УГРОЗЫ БЕЗОПАСНОСТИ В ОБЛАЧНЫХ ТЕХНОЛОГИЯХ И МЕТОДЫ ИХ УСТРАНЕНИЯ

А.С. Тонких, *аспирант*
Е.Ю. Авксентьева, *канд. пед. наук, доцент*
Национальный исследовательский университет ИТМО
(Россия, г. Санкт-Петербург)

DOI:10.24412/2500-1000-2024-1-2-232-238

Аннотация. *В данной работе изучаются актуальные проблемы и методы борьбы с ними в области облачных технологий. Особое внимание автор уделил безопасности в облачной среде, т.к. для обработки и хранения данных является универсальным решением, которым пользуются как большие компании, так и частные пользователи. Концепция облачных технологий очень важна, так как она может стать ключевым фактором в развитии бизнеса. Рынок полон различных сервисов разного качества, но у всех них есть ряд ключевых проблем, которые описаны в работе.*

Ключевые слова: *облачные технологии, безопасность, угрозы, атаки на облачную инфраструктуру, снижение воздействия.*

В настоящее время предприятия активно внедряют облачные сервисы в рамках цифровой трансформации, чтобы пересмотреть операции и перестроить бизнес-модели. Однако, такое широкое внедрение облачных сервисов создает новые возможности для киберпреступников. В преддверии цифровой трансформации, организации сталкиваются с ограниченным временем для обдумывания и внедрения эффективных мер безопасности. В результате, предприятия часто отказываются от применения проверенных рекомендаций и стандартных процедур, что затрудняет оценку и управление рисками. По мере перехода к облачным технологиям, организации осознают необходимость объединения разрозненных подходов и программ в единую стратегию. Они сталкиваются с вызовом сохранения гибкости и возможности использования облачных сервисов, при этом защищая конфиденциальность данных и обеспечивая безопасность транзакций. Для организаций, которые рассматривают переход к облачным сервисам, важно найти баланс между развитием стратегии «безопасность превыше всего» и использованием преимуществ облачных технологий. Это требует внимания к безопасности и защите конфиденциальности данных вместе с активным развитием облачных сервисов.

Исследования, проведенные поставщиками решений в области информационной безопасности, подтверждают наличие важных вызовов, с которыми сталкиваются пользователи облачных услуг. Согласно отчетам Trend Micro [1] и MBA (ISC)² [2] об облачной безопасности на 2023 год, облачные системы продолжают привлекать все большее внимание злоумышленников и становятся объектом различных типов атак и инцидентов безопасности.

Растущая тревожность аналитиков и экспертов в области информационной безопасности связана с угрозами, которые могут потенциально повлиять на облачные инфраструктуры. Отчет Trend Micro [1] указывает на такие проблемы, как мошенничество с использованием теневых облачных сервисов, уязвимости множественности облачных хранилищ, утечки данных, распространение вредоносных программ и DDoS-атаки. Например:

1. Мошенничество с использованием теневых облачных сервисов: согласно отчету, 33% организаций столкнулись с угрозой мошенничества с использованием таких сервисов.

2. Уязвимости облачных хранилищ: 66% организаций сообщили о случаях эксплуатации уязвимостей в облачных хранилищах, что позволяет злоумышленникам по-

лучать несанкционированный доступ к данным.

3. Утечки данных: более половины организаций (52%) столкнулись с проблемой утечки данных в облачной среде.

4. Распространение вредоносных программ: 22% организаций обнаружили проникновение вредоносных программ в свои облачные инфраструктуры.

5. DDoS-атаки: 29% организаций столкнулись с DDoS-атаками, направленными на их облачные ресурсы.

В свою очередь, отчет от MBA (ISC)² [2] подчеркивает важность реализации политик контроля доступа и обучения персонала в сфере облачной безопасности, однако только 28% организаций проводят регулярные программы повышения осведомленности и обучения по вопросам безопасности облака. Также отчет указывает на возрастающее значение облачной безопасности как услуги (CSaaS), где 60% организаций уже используют или планируют использовать такие услуги для повышения безопасности в облачной среде.

Проблемы облачной безопасности могут быть разделены на несколько категорий. Во-первых, это безопасность и конфиденциальность данных. Для обеспечения их безопасности применяются меры защиты данных, системы управления идентификацией, меры физической и личной безопасности, а также меры безопасности на уровне приложений и маскировки данных. Во-вторых, важным аспектом является соблюдение требований и нормативов, таких как PCI DSS, HIPAA и закон Сарбейнса-Оксли. Эти стандарты требуют частых проверок и отчетности со стороны поставщиков облачных услуг, чтобы обеспечить соответствие требованиям безопасности данных. Третья категория проблем связана с юридическими и договорными вопросами. Здесь стороны должны установить соглашения об ответственности, интеллектуальной собственности и условиях прекращения обслуживания. Это помогает регулировать юридические аспекты, связанные с облачными услугами и защитой данных.

Так же основной проблемой безопасности облака является безопасность доступа к нему. Она связана с определением, кому предоставлен доступ к информации. Особенно в публичных облаках, где поставщики услуг предоставляют общедоступные ресурсы, безопасность доступа является критическим вопросом. Системы управления идентификацией играют важную роль в облачной безопасности, предоставляя возможность контролировать доступ к облачным данным. Клиенты могут использовать инструменты мониторинга регистрации событий для снижения риска злоупотребления правами доступа со стороны администраторов поставщиков услуг. Обычно облачная безопасность и безопасность доступа к облаку рассматриваются как разные аспекты. Облачная безопасность охватывает все аспекты безопасности в облачной среде, в то время как безопасность доступа к облаку является одним из ключевых моментов облачной безопасности. Она направлена на обеспечение защиты облачного контента от неавторизованного доступа, что предотвращает нарушения безопасности и конфиденциальности данных.

Значительным фактором для облачной безопасности является управление и контроль над облачной инфраструктурой. Когда ресурсы и данные находятся в виртуальных машинах, владение и управление облаком требует особого внимания и строгих мер безопасности.

В целом, облачная безопасность включает в себя различные аспекты, проблемы и методы борьбы с рисками и угрозами связаны с использованием мер безопасности на разных уровнях - от защиты данных и систем управления идентификацией до соблюдения требований нормативов и обеспечения безопасности доступа к облаку.

Угрозы и методы борьбы с ними

Обеспечение безопасности данных в облачных вычислениях является важной задачей, и для этого необходимо анализировать наиболее распространенные угрозы. Развертывание облачных серверов сопряжено с определенными проблемами, которые отличаются от традиционных центров обработки данных. Переход в об-

лачную среду влечет за собой появление новых угроз, связанных с виртуализацией и управлением вычислительной мощностью через Интернет. Вместо физического управления серверами, как в традиционных дата-центрах, в облачной среде серверы управляются удаленно. Важно реализовать ограничение доступа и контролировать изменения системы для обеспечения безопасности данных.

Выделим следующие угрозы:

1. Уязвимости в виртуальной среде.
2. Недостаточное сегментирование и распределение ролей.
3. Небезопасные интерфейсы и API.
4. Инсайдеры.
5. Компрометация аккаунта или сервиса.
6. Использование облачных ресурсов в преступных целях.
7. Проблемы с технологией.
8. Неизвестный профиль риска.
9. Кража личных данных.
10. Потеря данных.

Уязвимости в виртуальной среде. Поскольку серверы облачных вычислений и локальные серверы используют одну и ту же операционную систему и приложения, угрозы вредоносного ПО и удаленные взломы становятся обычным явлением. Параллельное использование виртуальных машин увеличивает риск атаки. Для защиты от таких угроз необходимо разрабатывать правила детектирования и использовать методы блокирования вредоносной активности и постоянно проводить аудит безопасности.

Недостаточное сегментирование и распределение ролей. Недостаточное внимание сегментации в облачной среде позволяет злоумышленникам в случае проникновения беспрепятственно осуществлять боковое перемещение по зонам в облачной среде, что увеличивает радиус поражения. Каждой зоне в облачной среде должны быть выделены отдельные вычислительные ресурсы, сетевые ресурсы и ресурсы хранения [3]. Например, уровни управления и данных должны находиться в разных зонах и им должны быть выделены отдельные ресурсы. А также в рамках стратегии защиты сегментация используется для ограничения доступа к внутренним облачным зонам из общедоступной зоны, обмен данными между рабочими станциями в пределах одной зоны и между разными зонами должен быть ограничен разрешенными потоками трафика и путями. Применение этого принципа важно при предоставлении разрешений на доступ к сети для привилегированных и непривилегированных пользователей. Например, этот принцип применяется при предоставлении доступа привилегированным пользователям к интерфейсам управления и разрешения доступа непривилегированных пользователей к рабочим станциям или приложениям.

Небезопасные интерфейсы и API относятся к интерфейсам прикладного программирования, которые представляют собой стандарты и протоколы, используемые потребителями для подключения к облачным сервисам. Поскольку безопасность облачных сервисов зависит от этих API, они должны иметь безопасные стандарты сертификации, надлежащие механизмы контроля доступа и мониторинга активности, чтобы избежать таких угроз, как анонимный доступ, многоразовые токены или пароли, ненадлежащая авторизация, ограниченный мониторинг и возможность ведения журнала [4].

Инсайдеры. Это могут быть доверенные лица в организации, которые могут получить доступ к конфиденциальным активам. Они могут выполнять непривилегированные действия с активами организации и наносить ущерб производительности или их деятельность может привести к финансовым потерям.

Компрометация аккаунта или сервиса происходит, если злоумышленник получает доступ к учетным данным, после чего взломанный аккаунт становится инструментом для проведения атак. Злоумышленник может заниматься шпионажем, изменять информацию в собственных интересах, манипулировать, перенаправлять потребителей на нелегальные сайты.

Использование облачных ресурсов в преступных целях можно описать как неэтичные и незаконные действия потребителей, направленные на нелегитимное ис-

пользование услуг. Недорогая инфраструктура, большие ресурсы, предоставление услуг, слабые процедуры регистрации способствуют анонимности спамеров, преступников и других злоумышленников, чтобы достичь своей цели в атаке на систему. Поставщики облачных услуг, такие как Amazon, Google, Facebook, Twitter и т. д., используются для запуска троянов и ботнетов.

Проблемы с технологией возникают в многопользовательских системах, где услуги предоставляются с использованием общей инфраструктуры для разных пользователей, имеющих доступ к одной и той же виртуальной машине. Уязвимости в гипервизорах (используемых в целях изоляции) позволяют злоумышленникам получить неправомерный доступ и контролировать виртуальные машины легитимных пользователей.

Неизвестный профиль риска может возникать в случае экономии времени и ресурсов на поддержание инфраструктуры. Так как потребители не обязаны соблюдать внутренние процедуры безопасности, исправления, усиления, аудита, протоколирования и т. д., это приводит к появлению неизвестного профиля риска, который может стать причиной серьезных угроз [5].

Кража личных данных происходит, когда злоумышленник выдает себя за другого человека, чтобы получить учетные данные пользователя и доступ к его активам.

Таблица 1. Угрозы и методы борьбы с ними

Угрозы безопасности	Методы смягчения последствий
Уязвимости в виртуальной среде	- Необходимо проводить систематическое сканирование на уязвимости и настроить процесс их устранения
Недостаточное сегментирование и распределение ролей	- Уровни управления и данных должны находиться в разных зонах - Обмен данными между рабочими станциями в пределах одной зоны и между разными зонами должен быть ограничен разрешенными потоками трафика и путями - Разграничение доступа привилегированных и непривилегированных пользователей - Мониторинг сетевой активности и настройка межсетевых экранов
Небезопасные интерфейсы и API	- Использование надежных механизмов аутентификации и контроля доступа. - Использование шифрования при передаче данных. - Анализ интерфейсов облачных провайдеров. - Правильное понимание цепочки зависимостей, связанных с API.
Инсайдеры	- Необходимо управление ресурсами (HRM). - Подготовка юридического соглашения. - Строгое применение процедуры управления цепочкой поставок. - Обеспечение надлежащей ясности в вопросах безопасности и административных процессов.
Компрометация аккаунта или сервиса	- Правильное понимание политик безопасности и соглашений об уровне обслуживания (SLA). - Использование многофакторных методов аутентификации. - Строгий мониторинг для выявления несанкционированных действий. - Контроль обмена учетными данными между потребителями ислужбами.
Использование облачных ресурсов в преступных целях	- Использование строгой авторизации и аутентификации. - Надлежащий аудит сетевого трафика. - Усиленный мониторинг мошенничества с кредитными картами.
Проблемы с технологией	- Использование более совершенных механизмов аутентификации и контроля доступа. - Мониторинг среды на предмет несанкционированных изменений/действий. - Использование SLA для исправлений и устранения уязвимостей.
Неизвестный профиль риска	- Раскрытие соответствующих журналов, данных и деталей инфраструктуры.
Кража личных данных	- Надежные пароли, механизмы аутентификации и контроля доступа.
Потеря данных	- Регулярное резервное копирование.

	- Используя надлежащие методы шифрования. - Реализация генерации, хранения и управления сильными ключами. - Законодательное указание методов усиления и обслуживания поставщиков.

В работах [6-14] рассматриваются актуальные атаки на облачную инфраструктуру и методы снижения негативного воздействия.

Таблица 2. Атаки и методы борьбы с ними

Атаки	Методы снижения воздействия
SQL-инъекции [6]	- Избегание использования динамически генерируемого SQL в коде. - Использование соответствующую фильтрацию для обеззараживания вводимых пользователем данных. - Использование архитектуры на основе прокси для динамического обнаружения и извлечения пользовательского ввода.
Межсайтовый скриптинг (XSS)	- Использование активной фильтрации содержимого. - Использование совместной работы в браузере. - Использование технологии предотвращения утечки данных на основе контента. - Использование технологии обнаружения уязвимостей веб- приложений. - Подход, основанный на чертежах, позволяет минимизировать зависимость от веб-браузера. - Правильная настройка уровня защищенных сокетов (SSL). - Использование программ для защиты от вредоносного ПО.
Фишинг	- Идентификация спамерских писем. - Установка специализированных средств защиты.
DNS-атаки [7]	- Использование мер безопасности DNS, например, расширений безопасности системы доменных имен (DNSSEC).
MITM-атаки	- Правильная настройка уровня защищенных сокетов (SSL). - Использование инструментов шифрования, например, Dsniff, Ettercap, Wsniff, Airjack и т.д.
DOS-атаки [8]	- Использование более совершенных схем аутентификации и авторизации. - Использование системы обнаружения вторжений (IDS)/системы предотвращения вторжений (IPS).
DDOS-атаки [9]	- Использование более совершенных механизмов аутентификации и авторизации. - Использование системы обнаружения вторжений (IDS)/системы предотвращения вторжений (IPS). А также других специальных средств защиты.
Zombie Attacks	- Использование улучшенной аутентификации и авторизации. - Использование системы обнаружения вторжений (IDS)/системы предотвращения вторжений (IPS).
Sniffer Attacks	- Использование техники обнаружения снифферов на основе протокола разрешения адресов (ARP). - Использование техники обнаружения снифферов, основанной на времени передачи данных (Round-Trip Time, RTT).
Pollution attack [10]	- Обновление до актуальных версий сред и инструментов разработки
Wrapping Attack [11], [12]	- Использование надлежащего механизма подписи. - Использование правильной конфигурации Secure Socket Layer (SSL).
Cookie Poisoning [13]	- Реализация более совершенных схем шифрования. - Регулярная очистка данных cookies. - Управление сеансами.
CAPTCHA Breaking	- Увеличивая длину струны. - Использование пертурбативного фона. - Использование перекрытия букв для предотвращения атак вертикальной сегментации. - Использование шрифтов разного размера.
Google Hacking Attacks [14]	- Использование Robots.txt: Этот тег не может блокировать индексацию частного контента. Но он может помочь, если сканирование наносит вред вашему серверу. - Использование Robots meta: контролируют отображение отдельной HTML-

	страницы в результатах или вообще исключают ее из результатов. - Использование X-robots-tag: контролирует отображение страниц, отличных от HTML, в результатах или блокирует их отображение.
Атаки на гипервизоры	- Использование безопасный гипервизор и проводить мониторинг гипервизора. - Изоляция виртуальной машины.

Заключение

Облачные технологии представляют собой мощный эффективный инструмент использования информационных ресурсов. Количество угроз может быть снижено благодаря применению современных решений и защитных механизмов на различных уровнях виртуальной инфраструктуры.

Внедрение облачных технологий приводит к снижению затрат на программное обеспечение, улучшению качества и эффективности производственных процессов, а также обеспечению прозрачности и открытости данных. Благодаря возможностям, которые предоставляют облачные технологии, организации могут достичь своих целей в области информационной безопасности и повысить свою конкурентоспособность в современном цифровом мире.

Рассматриваемые угрозы и атаки на облачную инфраструктуру и методы борьбы с ними могут быть использованы для приоритезации возникающих инцидентов кибербезопасности в целях оценки защищенности данных в облачной системе.

Библиографический список

1. Trend Micro 2023 Cloud Security Report. – [Электронный ресурс]. – Режим доступа: https://resources.trendmicro.com/rs/945-CXD-062/images/2023-Cloud-Security-Report-TrendMicro-Final.pdf.

2. MBA (ISC)² 2023 Cloud Security Report. – [Электронный ресурс]. – Режим доступа: https://www.isc2.org/-/media/Project/ISC2/Main/Media/Marketing-Assets/CCSP/2023-Cloud-Security-Report-ISC2_final.pdf.

3. [Электронный ресурс]. – Режим доступа: https://www.cyber.gc.ca/sites/default/files/itsp80023-cloud-network-security-zones-v4-e.pdf.

4. CSA: The Notorious Nine Cloud Computing Top Threats // Cloud Security Alliance, 2013.

5. CSA: Top Threats to Cloud Computing // Cloud Security Alliance, 2010.

6. D. S. S. S. A. D. V. M. T. R. A. Katole. Detection Of Sql Injection Attacks By Removing The Parameter Values Of Sql Query // In 2018 2nd International Conference On Inventive Systems And Control (Icisc), Coimbatore, India, 2018.

7. [Электронный ресурс]. – Режим доступа: https://journals.edu.pl/index.php/awdj/article/view/10/5.

8. Rajendran R., Kumar S., Palanichamy Y. and Arputharaj K. Detection of Dos Attacks in Cloud Networks Using Intelligent Rule Based Classification System // Cluster Computing, 2018.

9. P. Z. N and P. H. Upadhyay. Preventing Cloud Systems Against Ddos Attack Using Hop Count Filter Approach // International Journal of Advanced Research In Computer Science. – 2018. – Vol. 9.

10. Anglano C., Gaeta R. and Grangetto M. Securing Coding-Based Cloud Storage Against Pollution Attacks, 2017.

11. Nasridinov A., Jeong Y.-S., Byun J.-Y. and Park Y.-H. A Histogram-Based Method For Efficient Detection Of Rewriting Attacks In Simple Object Access Protocol Messages // Security And Communication Networks. – 2016. – Vol. 9, № 6.

12. Kumar J., Rajendran B., Bindhumadhava B.S. and Babu N.S.C. Xml Wrapping Attack Mitigation Using Positional Token // In International Conference On Public Key Infrastructure And Its Applications (Pkia), Bangalore, India, 2017.

13. [Электронный ресурс]. – Режим доступа: https://www.techtarget.com/searchsecurity/definition/cookie-poisoning.
14. [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/contest/212086.php.

SECURITY THREATS IN CLOUD TECHNOLOGIES AND METHODS OF THEIR ELIMINATION

A.S. Tonkikh, *Postgraduate Student*
E.Yu. Avksentieva, *Candidate of Pedagogical Sciences, Associate Professor*
ITMO National Research University
(Russia, St. Petersburg)

Abstract. *This paper examines current problems and methods of dealing with them in the field of cloud technologies. The author paid special attention to security in the cloud environment, since it is a universal solution for data processing and storage, which is used by both large companies and private users. The concept of cloud technologies is very important, as it can become a key factor in business development. The market is full of various services of different quality, but they all have a number of key problems that are described in the work.*

Keywords: *cloud technologies, security, threats, attacks on cloud infrastructure, impact reduction.*