УДК 33 **DOI: 10.34670/AR.2023.40.12.047**

Инфраструктура информационной безопасности компании

Филатова Татьяна Александровна

Доктор экономических наук, доцент, профессор,
Факультет бизнеса, таможенного дела и экономической безопасности,
Санкт-Петербургский государственный экономический университет,
191023, Российская Федерация, Санкт-Петербург,
наб. канала Грибоедова, 30-32, А;
e-mail: werck@rambler.ru

Шумский Эльдар Олегович

Студент,
Факультет бизнеса, таможенного дела и экономической безопасности,
Санкт-Петербургский государственный экономический университет,
191023, Российская Федерация, Санкт-Петербург,
наб. канала Грибоедова, 30-32, А;
e-mail: shumskiyeldar977@yandex.ru

Лямин Егор Игоревич

Студент,
Факультет бизнеса, таможенного дела и экономической безопасности,
Санкт-Петербургский государственный экономический университет,
191023, Российская Федерация, Санкт-Петербург,
наб. канала Грибоедова, 30-32, А;
e-mail: egor.lyamin32@yandex.ru

Аннотация

В современном мире информационная безопасность обладает жизненно важным статусом для любой компании. На любом предприятии всегда существуют риск утечки или недобросовестной передачи данных злоумышленникам работниками организации, которые предпочитают рисковать ради какой-то скрытой цели. Инфраструктура любой организации включает в себя огромные объемы данных, которые раскрывают финансовое положение организации и позволяют злоумышленникам или конкурентам продумывать стратегию влияния на организацию различными способами. Эти данные хранятся и управляются базами данных, которые являются одной из основных целей злоумышленников. Целью исследования безопасности базы данных является предупреждение и предотвращение незаконного использования или уничтожения базы данных на исследуемом предприятии. Утечка финансовых или личных данных клиентов и сотрудников имеет негативное влияние на экономические, коммерческие и репутационные показатели любой организации, так-как влекут за собой штрафные санкции от государства, потерю клиентской базы и поставок от поставщиков материалов. Существует несколько

типов методов, применяемых для повышения уровня безопасности базы данных. Технологии безопасности, которые помогают защитить от злоупотреблений со стороны внешних хакеров и внутренних привилегированных пользователей, включают маскировку данных, шифрование данных, управление идентификацией, размагничивание, брандмауэры, аудит и обязательный контроль доступа. В данной статье будут даны ответы на следующие вопросы: что из себя представляет ИТ-безопасность и какова методология ее работы, какие методы незаконного проникновения в базы данных существуют, как защитить базы данных от незаконного проникновения.

Для цитирования в научных исследованиях

Филатова Т.А., Шумский Э.О., Лямин Е.И. Инфраструктура информационной безопасности компании // Экономика: вчера, сегодня, завтра. 2023. Том 13. № 4А. С. 382-389. DOI: 10.34670/AR.2023.40.12.047

Ключевые слова

Информационная безопасность, базы данных, защита данных, защита базы данных.

Введение

Безопасность в IT — это набор средств, реализуемых для снижения уязвимости компьютерных систем к случайным или преднамеренным угрозам, с которыми они могут столкнуться. Другими словами, это набор методов, которые гарантируют, что ресурсы информационной системы (аппаратное или программное обеспечение) организации используются только в том контексте, в котором они запланированы.

Основные требования ИТ-безопасности сводятся к обеспечению:

– Доступности: системная информация всегда должна быть доступна уполномоченным лицам.
– Конфиденциальности: информация о системе следует распространять только среди уполномоченных лиц.
– Целостности: информация о системе должна изменяться только уполномоченными лицами.

Основная часть

Методология управления IT безопасности состоит из трех элементов: анализ рисков, установления политики безопасности, внедрения методом обеспечения информационной безопасности. Каждой компании целесообразно оценивать риски, то есть измерять их в соответствии с вероятностью их появления и их возможными последствиями. После проведения анализа рисков вводится в действие политика безопасности. Она позволяет определить рамки использования ресурсов информационной системы, разработать методы обеспечения безопасности и обучения сотрудников. Далее непосредственно вводятся разработанные методы, которым относятся: проведение аудита уязвимостей и тестов на проникновение; защита данных с помощью шифрования и контроля доступа; мониторинг событий; обучение и инструктаж сотрудников, имеющих доступ к информации.

Система управления базами данных упорядочивает и предоставляет данные пользователям,

предотвращая несанкционированный доступ и модификацию данных.

В целом, основной риск, связанный с любой атакой, зависит от трех факторов: угроз, уязвимостей и воздействий.

Основными угрозами безопасности в базах данных являются:

1. SQL-инъекция.
2. Чрезмерное злоупотребление привилегиями.
3. Злоупотребление законными привилегиями.
4. Повышение привилегий.
5. Использование уязвимостей в неправильно настроенных базах данных.
6. Отказ в обслуживании.

При атаке SQL-инъекцией злоумышленник обычно вставляет (или «внедряет») несанкционированную информацию базы данных в уязвимую строку данных SQL. Как правило, затронутые строки данных включают хранимые процедуры и параметры ввода для веб-приложений. Эта введенная информация отправляется в базу данных, где она выполняется. Используя SQL-инъекцию, злоумышленники могут получить неограниченный доступ ко всей базе данных.

Привилегии доступа к базе данных, которые не соответствуют профессиональным функциями сотрудников, приводят к тому, что работники могут злоупотреблять этим. Пользователи баз данных могут в итоге получить чрезмерные привилегии по той простой причине, что в большинстве случаев у администраторов баз данных нет времени устанавливать или обновлять механизмы доступа для отдельного пользователя. Как в результате группы пользователей могут иметь общие привилегии доступа по умолчанию, которые намного превышают требования их конкретной функции. Данный факт может привести либо к потере конфиденциальности или целостности данных.

Пользователи также могут злоупотреблять законными правами доступа к базе данных в несанкционированных целях, что прежде всего сопряжено с созданием резервных копий. Данный факт сопряжен с двумя категориями сотрудников. Первые, используют уровень своего доступа наряду с некоторыми уязвимостями системы, что позволяет извлечь или изменить данные. Вторые, могут использовать копии по неосторожности для законных целей, однако такие данные могут быть украдены с носителя информации, например, если они хранятся на личном ноутбуке сотрудника, путём внедрения вируса или кражи.

Злоумышленники могут воспользоваться уязвимостями программного обеспечения платформы баз данных, чтобы превратить права доступа обычного пользователя в права администратора. В большинстве случаев все уязвимости можно обнаружить в хранимых процедурах, встроенных функциях, реализациях протоколов или даже в данных SQL. Например, разработчик программного обеспечения, работающий в финансовом учреждении, может воспользоваться уязвимой функцией, чтобы получить права администратора доступа к базе данных.

Базы данных могут быть неправильно настроены, имея учетные записи и конфигурации, установленные по умолчанию. В то время как поставщики разрабатывают пакеты исправлений с учетом конкретной уязвимости, корпоративные базы данных остаются доступными для свободного использования. Данный факт позволяет злоумышленнику получить доступ к базе данных, используя учетную запись по умолчанию, идентифицируя себя как законного пользователя.

Отказ в обслуживании или DOS-атака (Denial of Service) — это общая категория атак, которая лишает определенных пользователей доступа к сетевым приложениям. Условия отказа в обслуживании могут быть созданы с помощью многих методов, многие из которых связаны с вышеупомянутыми уязвимостями. Например, отказ в обслуживании может быть достигнут путем использования уязвимости платформы базы данных для отключения сервера. Другие распространенные методы отказа в обслуживании включают повреждение данных, перегрузку сети и нагрузку на ресурсы сервера (память, центральный процессор и т.д.). Отказ в обслуживании также может быть связан с заражением компьютерным червем.

Многие компании стремятся должным образом вести инвентаризацию всех своих баз данных. Новые базы данных могут создаваться без ведома службы безопасности, и конфиденциальные данные, скопированные в эти базы данных, могут быть раскрыты, если не будут применены необходимые средства контроля. Эти «скрытые» базы данных могут содержать потенциально конфиденциальные данные, такие как детали транзакций, а также контактную информацию клиентов и сотрудников. Однако, если сотрудники службы безопасности данных не знают содержимого этих баз данных, трудно гарантировать, что были применены необходимые средства контроля. Будь то намеренно или непреднамеренно сотрудники или хакеры могут затем незаконно получить доступ к конфиденциальным данным. Примером могут служить старые базы данных, которые были забыты и оставлены вне области видимости.

Перейдем к мерам обеспечения безопасности при реализации обозначенных выше угроз для баз данных.

1. Предотвращение SQL-инъекции.

Всего существует два метода для эффективной борьбы с SQL-инъекцией:

1.1. Технология предотвращения вторжений. Данная технология способна идентифицировать наиболее уязвимые данные для SQL-инъекции. Как правило, IP-адреса сами по себе ненадежны, поскольку SQL-инъекция дает много ложных срабатываний. Сотрудники службы безопасности, которые полагаются исключительно на технологию предотвращения вторжений, будут засыпаны предупреждениями о «возможных» SQL-инъекциях. Работая в одиночку, данная технология является не самой эффективной мерой защиты и её следует использовать в паре с запрашиваемым контролем доступа.

1.2. Запрашиваемый контроль доступа и корреляция событий.

В случае возникновения реальной SQL-инъекции злоумышленникам потребуется получить доступ от системы. Данный факт позволит очень точно идентифицировать вполне реальную атаку. Сигнатура SQL-инъекции и другой тип нарушения вряд ли появятся в одном и том же запросе во время обычной операции.

2. Предотвращение чрезмерного злоупотребления привилегиями.

Самое простое и логичное решение данного типа угрозы является устранение чрезмерных прав у пользователя. Для этого необходимо проводить анализ избыточности прав у пользователей, то есть таких прав, которые не являются для него необходимыми для выполнения своих функций и задач. Выполнение такой задачи вручную достаточно трудоемкий и сложный процесс поэтому его следует автоматизировать для сокращения затрачиваемых ресурсов и времени [Серебрякова, 2021].

Для более успешного предотвращение чрезмерного злоупотребления привилегиями необходимо средство контроля доступа к запросам. Контроль доступа к запросам относится к

механизму, который ограничивает привилегии доступа к базам данных до минимума. Степень детализации контроля доступа к данным должна быть расширена от простой таблицы к определенным строкам и столбцам в пределах одной и той же таблицы. Контроль доступа к запросам полезен не только для обнаружения чрезмерного злоупотребления привилегиями сотрудниками-злоумышленниками, но и для предотвращения большинства угроз, описанных ранее.

3. Предотвращение злоупотребления законными привилегиями.

Легитимным решение для данного вида угроз является контроль доступа к базе данных. Путем применения правила управления для клиентских приложений время и местоположение запроса на доступ и т.д., можно идентифицировать пользователей, которые подозрительным образом используют законные права доступа к базе данных.

4. Предотвращение повышения привилегий.

Злоупотребления повышением привилегий можно предотвратить, объединив традиционную систему предотвращения вторжений и контроль доступа по запросу, описанный ранее. Система предотвращения вторжений проверяет трафик базы данных для выявления шаблонов, соответствующих существующим уязвимостям. Система предотвращения вторжений может быть использована чтобы проверить, используется ли запрос доступа к базе данных с уязвимой функцией в то время, как управление доступом к запросу определяет, соответствует ли запрос типичному профилю пользователя. Если один запрос указывает на доступ к уязвимой функции или необычному профилю пользователя, то, безусловно, предпринимается попытка атаки.

5. Предотвращение использования уязвимостей в неправильно настроенных базах данных.

Чтобы ограничить риск возникновения угроз, связанных с неисправленными и уязвимыми базами данных, необходимо сначала оценить состояние безопасности баз данных и исправить любые выявленные уязвимости и пробелы в безопасности. Компаниям следует периодически проверять базы данных на наличие любых уязвимостей и исправлений. Оценки конфигурации должны обеспечивать четкий обзор текущего состояния конфигурации систем передачи данных. Эти оценки также должны выявлять базы данных, которые не соответствуют определенным правилам конфигурации. Любые отсутствующие патчи безопасности должны быть развернуты как можно скорее. Если уязвимость обнаружена, когда исправление еще не доступно или потому, что оно еще не было запущено поставщиком или потому, что оно еще не было развернуто, необходимо определить виртуальное исправление. Такое решение блокирует попытки воспользоваться этими уязвимостями. Уменьшение окна экспозиции достигается за счет применения виртуального патча. Это поможет защитить базу данных от попыток эксплойта до тех пор, пока не будет развернуто исправление.

6. Предотвращение отказа в обслуживании.

Предотвращение отказа в обслуживании требует защиты на нескольких уровнях. В данной статье рассматриваются специфические меры защиты для баз данных и сети. В данном случае рекомендуется развертывание управляемого потока подключения, по технологии предотвращения вторжений, а также следует использовать приложения для контроля доступа и времени отклика управления. Удалив нежелательные функции и настроив только то, что необходимо для базы данных, отказ в обслуживании можно в некоторой степени предотвратить. Ограничение ресурсов — это превентивная мера, которая может затруднить атаку злоумышленников на систему. Патчи безопасности необходимо применять на регулярной

основе, и администраторы должны запускать отчет о безопасности, чтобы постоянно проверять уязвимости системы безопасности.

Заключение

Для защиты от информационных атак баз данных организациям необходимо сосредоточить своё внимание на наиболее критических угрозах. Сталкиваясь с угрозами, компании должны соответствовать требованиям реагирования и ограничения рисков, предъявляемым к наиболее строго регулируемым отраслям. Следует отметить, что пренебрежение безопасностью очень часто приводит к критическим для организации последствиям. Действительно, повсеместное распространение ИТ в компаниях подразумевает, что вся конфиденциальная информация содержится в базах данных или, по крайней мере, на сервере или компьютере, который подключён к сети, что делает их потенциально уязвимыми.

Исследования, как правило, доказывают, что в ближайшем будущем попытки атак будут становиться все более распространенными, и поэтому организации должны помнить о важности проведения, в дополнение ко всем техническим мерам, профилактики для пользователей, особенно тех, кто привлечен к обработке конфиденциальных данных.

Библиография

1. Алимжанова, Ж.М. Защита и безопасность базы данных / Ж.М. Алимжанова, А.Б. Балтабекова, А.Д. Турдалы // Актуальные научные исследования в современном мире. – 2019. – № 12-4 (56). – С. 61-64. – ISSN 2524-0986.
2. Власова, О.А. Защита и безопасность базы данных / О.А. Власова, А.С. Васильева // Решетневские чтения. – 2017. – № 2. – С. 317-318. – ISSN 1990-7702.
3. Кошелев, А.Д. Обеспечение информационной безопасности предприятия в условиях массовой цифровизации / А.Д. Кошелев // Экономика: Вчера, Сегодня, Завтра. – 2021. – Т. 11, № 10-1. – С. 287-295. – ISSN 2222-9167.
4. Красочкин, С.Г. Информационная безопасность баз данных / С.Г. Красочкин // Международный журнал гуманитарных и естественных наук. – 2022. – № 7-1 (70). – С. 89-95. – ISSN 2500-1000.
5. ПАХАЕВ, Х.Х. Методы обеспечения информационной безопасности баз данных / Х.Х. Пахаев, И.А. Магомедов // Экономика: Вчера, Сегодня, Завтра. – 2021. – Т. 11, № 6-1. – С. 200-204. – ISSN 2222-9167.
6. Серебрякова, Т.А. Актуальные вопросы защиты информации в системах управления базами данных / Т.А. Серебрякова, Н.И. Щепилова // вопросы устойчивого развития общества. – 2021. – № 3. – С. 45-51.
7. Bertino, Elisa, and Ravi Sandhu. "Database security-concepts, approaches, and challenges." IEEE Transactions on Dependable and secure computing 1 (2005): 2-19.
8. Burtescu, Emil. "Database security-attacks and control methods." journal of applied quantitative methods 4.4 (2009): 449-454.
9. Malik, Mubina, and Trisha Patel. "Database security attacks and control methods." International Journal of Information 6.1/2 (2016): 175-183.
10. Monali Sachin Kawalkar, Dr. P. K. Butey "An Approach for Detecting and Preventing SQL Injection and Cross Site Scripting Attacks using Query sanitization with regular expression". International Journal of Computer Trends and Technology (IJCTT) V49(4):237-245, July 2017. ISSN:2231-2803.
11. Murray, Meg C. "Database security: What students need to know." Journal of information technology education: Innovations in practice 9 (2010): IIP-61.
12. Shivnandan Singh, Rakesh Kumar Rai, A Review Report on Security Threats on Database, International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014.
13. Shulman, Amichai, and C. T. O. Co-founder. "Top ten database security threats." How to Mitigate the Most Significant Database Vulnerabilities (2006).
14. Simanta Shekhar Sarmah, Data Migration, Science and Technology, Vol. 8 No. 1, 2018, pp. 1-10. doi: 10.5923/j.scit.20180801.01.
15. Sourav Mukherjee "Popular SQL Server Database Encryption Choices" International Journal of Engineering Trends and Technology 66.1 (2018): 14-19.

Information protection and information security

Tat'yana A. Filatova

Doctor of Economics, Professor,
Faculty of Business, Customs and Economic Security,
Saint Petersburg State University of Economics,
191023, A, 30-32, Kanala Griboedoba emb.,
Saint Petersburg, Russian Federation;
e-mail: werck@rambler.ru

El'dar O. Shumskii

Student,
Faculty of Business, Customs and Economic Security,
Saint Petersburg State University of Economics,
191023, A, 30-32, Kanala Griboedoba emb.,
Saint Petersburg, Russian Federation;
e-mail: shumskiyeldar977@yandex.ru

Egor I. Lyamin

Student,
Faculty of Business, Customs and Economic Security,
Saint Petersburg State University of Economics,
191023, A, 30-32, Kanala Griboedoba emb.,
Saint Petersburg, Russian Federation;
e-mail: egor.lyamin32@yandex.ru

Abstract

In the modern world, information security has a vital status for any company. In any company, there is always a risk of leakage or unfair transfer of data to attackers by employees of the organization who prefer to take risks for some hidden purpose. The infrastructure of any organization includes huge amounts of data that reveal the financial situation of the organization and allow attackers or competitors to think through a strategy of influencing the organization in various ways. This data is stored and managed by databases, which are one of the main targets of attackers. The purpose of the database security study is to prevent and prevent the illegal use or destruction of the database at the enterprise under study. Leakage of financial or personal data of clients and employees has a negative impact on the economic, commercial and reputational indicators of any organization, as they entail penalties from the state, loss of customer base and supplies from suppliers of materials. Security technologies that help protect against misuse by external hackers and internal privileged users include Data Masking, Data Encryption, Identity Management, Degaussing, Firewalls, Auditing, and Mandatory Access Controls. This article will answer the following questions: What is IT security and what is the methodology of its work, what methods of illegal penetration into databases exist and how to protect databases from illegal intrusion.

For citation

Filatova T.A., Shumskii E.O., Lyamin E.I. (2023) Infrastruktura informatsionnoi bezopasnosti kompanii [Information protection and information security]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 13 (4A), pp. 382-389. DOI: 10.34670/AR.2023.40.12.047

Keywords

Information security, databases, data protection, database protection.

References

1. Alimzhanova, Zh.M. Protection and security of the database / Zh.M. Alimzhanova, A.B. Baltabekova, A.D. Turdaly // Actual scientific research in the modern world. – 2019. – № 12-4 (56). – Pp. 61-64. – ISSN 2524-0986.
2. Vlasova, O.A. Database protection and security / O.A. Vlasova, A.S. Vasilyeva // Reshetnev readings. – 2017. – No. 2. – PP. 317-318. – ISSN 1990-7702.
3. Koshelev, A.D. Ensuring information security of the enterprise in the conditions of mass digitalization / A.D. Koshelev // Economy: Yesterday, Today, Tomorrow. – 2021. – VOL. 11, No. 10-1. – pp. 287-295. – ISSN 2222-9167.
4. Krasochkin, S.G. Information security of databases / S.G. Krasochkin // International Journal of Humanities and Natural Sciences. – 2022. – № 7-1 (70). – Pp. 89-95. – ISSN 2500-1000.
5. PAKHAEV, H.H. Methods of ensuring information security of databases / H.H. Pakhaev, I.A. Magomedov // Economy: Yesterday, Today, Tomorrow. – 2021. – VOL. 11, No. 6-1. – PP. 200-204. – ISSN 2222-9167.
6. Serebryakova, T.A. Actual issues of information protection in database management systems / T.A. Serebryakova, N.I. Shchepilova // Issues of sustainable development of society. – 2021. – No. 3. – pp. 45-51.
7. Bertino, Eliza and Ravi Sandhu. "Database security - concepts, approaches and problems". IEEE Transactions on Secure and Secure Computing 1 (2005):2-19.
8. Burtescu, Emil. "Database security - attacks and control methods". Journal of Applied Quantitative Methods 4.4 (2009):449-454.
9. Malik, Mubina and Trisha Patel. "Attacks on database security and control methods". International Information Journal 6.1/2 (2016):175-183.
10. Monali Sachin Kavalkar, Dr. P. K. Butey "An approach to detecting and preventing SQL injections and cross-site scripting attacks using query cleanup using regular expressions". International Journal of Computer Trends and Technologies (IJCTT) V49(4):237-245, July 2017 ISSN:2231-2803.
11. Murray, Meg S. "Database Security: What Students need to know." Journal of Information Technology Education: Innovations in Practice 9 (2010): IIP-61.
12. Shivnandan Singh, Rakesh Kumar Rai, Overview Report on Database Security Threats, International Journal of Computer Science and Information Technology, Volume 5(3), 2014.
13. Shulman, Amichai and co-founder of C. T. O. "The ten main threats to database security." How to eliminate the most significant database vulnerabilities (2006).
14. Simanta Shekhar Sarma, Data Migration, Science and Technology, Volume 1. 8 No. 1, 2018, pp. 1-10. doi:10.5923/j.scit.20180801.01.
15. Surav Mukherjee "Popular SQL Server database Encryption options" International Journal of Engineering trends and technologies 66.1 (2018): 14-19.