УДК 004.056 **DOI: 10.34670/AR.2021.65.75.021**

Методы обеспечения информационной безопасности баз данных

Пахаев Хусейн Хасинович

Студент,
Чеченский государственный университет,
364024, Российская Федерация, Грозный, ул. А. Шерипова, 32;
e-mail: pakhaev01@gmail.com

Магомедов Ислам Арбиевич

Ассистент,
факультет информационных технологий,
Чеченский государственный университет,
364024, Российская Федерация, Грозный, ул. А. Шерипова, 32;
e-mail: ismwork@mail.ru

Аннотация

В статье рассматриваются основные уязвимости, существующие в области защиты подключения баз данных, и методы для устранения уязвимостей и обеспечения информационной безопасности баз данных. Отмечается, что многие организации пренебрегают правилами защиты информации и существует ряд способов получить несанкционированный доступ к конфиденциальной информации той или иной организации. С развитием методов хранения информации на сетевых ресурсах выросло количество утечек информации и несанкционированного доступа к этой информации. Сегодня ни один сервис не может предложить стопроцентную информационную безопасность. Все более широкое использование компьютерных технологий обработки и хранения информации заставляет компании усиливать защиту баз данных. Выстраивание эффективной системы безопасности баз данных требует оценки угроз с опорой на ценность информации и сложившуюся в сфере ее обращения практику преступного посягательства на данные.

Для цитирования в научных исследованиях

Пахаев Х.Х., Магомедов И.А. Методы обеспечения информационной безопасности баз данных // Экономика: вчера, сегодня, завтра. 2021. Том 11. № 6А. С. 200-204. DOI: 10.34670/AR.2021.65.75.021

Ключевые слова

Информационные технологии, защита информации, защита баз данных, методы обеспечения информационной безопасности.

Введение

Информационная безопасность представляет собой комплексную систему, все составляющие которой призваны не допустить утечки конфиденциальных сведений по техническим каналам, а также воспрепятствовать стороннему доступу к носителям информации. Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий. Методы обеспечения безопасности баз данных делятся на несколько разновидностей. В данной статье рассмотрим уязвимости защиты подключения, инструменты для обеспечения защиты подключения и парольные политики.

Уязвимости защиты подключения

Первое, на что нужно обращать внимание, когда речь заходит о безопасности баз данных, – это защита подключения. Есть ли у базы данных доступ через API или запросы идут напрямую к базе данных? API – это набор программных функций, методов, классов и т.д. для взаимодействия других программ через данные методы с другой программой. API делится на три типа: RPC (Remote Procedure Call) – удаленные вызовы процедур; SOAP (Simple Object Access Protocol) – простой протокол доступа к данным; REST (Representational State Transfer) – для передачи состояний представления.

Можно отметить следующие плюсы предоставления доступа к базе данных через API: запросы к базе не идут напрямую; у разработчиков системы много возможностей расширять систему; одна и та же функция API может быть представлена и реализована в разных приложениях по-разному, но она будет знакома всем пользователям [Абдулов, 2005].

Минусами предоставления доступа к базе данных через API являются следующие особенности: если будут внесены изменения в основной сервис, данные изменения в API не всегда появляются сразу; API предназначен для общего доступа.

Инструменты обеспечения защиты подключения

Функциями класса Database filewall являются:

1. Защита от направленных внутренних и внешних атак на серверы баз данных (или же защита от DDOS – один из самых распространенных вариантов получения информации). Цель данной атаки – вывести из строя вычислительную систему. Средства для атаки – «компьютеры-зомби», которые выполняют одну простую роль: посылают бесконечные запросы на сервер, пока тот не упадет. Для того, чтобы в современном мире достичь успеха в DDoS, необходимо очень много таких «зомби-компьютеров», так как вычислительные мощности в наше время весьма хорошие, чтобы не падать при +- 50 вычислительных машин для атаки.

2. Контроль и мониторинг за всеми запросами от пользователей и защита от несанкционированного доступа к базе данных. Данный способ помогает отслеживать все запросы от пользователей. Скажем, если сервис ведет себя странно, можно отследить все манипуляции с базой данных. Также возможна блокировка прав и оповещение администратора базы данных при подозрительной активности пользователей [Адамчук, 2009].

Среди итогов применения Database firewall можно назвать снижение рисков потери конфиденциальной информации, уменьшение рисков вывода из строя сервера с базами данных, увеличение информационной безопасности баз данных, увеличение непрерывной работы

серверов организации. Данный программный комплекс соответствует требованиям законодательства Российской Федерации и международного законодательства.

Парольные политики

Первое и самое главное в безопасности – задавать сложные регистрационные данные для доступа к базам данных. Порою этим правилом пренебрегают многие пользователи и системные администраторы, ссылаясь на то, что их организации не коснется угроза слива информации [Бирюков, 2018]. Пароли лучше менять через определенный промежуток времени. Хороший пароль должен соответствовать следующим правилам: минимум 8 символов; минимум одна прописная буква; минимум одна цифра; один символ и более; латинские буквы.

Должны исключаться пароли со следующими данными: ФИО; дата рождения; номер мобильного телефона; домашний адрес; рабочий адрес; какая-либо личная информация ближайших родственников; одинаковый логин и пароль для доступа к информации.

Знание контекста сессии необходимой информацией необходимо для того, чтобы администраторы сети имели доступ к информации, в которой содержится описание того, что делает определенный пользователь: какие запросы от него идут к базе данных, какой результат будет возвращен базой данных по запросу пользователя. Необходимо настроить SSL, если нет сетевого разграничения СУБД от пользователей; если она не в отдельном VLAN (виртуальная компьютерная сеть), нужно обязательно защищать канал передачи информации между пользователями и СУБД.

Заключение

Таким образом, информационная безопасность – это защищенность информации от случайных или преднамеренных воздействий, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры. С развитием хранения информации на сетевых ресурсах выросло количество утечек информации и несанкционированного доступа к ней. К сожалению, в наше время ни один сервис не может предложить стопроцентную информационную безопасность. С помощью рассмотренных нами методов можно повысить уровень информационной безопасности баз данных.

Библиография

1. Абдулов А.Н. Контуры информационного общества. М., 2005. 162 с.
2. Адамчук В.В. Экономика труда. М.: Инфра-М, 2009. 415 с.
3. Бегишев И.Р. Правовые аспекты безопасности информационного общества // Информационное общество. 2011. № 4. С. 54-59.
4. Бирюков А.А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2018. 474 с.
5. Завельский М.Г. Экономика и социология труда. М.: Норма, 2011. 281 с.
6. Магомадов В.С. Исследование роли новейших информационных технологий в экономике совместного использования // ФГУ SCIENCE. 2019. С. 130-134.
7. Магомедов И.А., Мурзаев Х.А., Багов А.М. Роль цифровых технологий в экономическом развитии. IOP Publishing Limited, 2019.
8. Майкл Х., Дэвид. Л, Джон. В. 19 смертных грехов, угрожающих безопасности программ. М.: ДМК Пресс, 2016. 228 с.
9. Менциев А.У., Чебиева Х.С. Современные угрозы безопасности в сети Интернет и контрмеры (обзор) // Инженерный вестник Дона. 2019. № 3 (54). С. 16-23.
10. Родичев Ю. Нормативная база и стандарты в области информационной безопасности. СПб.: Питер, 2017. 256 с.

Methods for ensuring information security of databases

Khusein Kh. Pakhaev

Student,
Chechen State University,
364024, 32 Sheripova str., Grozny, Russian Federation;
e-mail: pakhaev01@gmail.com

Islam A. Magomedov

Assistant,
Faculty of information technologies,
Chechen State University,
364024, 32 Sheripova str., Grozny, Russian Federation;
e-mail: ismwork@mail.ru

Abstract

The article discusses the main vulnerabilities of database connection protection and methods for eliminating vulnerabilities and ensuring information security of databases. It is noted that many organizations neglect the rules of information protection and there are a number of ways to gain unauthorized access to confidential information of a particular organization. With the development of information storage on network resources, the number of information leaks and unauthorized access to this information has increased. Today, no service can offer one hundred percent information security. The increasing use of computer technologies for processing and storing information forces companies to strengthen the protection of databases. It is noted that the first and foremost security is to specify complex credentials for accessing databases. Sometimes, this rule is neglected by many users and system administrators, referring to the fact that their organization will not be affected by the threat of information leakage. Building an effective database security system will require an assessment of threats based on the value of information and the practice of criminal encroachment on data that has developed in the sphere of its circulation.

For citation

Pakhaev Kh.Kh., Magomedov I.A. (2021) Metody obespecheniya informatsionnoi bezopasnosti baz dannykh [Methods for ensuring information security of databases]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 11 (6A), pp. 200-204. DOI: 10.34670/AR.2021.65.75.021

Keywords

Information technology, information security, database protection, information security methods.

References

1. Abdulov A.N. (2005) *Kontury informatsionnogo obshchestva* [The contours of the information society]. Moscow.
2. Adamchuk V.V. (2009) *Ekonomika truda* [Labor economics]. Moscow: Infra-M Publ.

3. Begishev I.R. (2011) Pravovye aspekty bezopasnosti informatsionnogo obshchestva [Legal aspects of information society security]// *Informatsionnoe obshchestvo* [Information society], 4, pp. 54-59.
4. Biryukov A.A. (2018) *Informatsionnaya bezopasnost': zashchita i napadenie* [Information security: defense and attack]. Moscow: DMK Press Publ.
5. Magomadov V.S. (2019) Issledovanie roli noveishikh informatsionnykh tekh-nologii v ekonomike sovmestnogo ispol'zovaniya [Investigation of the role of the latest information technologies in the sharing economy]. *FGU SCIENCE*, pp. 130-134.
6. Magomedov I.A., Murzaev Kh.A., Bagov A.M. (2019) *Rol' tsifrovykh tekhnolo-gii v ekonomicheskom razvitii* [The role of digital technologies in economic development]. IOP Publishing Limited Publ.
7. Maikl X., Devid. L, Dzhon. V. (2016) *19 smertnykh grekhov, ugrozhayushchikh bezopasnosti program* [19 deadly sins that threaten the security of programs]. Moscow: DMK Press Publ.
8. Mentsiev A.U., Chebieva Kh.S. (2019) Sovremennye ugrozy bezopasnosti v seti Internet i kontrmery (obzor) [Modern security threats on the Internet and countermeasures (overview)]. *Inzhenernyi vestnik Dona* [Engineering Bulletin of the Don], 3 (54), pp. 16-23.
9. Rodichev Yu. (2017) *Normativnaya baza i standarty v oblasti informatsionnoi bezopasnosti* [Normative base and standards in the field of information security]. Saint Petersburg: Piter Publ.
10. Zavel'skii M.G. (2011) *Ekonomika i sotsiologiya* truda [Economics and sociology of labor]. Moscow: Norma Publ.