COMPUTER SCIENCE

УДК 000.00.000

Зонова Дарья Юрьевна
студентка бакалавриата,
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
DOI: 10.24412/2520-6990-2024-2195-10-14

СПОСОБЫ ЗАЩИТЫ ОБЛАЧНЫХ ХРАНИЛИЩ

Zonova Darya Yuryevna
undergraduate student,
St. Petersburg State Electrotechnical University "LETI"

WAYS TO PROTECT CLOUD STORAGE

Аннотация.
В последние годы задача хранения информации является очень актуальной как для личного использования, так и для бизнеса, где компаниям необходимо хранить огромное количество данных. Для хранения информации небольшим компаниям достаточно использования файловых хранилищ. В более крупных компаниях большинство данных хранится на серверах, сетевых накопителях или же они загружаются в облачные хранилища данных. Облачные хранилища позволяют пользователям хранить данные в интернете и получать к ним доступ из любой точки мира, что делает их удобными для обмена и совместной работы над документами.

Abstract.
In recent years, the task of storing information has become very relevant both for personal use and for business, where companies need to store huge amounts of data. To store information, small companies simply need to use file storage. In larger companies, most data is stored on servers, network-attached storage devices, or uploaded to cloud storage. Cloud storage allows users to store data online and access it from anywhere in the world, making it convenient for sharing and collaborating on documents.

Ключевые слова: *DDos-аттаки, облачные хранилища, TLS/SSL, Advanced Encryption Standard, Security Information and Event Management (SIEM).*
Keywords: *DDos attacks, cloud storage, TLS/SSL, Advanced Encryption Standard, Security Information and Event Management (SIEM).]*

Введение

История развития облачных хранилищ началась еще в начале 2000-х годов и с тех пор активно развивается с каждым годом. В то время компании Google и Amazon начали создавать масштабируемые инфраструктуры для своих собственных нужд и осознали, что эти инфраструктуры могут быть использованы для предоставления облачных услуг. Сегодня облачные хранилища используются во многих отраслях, включая банковское дело, медицину, образование, мультимедиа и др.

Однако, как и другие способы хранения информации, облачные хранилища имеют свои риски и уязвимости, в том числе связанные с безопасностью. Данный вопрос безопасности становится критически важным. На сайте Федеральной службы по техническому и экспортному контролю опубликован в открытом доступе «Банк данных угроз безопасности информации», в котором содержится информация о тысячах уязвимостях, которые связаны с различными технологиями и программными продуктами. Среди уязвимостей в этой таблице можно найти такие, в которых объектом воздействия являются данные, хранимые в облаке. Это может быть связано с недостаточной защитой данных, утечкой информации, несанкционированным доступом или другими видами угроз безопасности.

Аспект безопасности	Русские облачные хранилища	Зарубежные облачные хранилища
Шифрование данных	Обычно предоставляются различные методы шифрования данных, включая TLS/SSL и AES-256.	Первостепенное внимание уделяется шифрованию данных, особенно AES-256 и дополнительным методам шифрования.
Физическая безопасность	Центры обработки данных обычно находятся в стратегических местах с высокой степенью физической безопасности, включая охрану, контролируемый доступ и видеонаблюдение.	Аналогично реализована высокая физическая безопасность, обеспечивающая защиту от несанкционированного доступа.
Защита от DDoS-атак	Некоторые русские облачные хранилища обладают механизмами защиты от DDoS-атак, используя специальные системы фильтрации трафика и заглушения атакующих узлов.	Зарубежные хранилища также предлагают мощные системы защиты от DDoS-атак, часто используя глобальные сети масштаба провайдера.
Резервное копирование	Русские облачные хранилища обычно предлагают функции автоматического резервного копирования данных, позволяющие восстанавливать файлы и системы в случае сбоя или потери данных.	Зарубежные хранилища также обеспечивают функции резервного копирования и восстановления данных для предотвращения потери информации.
Уровень доступа и аутентификация	Обеспечивается разграничение прав доступа и механизмы аутентификации для защиты от несанкционированного доступа к данным.	Также доступны многоуровневые механизмы аутентификации и контроля прав доступа, позволяющие предотвратить несанкционированный доступ к информации.
Стоимость	Цены на русские облачные хранилища могут быть более доступными для отечественных потребителей, особенно для небольших предприятий и частных лиц.	Стоимость зарубежных хранилищ может быть немного выше, но зачастую они предлагают более широкий выбор опций и служб, что может оправдать эту цену.

Следовательно, разработка и использование эффективных технологий безопасности в облачных системах является критически важным для защиты данных и предотвращения возможных угроз.

Исследование

В данном исследовании будут рассмотрены технологии безопасности в облачных системах, проведен обзор существующих решений и методов защиты данных на примере Яндекс Диска.

Шифрование данных

Одной из важных и наиболее распространенных технологий является шифрование данных. С помощью шифрования данные защищаются путем их преобразования в закодированный формат, который может быть декодирован только с использованием специального ключа. Например, хранилище Яндекс Диск передает данные с использованием SSL-шифрования для их защиты во время передачи по сети, то есть в момент «загрузки информации» на диск.

Шифрование данных на Яндекс.Диске обеспечивается с помощью алгоритма Advanced Encryption Standard (AES) с длиной ключа 256 бит. Этот алгоритм является стандартом шифрования в большинстве современных систем и обеспечивает высокий уровень защиты данных от несанкционированного доступа. Шифрование происходит на нескольких уровнях:

1. Шифрование во время передачи данных - Яндекс.Диск использует протоколы шифрования данных, такие как TLS/SSL, для защищенной передачи информации между устройством пользователя и серверами Яндекса. Это позволяет защитить данные от перехвата или изменения в процессе передачи.

2. Шифрование в покое - Данные на серверах Яндекса также защищены при помощи методов шифрования в покое. Это обеспечивает защиту информации на физическом уровне, чтобы предотвратить несанкционированный доступ к данным даже в случае физического доступа к серверам.

3. Шифрование паролем - Для дополнительной защиты данных в Яндекс.Диске пользователи могут использовать свой пароль от учетной записи Яндекса. При логине в Яндекс.Диск осуществляется шифрование данных с использованием этого пароля. Важно выбрать надежный пароль, чтобы защитить свою учетную запись и данные.

Пользователям рекомендуется также применять хорошие практики безопасности, такие как использование сложных паролей, активация двухфакторной аутентификации и обновление программного обеспечения на устройствах для минимизации рисков безопасности. Стоит учесть, что ключи шифрования хранятся отдельно от данных.

Процесс шифрования данных на Яндекс.Диске выглядит следующим образом:

1. Пользователь загружает файл на свой Яндекс.Диск.

2. Яндекс.Диск автоматически разбивает файл на небольшие блоки размером около 16 килобайт.

3. Для каждого блока генерируется уникальный ключ шифрования. Этот ключ состоит из двух частей: секретного ключа, известного только Яндексу, и открытого ключа, который доступен пользователю.

4. Каждый блок файла шифруется с использованием секретного ключа. В результате получается зашифрованный блок данных.

5. Зашифрованные блоки данных отправляются на серверы Яндекса, где они хранятся в зашифрованном виде.

6. При скачивании файла с Яндекс.Диска, Яндекс дешифрует каждый блок с использованием открытого ключа. В результате пользователь получает расшифрованный файл, который можно открыть и использовать.

Таким образом, данные на Яндекс.Диске всегда хранятся в зашифрованном виде, что обеспечивает их защиту от неправомерного доступа.

Аутентификация и авторизация

Технологии, обеспечивающие идентификацию и управление доступом к облачным ресурсам. Аутентификация используется для проверки подлинности пользователей, например, с помощью сравнения введенного пользователем пароля с ключом, который хранится в базе данных. Также аутентификация возможна с помощью электронной цифровой подписи (ЭЦП). В этом случае пользователь вводит логин и пароль, на основе которых формируется приватный ключ с использованием SHA-256 шифрования. Далее клиент получает от сервера случайное число и генерирует второе случайное число для себя. С помощью приватного ключа и формируется ЭЦП, являющаяся функцией от зашифрованного логина и пароля. Сервер проверяет корректность ЭЦП с помощью открытого ключа. Авторизация же необходима для управления доступом к облачным ресурсам. Это означает, что только авторизированные пользователи получат доступ к информации, и их подлинность будет однозначно определена. Например: вход в яндекс аккаунт.

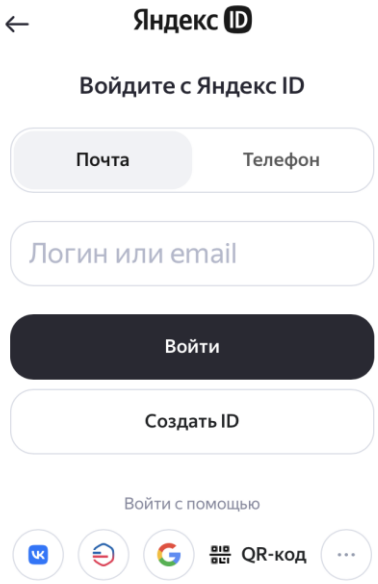

Рисунок 1 - При входе в Яндекс аккаунт через браузер.

В Яндексе собственная экосистема и в любую из множества систем можно войти с помощью яндекс ID, абсолютно разными способами.

Аутентификация на Яндекс.Диске процесс подтверждения того, что пользователь является тем, за кого себя выдает. Для этого используется двухфакторная аутентификация. Она заключается в том, что при входе в свой аккаунт пользователь должен ввести не только свой пароль, но и код подтверждения, который приходит на указанный им номер телефона.

Авторизация на Яндекс.Диске предоставление пользователю прав на доступ к определенным ресурсам или действиям. Работает следующим образом: пользователь может предоставить другим людям права на просмотр, редактирование или скачивание определенных файлов или папок. Для этого нужно просто отправить ссылку на нужный файл или папку и указать, какие права нужно предоставить.

Мониторинг безопасности

Еще одной важной технологией является мониторинг безопасности. Он представляет собой сбор, систематизирование и анализ сведений о состоянии корпоративной сети и поведении ее пользователей, необходим для отслеживания активности и обнаружения возможных угроз безопасности в облачных системах.

Основной целью анализа является выявление несанкционированных действий сотрудников компании или посторонних лиц. Мониторинг информационной безопасности производится на нескольких уровнях. На уровне операционной системы и сетевой инфраструктуры используется инструментарий для отслеживания событий и сетевой активности, позволяющий регистрировать события безопасности. Для мониторинга безопасности приложений

используется специализированное программное обеспечение, позволяющее обнаруживать уязвимости в коде, контролировать их исправление. Компания Яндекс также использует системы Security Information and Event Management (SIEM) для централизованного мониторинга и обнаружения угроз в реальном времени.

Security Information and Event Management (SIEM) - это система, которая собирает, анализирует и хранит информацию о событиях, связанных с безопасностью. Она позволяет централизованно контролировать и анализировать данные о безопасности, а также обнаруживать угрозы в режиме реального времени.

SIEM-системы используют различные методы анализа данных, такие как корреляция событий, обнаружение аномалий, анализ поведения пользователей и другие. Это позволяет выявлять угрозы на ранних стадиях, когда они еще не успели нанести серьезный ущерб.

Кроме того, SIEM-системы могут быть интегрированы с другими системами безопасности, такими как системы предотвращения вторжений (IDS), системы мониторинга и управления сетями (NMS) и другие. Это позволяет создать комплексную систему безопасности, которая будет эффективно защищать организацию от различных видов угроз.

Атаки на облачные хранилища

Кросс-облачные атаки

Одним из примеров таких атак является атака, основанная на уязвимости с недостаточной проверкой прав доступа. В этом случае злоумышленник может получить доступ к файлам, находящимся на диске, если у него есть ссылка на файл или он знает путь к нему. Злоумышленник может использовать различные методы для получения ссылки на файл, например, перехватывая трафик или выполняя фишинговые атаки.

В 2022 году стало известно, что хакеры начали использовать ресурсы облачного сервиса «Яндекс Диск» в качестве вспомогательного места хранения зловредных скриптов при проведении кибератак на российские компании. Ранее в подобных схемах злоумышленники использовали сервисы OneDrive и Dropbox.

Причина перестройки на отечественную платформу заключается в том, что корпоративным системам безопасности сложно идентифицировать вредоносное ПО, которое применяет «Яндекс Диск» в качестве контрольного сервера. Трафик оттуда и туда разрешён во многих российских компаниях, так как эта платформа применяется для обмена документов с филиалами или удалёнными сотрудниками в качестве альтернативы зарубежным решениям.

Пример такой атаки заключается в том, что жертва получает по электронной почте письмо с вложением текстового документа. При попытке его открытия начинается загрузка макроса с «Яндекс Диска», а также его запуск для копирования вредоносной библиотеки на ПК. Пользователь ничего не может заметить, так как он видит только открытый присланный документ.

В данном случае злоумышленники используют пункт в условиях использования «Яндекс Диск», где указано, что сервис не проверяет содержимое облачных папок пользователей, так как это нарушает их конфиденциальность. Если код выложили в хранилище, то «Яндекс» не может проверить, для чего он предназначен.

В этом случае под видом легитимного трафика передаются команды от хакеров через «Яндекс Диск». По утверждению экспертов, «передача команд производится путём записи их в файлы с определённым именем в определённой директории, уникальной для каждого заражённого хоста, а ответы на команды передаются аналогичным образом». Они рекомендуют пользователям не открывать незнакомые письма и вложения в них, так как даже эксперты по безопасности не могут сразу определить с помощью специальных инструментов, что в какой-то момент на ПК запустились макросы для распространения вредоносного софта. Эти вредоносны файлы можно обнаружить лишь в динамике при помощи средств мониторинга, а также с использованием последних версий корпоративного антивирусного ПО с возможностью анализа и блокирования подобных инцидентов.

DDoS-атаки

На облако могут быть предприняты атаки типа «отказ в обслуживании», которые вызывают перегрузку инфраструктуры, заставляя задействовать огромный объем системных ресурсов и не давая заказчикам пользоваться этой услугой. Внимание прессы чаще всего привлекают распределенные, или

DDoS-атаки, но есть и другие типы DoS-атаки, которые могут блокировать облачные вычисления. К примеру, злоумышленники могут запустить асимметричные DoS-атаки прикладного уровня, используя уязвимости в

Web-сервисах, базах данных или других облачных ресурсах, чтобы завалить приложение с очень малой полезной нагрузкой.

Вот, что нам предоставляет яндекс cloud в защиту от DDos-атак.

Рисунок 2 - Yandex cloud for DDoS.

Существует много команд хакеров, которые искусно разрабатывают новые способы атак на облачные хранилища, ежегодно появляются в сети слиты данные пользователей той или иной инфраструктуры. При этом всем компании не стоят на месте и модернизируют систему безопасности.

Кроме внешних атак есть и внутренняя угроза из-за халатности сотрудников

Ошибки и халатность сотрудников - одна из самых серьезных проблем безопасности, с которыми сталкиваются облачные вычислительные системы. Слабые методы обеспечения безопасности могут создать уязвимость для компаний, например, из-за входа в облачную инфраструктуру организации с помощью своих мобильных телефонов и домашних планшетов, тем самым оставляя уязвимую точку доступа, через которую организация может быть скомпрометирована.

Заключение

Облако и связанные с ним программные сервисы охватывают интернет-платформы, которые обеспечивают хранение данных, безопасность данных, приложения с повышенной гибкостью и возможностью совместной работы.

Глобальное внедрение облачных технологий происходит стремительными темпами. Причины такой массовой миграции заключаются в том, что организации хотят воспользоваться такими преимуществами, как более низкие фиксированные затраты, удобство автоматического обновления программного обеспечения, свобода от централизованного размещения, что, в свою очередь, способствует удаленной работе, наряду с улучшением сотрудничества и гибкости. Однако преимущества облачных услуг ограничиваются проблемами безопасности, связанными с использованием и развертыванием облака. Таким образом, понимание рисков, связанных с использованием облака, и способов их снижения, имеет первостепенное значение для компаний и частных лиц, которые хотят получить максим преимуществ от облачных технологий.

Литература:

1. Атака на облака [Электронный ресурс] Режим доступа: https://xakep.ru/2020/07/22/azure-aws-hacking-guide/
2. О защите веб-приложений [Электронный ресурс] Режим доступа: https://cloudnetworks.ru/application-protection/
3. DDoS-атаки в 2022 и методы защиты от них [Электронный ресурс] Режим доступа: https://habr.com/en/companies/slurm/articles/674218/
4. GoGrid Cloud Storage. http://www.gogrid.com/cloud-hosting.
5. GoGrid SLA. http://www.gogrid.com/legal/sla.php.
6. Internet Archive. http://www.archive.org/.
7. Nirvanix Storage Deliver Network. http://www.nirvanix.com/how-to-buy/self-service-pricing.aspx.
8. Rackspace Cloud Files. http://www.rackspacecloud.com/cloud_hosting_products/files.
9. Rackspace june 2009 outage. http://www.bbc.co.uk/blogs/technology/2009/10/the_sidekick_cloud_disaster.html.

Literature:

1. Attack on clouds [Electronic resource] Access mode: https://xakep.ru/2020/07/22/azure-aws-hacking-guide/
2. On the protection of web applications [Electronic resource] Access mode: https://cloudnetworks.ru/application-protection/
3. DDoS attacks in 2022 and methods of protection against them [Electronic resource] Access mode: https://habr.com/en/companies/slurm/articles/674218/
4. GoGrid Cloud Storage. http://www.gogrid.com/cloud-hosting.
5. GoGrid SLA. http://www.gogrid.com/legal/sla.php.
6. Internet Archive. http://www.archive.org/.
7. Nirvanix Storage Deliver Network. http://www.nirvanix.com/how-to-buy/self-service-pricing.aspx.
8. Rackspace Cloud Files. http://www.rackspacecloud.com/cloud_hosting_products/files.
9. Rackspace June 2009 outage. http://www.bbc.co.uk/blogs/technology/2009/10/the_sidekick_cloud_disaster.html.