статья структурирована следующим образом: В разделе 2 обсуждаются облачные вычисления и вопросы безопасности. В разделе 3 объясняются мотивы и уровень опасности инсайдерских угроз, характерных для облачных вычислений. В разделе 4 обсуждается анализ существующих стратегий и методов смягчения последствий для сокращения количества инсайдеров в облачных вычислениях. Раздел 5 завершает документ и определяет направление будущих исследований.

Облачные вычисления и вопросы безопасности

Облачные вычисления — это тип параллельной и распределенной системы, состоящей из набора взаимосвязанных и виртуализированных компьютеров, которые динамически выделяются и представляются как один или несколько унифицированных вычислительных ресурсов на основе соглашений об уровне обслуживания, установленных в ходе переговоров между поставщиком услуг и потребителями. Облачные вычисления — это новая парадигма хостинга и предоставления услуг через Интернет [3]. Он объединяет многие вычислительные концепции и технологии, такие как сервис-ориентированная архитектура (SOA), Web 2.0, виртуализация и другие технологии, зависящие от Интернета.

Согласно общепринятой классификации, существуют три сервисные модели облачных вычислений [4]:

а) Программное обеспечение как услуга (SaaS) — возможность, предоставляемая потребителю, заключается в использовании приложения поставщика, работающего в облачной инфраструктуре. В этой модели программное приложение размещается как служба, и конечные пользователи используют приложение в веб-браузере.

б) Платформа как услуга (PaaS) — возможность, предоставляемая потребителю, заключается в развертывании в облачной инфраструктуре его собственных приложений без установки какой-либо платформы или инструментов на их локальных компьютерах. В этой модели конечный пользователь создает, тестирует и загружает приложение, используя инструменты и библиотеки, размещенные поставщиком услуг.

в) Инфраструктура как услуга (IaaS) — возможность, предоставляемая потребителю, заключается в обеспечении обработки, хранения, сетей и других основных вычислительных ресурсов, где потребитель может развертывать и запускать произвольное программное обеспечение, которое может включать операционные системы и приложения. Эта модель включает в себя размещение аппаратных вычислительных услуг, таких как хранилище, жесткий диск, серверы и сетевые компоненты. Поставщик услуг несет ответственность за обслуживание и управление всеми этими ресурсами.

Облачные вычисления обеспечивают повсеместный и удобный сетевой доступ по запросу к общему пулу настраиваемых вычислительных ресурсов, таких как сети, серверы, хранилища, приложения и услуги, которые можно быстро подготовить и выпустить с минимальными усилиями по управлению или взаимодействием с поставщиком услуг. Облачные системы очень экономичны и полезны для предприятий любого размера, среди их преимуществ: безграничная гибкость с доступом к миллионам различных баз данных и возможность объединять их в индивидуальные услуги; повышение надежности и безопасности, поскольку пользователям больше не нужно беспокоиться о сбое оборудования или его краже; расширенное сотрудничество за счет возможности онлайн-обмена информацией и приложениями, облако предлагает пользователям новые способы совместной работы и сотрудничества; переносимость, поскольку пользователи могут получить доступ к своим

данным из любого места; более простые устройства, поскольку данные хранятся и обрабатываются в облаке, пользователям просто нужен интерфейс для доступа и использования этих данных, игр и т. д.; неограниченное хранилище, поскольку облако предлагает большое расширяемое хранилище, которое можно обновить при необходимости; доступ к быстрой вычислительной мощности с использованием новейших технологий и инфраструктуры, что ускоряет предоставление услуг.

Несмотря на множество преимуществ внедрения облачных вычислений, с ним также связаны некоторые ограничения. Безопасность — самая большая проблема в облачных вычислениях. Это связано с тем, что облако предлагает услугу хранения в удаленном месте, и потребители должны доверять поставщику облака, даже если потребители не знают, что происходит с их данными. По мнению ряда специалистов ИБ, внешнее хранилище данных, зависимость от общедоступного Интернета и отсутствие контроля над данными в совокупности делают облачные вычисления рискованными для многих проблем безопасности [5].

Поскольку отдельные лица и предприятия производят все больше и больше данных, которые необходимо хранить и использовать (электронная почта, личные медицинские записи, фотоальбомы, факсимильные документы, финансовые операции и т.д.), они заинтересованы в передаче своих локальных сложных систем управления данными в облако благодаря его большей гибкости и экономичности. Однако, как только пользователи больше физически не владеют своими данными, их конфиденциальность и целостность могут оказаться под угрозой. Традиционно для контроля за распространением конфиденциальных данных устанавливается доверенный сервер для локального хранения данных в открытом виде, а затем этот сервер контролируется, чтобы проверять, предоставляют ли запрашивающие пользователи надлежащие учетные данные, прежде чем им будет предоставлен доступ к данным. С точки зрения безопасности эта система управления доступом больше не применима, когда данные хранятся в облаке. Это связано с тем, что пользователи и облачные серверы расположены в разных географических точках, и серверу больше нельзя полностью доверять для определения и применения политик контроля доступа и управления сведениями о пользователях. В случае компрометации сервера или возможных внутренних атак личные данные пользователей могут быть раскрыты. Потеря прямого контроля над своими данными является основной проблемой безопасности для клиентов. Перемещая свои личные данные в облако, пользователи вынуждены доверять поставщикам облачных услуг безопасное и надлежащее управление своими данными.

Среди угроз безопасности в облаке серьезную опасность для клиентов представляют внутренние угрозы, такие как злонамеренные действия системных администраторов. Проблема сложная, потому что системные администраторы имеют повышенные привилегии для выполнения реальных задач по обслуживанию и администрированию системы. Еще одна возможность атаки, которую необходимо учитывать, — это ИТ-саботаж, когда сотрудники пытаются нанести вред ИТ-инфраструктуре работодателя. Недовольство инсайдера поставщиком облачных услуг может привести к причинению вреда организации-жертве с намерением нанести ущерб репутации поставщика облачных услуг [1, 6].

Инсайдерская угроза в Облаке

Как правило, инсайдеры совершают действия, противоречащие политике безопасности, используя свой легитимный доступ. В противном случае, не имея желаемого уровня доступа к данным ввиду отсутствия соответствующих полномочий в рамках своей функциональной роли в организации инсайдеры стараются злоупотреблять возможностями расширения пользовательских привилегий, что позволяет им нарушать как контроль доступа, так и политики безопасности и получать избыточную информацию, в которой они не нуждались бы при честном исполнении своих трудовых обязанностей. Они стараются заполучить роль доверенных лиц, которые имеют максимально возможные привилегии и доступ к ключевым активам. Так, чрезмерные и ненужные привилегии пользователей систем — это значительная уязвимость перед лицом инсайдерских атак.

Наиболее опасные инсайдеры могут потенциально образоваться из наиболее опытных и даже ценных сотрудников. Они хорошо обучены и хорошо разбираются в инфраструктуре, инструментах и оборудовании для выполнения своих задач. Они осведомлены о задачах, видении, стандартных операционных процедурах, правилах, положениях и условиях, а также политике организации. Однако они могут внезапно превратиться в противников, когда недовольны принимаемыми организацией решениями, их требования не выполняются, они не получают справедливого вознаграждения и организация плохо к ним относится. Они более опасны по сравнению с внешним хакером, потому что они могут выполнять вредоносные действия очень структурированным образом, плавно, быстро и нечетко, что может серьезно повлиять на организацию.

Инсайдерские атаки могут выполняться злоумышленниками на территории провайдера или пользователя. Злоумышленник может легко получить пароли, криптографические ключи и файлы. Эти атаки могут включать в себя различные виды мошенничества, повреждения или кражи информации и неправомерного использования ИТ-ресурсов. Угроза вредоносных атак возросла из-за отсутствия прозрачности в процессах и процеду-

рах облачного провайдера. Это означает, что провайдер может не раскрывать, как сотрудникам предоставляется доступ и как этот доступ контролируется или как анализируются отчеты, а также соответствие политикам. Кроме того, пользователи плохо осведомлены о методах найма своего провайдера, которые могут открыть дверь для хакеров или других злоумышленников в Облако, чтобы украсть конфиденциальную информацию или получить контроль над Облаком. Предоставленный уровень доступа может позволить злоумышленникам собирать конфиденциальные данные или получить полный контроль над облачными службами практически без риска обнаружения. Поэтому перемещение критически важных приложений и конфиденциальных данных в общую облачную среду является серьезной проблемой. Это связано с тем, что организация теряет контроль над данными и полностью зависит от безопасности и защиты данных облачного провайдера. Чтобы смягчить эти опасения, поставщик облачных решений должен гарантировать, что клиенты могут по-прежнему пользоваться теми же средствами контроля безопасности и конфиденциальности своих приложений и служб, предоставляя этим клиентам доказательства того, что их организация и клиенты защищены.

Анализ стратегий смягчения последствий

Одними из первых рассмотрели проблему управления конфиденциальной информацией в среде совместных информационных систем (CIS) Чен и Малин [7]. Они предложили структуру под названием «Система обнаружения аномалий на базе сообщества» (CADS) для обнаружения внутренних угроз на основе информации, записанной в журналах доступа к средам совместной работы. CADS использует формальную статистическую модель для измерения отклонения пользователей от предполагаемых сообществ, чтобы предсказать, какие пользователи являются аномальными, путем анализа журналов доступа к CIS и, следовательно, изучения моделей поведения пользователей для обнаружения аномальных инсайдеров.

Чиа Мей, Гуан и др. [8] исследовали проблему последовательности действий при атаке для компрометации системы в облаке. Злоумышленник может сочетать несколько уязвимостей в системе безопасности и часто применяет подход к постоянной атаке, состоящий из последовательности атакующих действий в интеллектуальной атаке. Инсайдер может злоупотреблять облачными вычислениями или атаковать несколько машин в облаке. Это наносит более серьезный ущерб, чем в сетевой среде, где машины распределены и независимы. Поэтому авторы предложили Скрытую марковскую модель для обнаружения таких атак путем изучения этапов плана атаки и анализа журналов для определения последовательности атак.

В своём исследовании Жунь-Хо, Мин-Ву и др. [9] решили проблему того, что инсайдеры используют свои легитимные полномочия для утечки информации в сеть. Инсайдеры могут использовать привилегии программы и запускать программу ненормальным образом, чтобы достичь целей своей атаки. Поэтому авторы применили дерево атак и специальный монитор неправомерного использования, чтобы уменьшить нарушение безопасности за счет выявления инсайдерской информации, предотвращения ненормальных действий инсайдеров, предотвращения неправомерного использования ресурсов и управления политикой безопасности и обновления базы данных.

Йезин и Панда [10] исследовали проблему злонамеренных модификаций реляционных баз данных инсайдерами. Зависимости могут использоваться инсайдерами для внесения несанкционированных изменений в данные. Инсайдеры могут изучать ограничения на зависимости между таблицами, атрибутами и элементами данных для изменения данных. Поэтому сокрытие зависимостей от инсайдеров может помешать им изменить данные. Однако они все еще могут обнаружить скрытые зависимости, сотрудничая и обмениваясь информацией о различных зависимостях между собой. Для предотвращения модификаций были разработаны два метода: алгоритм разреза и граф модификации. Алгоритм вырезания определяет, какие зависимости следует скрыть. Изменения, сделанные авторизованными и неавторизованными инсайдерами, создают графы модификаций инсайдеров. Граф модификации, сгенерированный алгоритмами, показывает разрешенные и неавторизованные элементы данных, которые может изменить инсайдер.

Отдельного внимания заслуживает подход Брдичка и др. [11], в котором они рассматривают проблему обнаружения злонамеренного внутреннего нарушителя путем мониторинга сетевой активности и использования корпоративных приложений с помощью анализа графов, динамического отслеживания и машинного обучения. Эти инструменты могут точно идентифицировать известные атаки, но они реагируют и могут ускользнуть от ранее невидимого враждебного поведения. Поэтому авторы предложили подход, сочетающий обнаружение структурных аномалий из социальных и информационных сетей и психологическое профилирование индивидуумов. Психологическая модель позволит определить лиц, обладающих мотивацией и способностью совершить нападение.

Также не менее полезна может быть платформа, предложенная Нитиянандам, Тамилселван и др. [12]. Структурно она поделена на уровни для мониторинга активности пользователей с целью предотвращения злонамеренных действий изнутри. Платформа предотвращает аномальные действия инсайдеров в ИС, отслеживая актив-

ность точки использования. Она отслеживает носители передачи данных и проверяет неправомерное использование ресурсов инсайдером, сравнивая переданный ресурс с базой данных.

Заключение

Инсайдерские атаки, существующие в облачной системе, пытаются использовать ее слабые места и представляют серьезную угрозу для организаций. Благодаря гибкости облачной системы злоумышленники-инсайдеры могут манипулировать привилегиями для удаленного доступа к конфиденциальной информации. Хуже того, вредоносную активность внутри системы поставщика облачных услуг трудно обнаружить, когда в облачной среде существует сговор и сотрудничество между несколькими инсайдерами или между инсайдером и злоумышленниками извне. И это может иметь серьезные последствия для конфиденциальности, целостности и доступности данных. Однако до сих пор не существует однозначного и исчерпывающего подхода по противодействию инсайдерской угрозе в Облаке. Для решения этой проблемы необходимо взвешенное сочетание как организационных методов, так и технических средств и систем защиты с учётом специфики деятельности конкретной организации и, конечно же, дальнейшие исследования в данной сфере для создания принципиально новых подходов.

ЛИТЕРАТУРА

1. Claycomb, W.R., & Nicoll, A. (2021). Insider Threats to Cloud Computing: Directions for New Research Challenges. Paper presented at the Computer Software and Applications Conference (COMPSAC), IEEE 36th Annual.
2. Richardson, Robert. (2018). CSI computer crime and security survey. Computer Security Institute, 1, 1–30.
3. Buyya, Rajkumar, Yeo, Chee Shin, Venugopal, Srikumar, Broberg, James, & Brandic, Ivona. (2019). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems, 25(6), 599–616.
4. Jianfeng, Yang, & Zhibin, Chen. (2020). Cloud Computing Research and Security Issues. Paper presented at the Computational Intelligence and Software Engineering (CiSE), International Conference on.
5. AlZain, M.A., Pardede, E., Soh, B., & Thom, J. A. (2021). Cloud Computing Security: From Single to Multi-clouds. Paper presented at the System Science (HICSS), 45th Hawaii International Conference on.
6. Sundararajan, Sudharsan, Narayanan, Hari, Pavithran, Vipin, Vorungati, Kaladhar, & Achuthan, Krishnashree. (2011). Preventing Insider Attacks in the Cloud. In A. Abraham, J. Lloret Mauri, J. Buford, J. Suzuki & S. Thampi (Eds.), Advances in Computing and Communications (Vol. 190, pp. 488–500): Springer Berlin Heidelberg.
7. Chen, You, & Malin, Bradley. (2021). Detection of anomalous insiders in collaborative environments via relational analysis of access logs. Paper presented at the Proceedings of the first ACM conference on Data and application security and privacy.
8. Chia-Mei, Chen, Guan, D.J., Yu-Zhi, Huang, & Ya-Hui, Ou. (2012). Attack Sequence Detection in Cloud Using Hidden Markov Model. Paper presented at the Information Security (Asia JCIS), Seventh Asia Joint Conference on.
9. Jung-Ho, Eom, Min-Woo, Park, Seon-Ho, Park, & Tai-Myoung, Chung. (2021). A framework of defense system for prevention of insider's malicious behaviors. Paper presented at the Advanced Communication Technology (ICACT), 13th International Conference on.
10. Yaseen, Q., & Panda, B. (2020). Malicious Modification Attacks by Insiders in Relational Databases: Prediction and Prevention. Paper presented at the Social Computing (SocialCom), IEEE Second International Conference on.
11. Brdiczka, O., Juan, Liu, Price, B., Jianqiang, Shen, Patil, A., Chow, R., . . . Ducheneaut, N. (2021). Proactive Insider Threat Detection through Graph Learning and Psychological Context. Paper presented at the Security and Privacy Workshops (SPW), IEEE Symposium on.
12. Nithiyanandam, C., Tamilselvan, D., Balaji, S., & Sivaguru, V. (2021). Advanced framework of defense system for prevetion of insider's malicious behaviors. Paper presented at the Recent Trends In Information Technology (ICRTIT), International Conference on.

Журнал «Современная наука: актуальные проблемы теории и практики»