УДК 004.42

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ УПРАВЛЕНИЯ РИСКАМИ БЕЗОПАСНОСТИ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

© 2024 М. А. Лапина[1], В. Г. Лапин[1], Д. О. Самко[2], М. Е. Токмакова[2]

[1] доцент кафедры вычислительной математики и кибернетики
e-mail: mlapina@ncfu.ru
Северо-Кавказский федеральный университет, Ставрополь
[2] студент кафедры вычислительной математики и кибернетики
Северо-Кавказский федеральный университет, Ставрополь

В статье рассматриваются исследования в области обеспечения безопасности облачных инфраструктур. Основной целью является разработка программного комплекса для оценки рисков безопасности в условиях возникновения угроз, что способствует повышению защиты учетных записей пользователей. Работа включает в себя анализ современных методов обеспечения информационной безопасности и моделирования угроз. В ходе исследования были выявлены основные механизмы работы с паролями, проведен анализ состояния информационной безопасности критических инфраструктур и разработан программный комплекс для выявления слабых мест в облачных системах. Полученные результаты должны способствовать снижению числа успешных кибератак и укреплению общей информационной безопасности.

Ключевые слова: безопасность, облачные инфраструктуры, информационная безопасность, программный комплекс, оценка рисков, угрозы, пароли, моделирование угроз, MFA (Multi-Factor Authentication), уязвимости.

DEVELOPMENT OF SECURITY RISK MANAGEMENT SOFTWARE FOR CLOUD INFRASTRUCTURE BASED ON DATA MINING

© 2024 M. A. Lapina[1], V. G. Lapin, D. O. Samko[2], M. E. Tokmakova[2]

[1] Docent, Department of Computational Mathematics and Cybernetics
e-mail: mlapina@ncfu.ru
North Caucasus Federal University
[2] Student, Department of Computational Mathematics and Cybernetics
North Caucasus Federal University, Stavropol

This article discusses the problem of ensuring the security of cloud infrastructures. The main goal is to develop a software package for assessing security risks in the face of threats, which helps to increase the protection of user accounts. The work includes an analysis of modern methods of ensuring information security and threat modeling. The study identified the main mechanisms for working with passwords, analyzed the state of information security of critical infrastructures, and developed a software package to identify weaknesses in cloud systems. The results obtained should help reduce the number of successful cyber-attacks and strengthen overall information security.

Keywords: security, cloud infrastructures, information security, software package, risk assessment, threats, passwords, threat modeling, MFA (Multi-Factor Authentication), vulnerabilities.

В условиях развития облачных технологий и возрастающей сложности информационных систем обеспечение безопасности становится ключевым

фактором для успешного и надежного функционирования бизнеса, его компонентов и систем [2–5]. Облачные инфраструктуры, предлагая гибкость и масштабируемость, одновременно открывают новые вектор атак для злоумышленников, и, к сожалению, традиционные методы оценки рисков безопасности часто оказываются недостаточными для эффективной защиты в динамично меняющихся условиях облачной среды.

Исследование посвящено разработке программного комплекса для оценки рисков безопасности облачной инфраструктуры на основе интеллектуального анализа данных. Система, основанная на передовых алгоритмах машинного обучения, способна выявлять угрозы, предсказывать потенциальные инциденты и предоставлять конкретные рекомендации по минимизации рисков [6, 7]. В статье подробно рассматриваются принципы работы разработанного комплекса, архитектура системы, используемые алгоритмы машинного обучения и результаты проведенных испытаний. Особое внимание уделено практическому применению системы в реальных условиях и ее влиянию на повышение уровня безопасности облачных инфраструктур.

Ожидается, что разработанный комплекс станет эффективным инструментом для управления рисками безопасности облачных инфраструктур, способствуя созданию более безопасной и надежной среды для хранения и обработки данных.

В соответствии с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017, объектами критической информационной инфраструктуры являются информационные системы, информационно-коммуникационные сети и автоматизированные системы управления объектами критической информационной инфраструктуры [1, 13].

Сегодня, когда цифровые технологии стремительно внедряются во все сферы экономики, количество компьютерных атак на критически важные информационные ресурсы государственных и коммерческих организаций, промышленных компаний, корпораций и частных лиц растет не менее стремительно [8, 9].

Согласно данным, представленным в аналитическом отчете Positive Technologies, в IV квартале 2020 г. количество инцидентов увеличилось на 3,1% по сравнению с III кварталом и на 41,2% по сравнению с аналогичным периодом 2019 г. На долю целевых атак пришлось 80% от общего числа.

В таблице 1 показаны виды сетевых атак. Они бывают разных типов, и каждый из них представляет собой угрозу для данных, ресурсов и конфиденциальности пользователей.

Таблица 1

Виды сетевых атак и типовые методы борьбы

Тип атаки	**Описание**	**Реализация**	**Методы борьбы**
Переполнение буфера (buffer overflows)	Поиск уязвимостей, способных вызвать нарушение границ памяти, выполнить произвольный бинарный код от имени авторизованного пользователя	Подготовка кода для привилегированного выполнения. Модификация последовательности команд программы для передачи управления подготовленному коду	Корректировка исходных кодов программы. Использование неисполнимых буферов. Применение проверок выхода за границы. Проведение проверок целостности
Спец. программы	Вирусы, троянский конь, сниффер, руткит	Скрытый характер функционирования в системе, сбор данных	Антивирусные средства и регулярное обновление их сигнатур, шифрование

Тип атаки	Описание	Реализация	Методы борьбы
Сетевая разведка	Сбор информации о сети с помощью общедоступных данных и приложений для планирования атаки	Сетевая разведка с помощью DNS-запросов, ICMP-запросов (эхо) и сканирования портов	Блокирование ICMP-запросов и ответов на пограничных маршрутизаторах. Использование систем обнаружения вторжений
IP-спуфинг	Злоумышленник выдает себя за пользователя системы	Вставка ложной информации или вредоносных команд в обычный поток данных	Контроль доступа, использование криптографической аутентификации
Инъекции	SQL-инъекция, межсайтовый скриптинг (XSS-атака), XPath-инъекция	Изменение параметров запроса к БД, встраивание в веб-страницу произвольного кода	Правила построения SQL-запросов, кодирование данных и управляющих символов, регулярное обновление
Отказ в обслуживании (DoS)	Легитимные пользователи не могут получить доступ к системе	Сохранение всех соединений в занятом состоянии	Функции антиспуфинга, применение систем обнаружения сетевых атак
Phishing-атаки	Обман или социальная разработка сотрудников для воровства их данных	Использование spam-рассылки через электронную почту или мессенджеры	Использование проверенных ресурсов, антивирусные средства, обновление баз сигнатур

В исследовании использовалось Amazon S3 (Simple Storage Service) – это объектное хранилище для хранения и извлечения любых объемов данных в любое время и из любого места в Интернете. Amazon S3 предлагает высокую доступность, долговечность и масштабируемость.

В таблице 2 приведена сравнительная характеристика для Amazon S3, Amazon EC2 И AWS IAM. Amazon S3, Amazon EC2 и AWS IAM являются ключевыми компонентами для создания и управления облачными решениями в AWS. Правильное использование этих сервисов обеспечивает надежность, масштабируемость, безопасность и эффективность работы облачных приложений.

Таблица 2

Сравнительная характеристика для Amazon S3, Amazon EC2 и AWS IAM

Характеристика	Amazon S3	Amazon EC2	AWS IAM
Основная функция	Облачное хранилище для объектов и файлов	Виртуальные серверы для запуска приложений	Управление идентификацией и доступом
Сценарии использования	Резервное копирование, архивирование, озера данных, аналитика больших данных	Хостинг приложений, баз данных и других сервисов	Управление пользователями, группами, ролями и политиками доступа
Масштабируемость	Автоматическое масштабирование объема хранилища	Масштабирование вычислительных ресурсов с различными типами инстансов	Масштабируется с числом пользователей и управляемых ресурсов
Модель оплаты	Оплата за используемое хранилище и передачу	Оплата за час использования инстансов, с опциями	Бесплатный уровень доступен, оплата за дополнительное

Характеристика	Amazon S3	Amazon EC2	AWS IAM
	данных	резервированных и спотовых инстансов	использование
Производительность	Высокая надежность и доступность (99% долговечности)	Высокая производительность с опциями для CPU, памяти и GPU	Не влияет на производительность, обеспечивает безопасный доступ
Интеграция	Интеграция с другими сервисами AWS, такими как EC2, RDS и Lambda	Используется с другими сервисами AWS, такими как S3, RDS и Lambda	Интеграция со всеми сервисами AWS для управления доступом
Управление	Управление через AWS Management Console, CLI, SDK	Управление через AWS Management Console, CLI, SDK	Управление через AWS Management Console, CLI, SDK
Документация	Обширная документация и примеры на сайте AWS	Обширная документация и примеры на сайте AWS	Обширная документация и примеры на сайте AWS

Эти сервисы дополняют друг друга, обеспечивая надежную облачную вычислительную среду, где S3 обрабатывает хранение, EC2 – вычислительную мощность, а IAM – безопасное управление доступом.

Функция для получения списка S3 бакетов отправляет запрос на получение списка всех S3 бакетов и выводит их имена.

s3_client. ListBuckets (): отправляет запрос на получение списка всех S3 бакетов.

outcome.IsSuccess(): проверяет, успешен ли запрос.

outcome.GetResult().GetBuckets(): возвращает список бакетов.

request.SetBucket(bucket_name): устанавливает имя бакета для проверки.

s3_client. GetBucketAcl(request): отправляет запрос на получение списка ACL (Access Control List) для указанного бакета.

outcome.GetResult().GetGrants(): возвращает список грантов (прав доступа).

grant.GetPermission() == Aws::S3::Model::Permission::READ: проверяет, есть ли у гранта разрешение на чтение.

ec2_client. DescribeInstances(request): отправляет запрос на получение списка всех EC2 экземпляров.

outcome.GetResult().GetReservations(): возвращает список резервирований.

reservation.GetInstances(): возвращает список экземпляров в каждом резервировании.

instance.GetPublicIpAddress().length() > 0: проверяет, есть ли у экземпляра публичный IP-адрес. Эта функция отправляет запрос на получение списка всех EC2 экземпляров и выводит их идентификаторы.

iam_client.ListUsers(request): отправляет запрос на получение списка всех IAM пользователей.

outcome.GetResult().GetUsers(): возвращает список пользователей.

request.SetUserName(user_name): устанавливает имя пользователя для проверки.

iam_client.ListMFADevices(request): отправляет запрос на получение списка MFA устройств для указанного пользователя.

outcome.GetResult().GetMFADevices().size() == 0: проверяет, если у пользователя нет MFA устройств.

Aws::SDKOptions options: опции для инициализации AWS SDK.

Aws::InitAPI(options): инициализирует библиотеку AWS SDK.

Aws::ShutdownAPI(options): завершает работу библиотеки AWS SDK, освобождая все ресурсы.

Таким образом, проведен анализ методов обеспечения безопасности облачных инфраструктур, а также разработан программный комплекс для оценки рисков безопасности на базе AWS.

Программный комплекс проверяет ключевые аспекты безопасности, такие как публичный доступ к S3 пакетам, наличие публичных IP у EC2 экземпляров и использование MFA у IAM пользователей. Эти проверки помогают идентифицировать потенциальные уязвимости и принимать меры для повышения уровня защиты [10, 11].

Был проведён анализ текущего состояния дел в области комплексной оценки рисков информационной безопасности объектов критической информационной инфраструктуры. Было выявлено, что современные облачные системы часто подвергаются различным видам атак и существует необходимость в разработке специализированных инструментов для их защиты.

Результаты работы показали, что использование методов интеллектуального анализа данных для оценки безопасности аспектов облачной инфраструктуры открывает новые возможности для защиты данных. Программный комплекс доказал свою эффективность в повышении безопасности учетных записей пользователей и может быть рекомендован для дальнейшего использования.

Библиографический список

1. Федеральный закон № 187–ФЗ «О безопасности критической ин–формационной инфраструктуры Российской Федерации» от 26.07.2017 [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/.

2. *Бобов, М. Н., Горячко, Д. Г.* Оценка рисков информационной безопасности с использованием стандарта CVSS 3.0. – 2017.

3. *Дойникова, Е. В., Чечулин, А. А., Котенко И. В.* Оценка защищенности компьютерных сетей на основе метрик CVSS // Информационно-управляющие системы. – 2017. – №. 6 (91).

4. *Doynikova, E., Kotenko, I.* CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection // 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP). IEEE. 2017. P. 346–353.

5. *Зегжда, Д. П.* Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. – Москва: Горячая Линия–Телеком, 2020. – 560 с.

6. *Нуруллаев, Р.Т.* Ограничение доступа к интернет-ресурсам как новый способ противодействия нарушениям авторских прав // Труды Института государства и права РАН. 2015. № 2 [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/ogranichenie–dostupa–k–internet–resursam–kak–novyy–sposob–protivodeystviya–narusheniyam–avtorskih–prav.

7. *Шамухамедов, Г. Х., Хыдыров, Н. К., Союнова, О. М.* Анализ современных методов хеширования // Science Time. – 2015. – №6 (18) [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/analiz–sovremennyh–metodov–heshirovaniya.

8. *Швыряев, П.С.* утечки конфиденциальных данных: главный враг внутри // Государственное управление. Электронный вестник. 2022. № 91. – URL: https://cyberleninka.ru/article/n/utechki–konfidentsialnyh–dannyh–glavnyy–vrag–vnutri.

9. *Штанько, И.А.* Быстродействующий алгоритм хеширования с высокой защищенностью от вскрытия // Радиоэлектроника и информатика. – 1998. – №3 (4). – URL: https://cyberle ninka.ru/article/n/bystrodeystvuyuschiy–algoritm–heshirovaniya–s–vysokoy–zaschischennostyu–ot–vskrytiya.

10. «Соленое» хеширование паролей // Интернет технологии.ру [Сайт]. – URL: https://www.garant.ru/products/ipo/prime/doc/71634878/.

11. Распоряжение Правительства России от 28 июля 2017 г. №1632-р [Электронный ресурс]. – URL: https://www.kaspersky.ru/resource–center/definitions/brute–force–attack.

12. Введение в цепи Маркова // Хабр [Сайт]. – URL: https://habr.com/ru/articles/455762/ (дата обращения: 12.03.2024).

13. Надлежащее хэширование паролей // securitylab [Сайт]. – URL: https://www.securitylab.ru/analytics/427930.php.