УДК 004.056

О.В. Литвинова[1], В.В. Михаэлис[1]

[1]Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

ЗНАЧИМОСТЬ ИНСТРУМЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ АДМИНИСТРИРОВАНИИ СЕРВЕРОВ БАЗ ДАННЫХ АВАПЕРЕВОЗОК

Аннотация. В современном мире информационных технологий обеспечение безопасности данных становится все более важным аспектом, особенно в сфере онлайн-бронирования путешествий и авиаперевозок. Статьи рассматривают различные аспекты информационной безопасности в контексте агентств по бронированию, включая механизмы аутентификации пользователей, шифрование данных, мониторинг системы и обновление программного обеспечения. Подчеркивается важность комплексного подхода к обеспечению информационной безопасности для защиты данных клиентов и обеспечения сохранности корпоративных систем.

Ключевые слова: информационная безопасность, администрирование серверов баз данных, угрозы безопасности данных, межсетевые атаки, управление доступом, шифрование данных, мониторинг системы.

O.V. Litvinova[1], V.V.Mikhaelis[1]

[1] Irkutsk State Transport University, Irkutsk, the Russian Federation

IMPORTANCE OF INFORMATION SECURITY TOOLS IN ADMINISTRATION OF AIR TRANSPORTATION DATABASE SERVERS

Abstract. In the modern world of information technology, data security is becoming an increasingly important aspect, especially in the field of online travel and air travel booking. The articles consider various aspects of information security in the context of booking agencies, including user authentication mechanisms, data encryption, system monitoring and software updates. The importance of an integrated approach to information security is emphasized to protect customer data and ensure the safety of corporate systems.

Keywords: information security, database server administration, data security threats, firewall attacks, access control, data encryption, system monitoring.

Введение

Администрирование серверов баз данных в современном мире информационных технологий представляет собой критически важный аспект, особенно в условиях нарастающих угроз безопасности данных. Современные технологии информационных систем обусловили широкое распространение серверов баз данных, которые стали неотъемлемыми для хранения и обработки данных организаций. Однако вместе с этим возросли и угрозы безопасности, ставящие под сомнение конфиденциальность, целостность и доступность данных. Понимание этих угроз и применение соответствующих средств информационной безопасности играют ключевую роль в обеспечении защиты данных и сохранности информационных систем [1].

Основные угрозы безопасности данных

В современном мире серверы баз данных подвержены различным угрозам безопасности, в числе которых выделяется несанкционированный доступ. Примером такой угрозы служит инцидент безопасности, произошедший в 2017 году с компанией Equifax, когда утечка данных о более чем 147 миллионах человек произошла из-за уязвимости в их веб-приложении. Другой серьезной угрозой являются внутренние угрозы, связанные с деятельностью даже доверенных сотрудников, как это было в компании Tesla в 2018 году.

Межсетевые атаки, такие как DDoS-атаки или инъекции SQL, также представляют значительную угрозу для серверов баз данных [2-3]. Примером такой атаки может служить инцидент безопасности с сервисом микроблогов Twitter в 2020 году, когда злоумышленники получили доступ к учетным записям высокопоставленных личностей.

Утечки данных, вызванные некорректной настройкой сервера или уязвимостями в программном обеспечении, также могут иметь серьезные последствия [4]. Примером такой утечки является инцидент безопасности с компанией Target в 2013 году, когда хакеры получили доступ к данным более чем 40 миллионов кредитных и дебетовых карт клиентов компании.

Важность серверов баз данных в информационных системах подчеркивает необходимость их защиты от угроз безопасности. Для обеспечения безопасности данных применяются разнообразные инструменты и методы информационной безопасности, включая аутентификацию, шифрование, мониторинг и другие [5].

Администрирование серверов баз данных (СУБД) является критически важным аспектом в сфере информационных технологий, особенно для агентств по бронированию авиабилетов, где хранятся и обрабатываются огромные объемы данных о клиентах, рейсах, бронированиях и финансовых операциях. В свете растущих угроз кибербезопасности администрирование серверов баз данных становится предметом повышенного внимания и требует эффективных инструментов информационной безопасности [6, 7].

Администрирование серверов баз данных в сфере авиаперевозок

В сфере авиаперевозок защита данных начинается с обеспечения правильной аутентификации пользователей и строгой авторизации доступа. В связи с чувствительностью данных о клиентах и платежах, использование сильных методов аутентификации, таких как многофакторная аутентификация, становится необходимостью. Авторизация должна быть тщательно настроена для разграничения прав доступа сотрудников к различным данным в базе. Например, сотрудники отдела продаж должны иметь доступ только к данным о бронированиях, в то время как финансовый отдел должен иметь доступ к финансовым операциям, но не к персональной информации клиентов [8].

Шифрование данных является основным механизмом обеспечения конфиденциальности информации на серверах баз данных. Для защиты конфиденциальных данных о клиентах и платежах, агентства по бронированию авиабилетов должны применять современные методы шифрования. Например, шифрование данных на уровне базы данных может предотвратить доступ к данным даже в случае компрометации самого сервера [9].

Регулярный мониторинг и ведение журналов событий играют важную роль в обеспечении безопасности серверов баз данных. Записи всех действий пользователей и

администраторов баз данных помогают оперативно обнаруживать аномальную активность и потенциальные угрозы безопасности. Системы мониторинга SIEM (Security Information and Event Management) могут анализировать большие объемы данных из различных источников и выявлять аномалии, указывающие на возможные инциденты безопасности.

Ограничение доступа к серверам баз данных из внешних сетей и защита их от внешних атак становится необходимостью для агентств по бронированию авиабилетов. Брандмауэры и другие сетевые механизмы безопасности могут фильтровать трафик, контролировать доступ и обнаруживать атаки на ранних стадиях.

Регулярное обновление программного обеспечения и установка патчей также являются важными мерами для устранения известных уязвимостей и снижения риска компрометации сервера баз данных. Агентства и компании должны следить за выходом обновлений и незамедлительно их устанавливать, чтобы обеспечить надежную защиту данных.

Наконец, обучение персонала по вопросам информационной безопасности играет важную роль в обеспечении безопасности серверов баз данных. Сотрудники должны быть ознакомлены с правилами безопасного обращения с данными, методами обнаружения и реагирования на инциденты безопасности, а также с последствиями нарушений правил безопасности.

Агентства по бронированию путешествий активно применяют ряд инструментов и методов для обеспечения информационной безопасности в системах онлайн-бронирования. Например, они реализуют многофакторную аутентификацию, требуя от пользователей не только пароль, но и дополнительный код, получаемый через мобильное устройство или электронную почту. Это подобно процессу, который многие пользователи видят при входе в банковские приложения, когда помимо пароля им необходимо ввести одноразовый код, полученный по SMS или через приложение аутентификации. Такой подход обеспечивает дополнительный уровень безопасности, предотвращая несанкционированный доступ даже в случае компрометации пароля.

Также агентства строго разграничивают права доступа пользователей в зависимости от их ролей. Например, администраторы имеют расширенные права доступа для управления системой и данными, в то время как обычные пользователи имеют ограниченные права доступа только к функциям бронирования. Это можно сравнить с системами управления правами доступа в корпоративных сетях, где различным пользователям предоставляются разные уровни доступа в зависимости от их ролей и обязанностей в организации [1].

Для обеспечения конфиденциальности информации агентства применяют шифрование данных. Например, при передаче данных между клиентом и сервером используется протокол SSL/TLS, который обеспечивает защиту от перехвата или изменения трафика третьими лицами. Этот протокол широко используется в интернет-банкинге и онлайн-платежах для защиты конфиденциальных данных пользователей. Кроме того, агентства применяют шифрование данных на уровне базы данных, что обеспечивает дополнительный уровень защиты от несанкционированного доступа к данным. Такой подход защищает информацию даже в случае компрометации сервера [6, 10].

Регулярный мониторинг системы и ведение журналов событий помогают оперативно обнаруживать и реагировать на потенциальные угрозы безопасности.

Например, системы мониторинга анализируют трафик и действия пользователей, выявляя аномальную активность, которая может указывать на попытки несанкционированного доступа или другие атаки. Журналы событий записывают все действия пользователей и администраторов, что позволяет проводить расследование и улучшать систему безопасности.

Для защиты от внешних атак агентства используют брандмауэры и другие сетевые механизмы безопасности. Например, брандмауэры контролируют и фильтруют трафик, ограничивая доступ к серверам только из доверенных источников. Это помогает предотвратить попытки атак извне, такие как DDoS-атаки или попытки взлома.

Регулярное обновление программного обеспечения и установка патчей также являются важной частью стратегии безопасности. Например, обновления исправляют известные уязвимости в системе и обеспечивают защиту от новых видов атак и методов взлома.

Администрирование сервера баз данных требует не только хорошего знания технических аспектов управления данными, но и глубокого понимания принципов информационной безопасности. Использование соответствующих инструментов информационной безопасности помогает минимизировать риск утечки, повреждения или несанкционированного доступа к данным. Каждый из предложенных инструментов имеет свои преимущества и недостатки, и их эффективное использование зависит от конкретных потребностей и характеристик инфраструктуры баз данных. В целом, интеграция комплексного подхода к обеспечению информационной безопасности позволяет повысить защищенность серверов баз данных и обеспечить сохранность ценных корпоративных данных.

Заключение

В результате проведенного анализа ключевых аспектов информационной безопасности в системах онлайн-бронирования путешествий делаются следующие предварительные выводы:

1. Разграничение прав пользователей. Правильное использование Active Directory повышает безопасность данных.
2. Внедрение многофакторной аутентификации и строгое управление доступом к данным позволяют агентствам обеспечить надежную защиту от несанкционированного доступа, даже при возможной утечке паролей.
3. Применение шифрования данных на различных уровнях, включая транспортный и уровень базы данных, обеспечивает конфиденциальность информации и защиту от компрометации данных в случае атак.
4. Регулярный мониторинг системы и ведение журналов событий позволяют оперативно обнаруживать и реагировать на потенциальные угрозы безопасности, улучшая общий уровень защиты данных.
5. Использование брандмауэров и других сетевых механизмов безопасности позволяет агентствам эффективно защищать свою инфраструктуру от внешних атак.
6. Регулярное обновление программного обеспечения и установка патчей являются важными мерами для устранения известных уязвимостей и обеспечения защиты от новых видов атак.

В целом, применение комплексного подхода к обеспечению информационной безопасности позволяет агентствам по бронированию путешествий обеспечить

надежную защиту данных своих клиентов и сохранить доверие пользователей в условиях растущих киберугроз.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Вартанян А.А. Угрозы и атаки сетевой безопасности. – URL: https://cyberleninka.ru/article/n/ugrozy-i-ataki-setevoy-bezopasnosti/viewer (дата обращения: 28.03.2024).

2. Аршинский Л.В., Жукова М.С. Интеллектуальные информационные системы и технологии: учебное пособие. – Иркутск: ИрГУПС, 2023. – 128 с.

3. Аршинский Л.В., Шурховецкий Г.Н. Особенности применения метода рассечения-разнесения для безопасного хранения данных во внешних хранилищах // Информационные технологии, 2021. №5. т. 27. С. 259-266

4. Намиот Д.Е. Введение в атаки отравлением на модели машинного обучения // International Journal of Open Information Technologies, 2023. – Т. 11, № 3. – С. 58-66.

5. Михаэлис, В. В. Проектирование модуля безопасности, обеспечивающего идентификацию личности при прохождении тестирования в системе электронного обучения / В. В. Михаэлис // Инженерный вестник Дона. – 2023. – № 3(99). – С. 98-106

6. Бабенко Г.В. Анализ современных угроз безопасности информации, возникающих при сетевом взаимодействии // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика, 2010. – № 2. – URL: https://cyberleninka.ru/article/n/analiz-sovremennyh-ugroz-bezopasnosti-informatsii-voznikayuschih-pri-setevom-vzaimodeystvii/viewer (дата обращения: 28.03.2024).

7. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. – Екатеринбург: Изд-во Урал. Ун-та, 2019. – 204 с.

8. Siddappa S. Statistical modeling approach to airline revenue management with overbooking // Ph.D. thesis – USA: The University of Texas at Arlington, 2006. – С. 25–44.

9. Михаэлис, В. В. Шифрование в среде MS Excel для безопасной передачи и хранения данных / В. В. Михаэлис, С. И. Михаэлис // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2023. – № 4-2. – С. 99-102.

10.Михаэлис, В. В. Защита беспроводных сетей / В. В. Михаэлис, С. И. Михаэлис // Информационные технологии и проблемы математического моделирования сложных систем. – 2015. – № 14. – С. 4-10.

REFERENCES

1. Vartanyan A. A. Threats and attacks to network security. - URL: https://cyberleninka.ru/article/n/ugrozy-i-ataki-setevoy-bezopasnosti/viewer (date of access: 03/28/2024).

2. Arshinsky L. V., Zhukova M. S. Intelligent information systems and technologies: a tutorial. - Irkutsk: IrGUPS, 2023. - 128 p.

3. Arshinsky L.V., Shurkhovetsky G.N. Features of the application of the dissection-diversification method for secure data storage in external storage // Information Technologies, 2021. No. 5. Vol. 27. Pp. 259-266. DOI: 10.17587/it.27.259-266

4. Namiot D.E. Introduction to poisoning attacks on machine learning models // International Journal of Open Information Technologies, 2023. - Vol. 11, No. 3. - Pp. 58-66.

5. Michaelis, V.V. Design of a security module that provides personal identification when passing testing in an e-learning system / V.V. Michaelis // Engineering Bulletin of the Don. - 2023. - No. 3 (99). - Pp. 98-106. – EDN RGZDFL

6. Babenko G.V. Analysis of modern threats to information security arising from network interaction // Bulletin of ASTU. Series: Management, computing equipment and informatics, 2010. – No. 2. – URL: https://cyberleninka.ru/article/n/analiz-sovremennyh-ugroz-bezopasnosti-informatsii-voznikayuschih-pri-setevom-vzaimodeystvii/viewer (date of access: 03/28/2024).

7. Vostretsova E.V. Fundamentals of information security: a textbook for university students. – Ekaterinburg: Publishing house of the Ural. University, 2019. – 204 p.

8. Siddappa S. Statistical modeling approach to airline revenue management with overbooking // Ph.D. thesis – USA: The University of Texas at Arlington, 2006. – P. 25–44.

9. Michaelis, V. V. Encryption in MS Excel for Secure Data Transfer and Storage / V. V. Michaelis, S. I. Michaelis // Modern Science: Current Problems of Theory and Practice. Series: Natural and Technical Sciences. – 2023. – No. 4-2. – P. 99-102.

10. Michaelis, V. V. Wireless Network Security / V. V. Michaelis, S. I. Michaelis // Information Technologies and Problems of Mathematical Modeling of Complex Systems. – 2015. – No. 14. – P. 4-10.

Информация об авторах

Михаэлис Владимир Вячеславович - к. п. н., доцент, доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e–mail: mihaelis_vv@irgups.ru

Литвинова Оксана Владимировна - магистрант кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e–mail: 12023115751@irgups.ru

Information about the authors

Vladimir Vyacheslavovich Mikhaelis - Ph.D., associate Professor of the Department «Information systems and information protection», Irkutsk State Transport University, Irkutsk, e–mail: mihaelis_vv@irgups.ru

Oksana Vladimirovna Litvinova - master student of the Department «Information Systems and Information Security», Irkutsk State Transport University, Irkutsk, e–mail: 12023115751@irgups.ru