Поляков А.А. Скрытые риски массовых обновлений данных: как избежать потери и утечки информации // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 12(50) с. 12–15

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.8

СКРЫТЫЕ РИСКИ МАССОВЫХ ОБНОВЛЕНИЙ ДАННЫХ: КАК ИЗБЕЖАТЬ ПОТЕРИ И УТЕЧКИ ИНФОРМАЦИИ

Поляков А.А.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: artpol2001@gmail.com

Массовые обновления данных играют важную роль в поддержании актуальности информации в крупных компаниях и организациях. Однако такие процессы могут сопровождаться рисками, связанными с потерей данных, нарушением целостности и утечками информации. В статье рассматриваются основные скрытые угрозы, возникающие при массовых обновлениях данных, а также предлагаются методы защиты, такие как управление правами доступа, резервное копирование и проверка целостности данных, чтобы минимизировать риски.

Ключевые слова: Массовое обновление данных, утечка информации, потеря данных, безопасность, резервное копирование, управление доступом, целостность данных.

HIDDEN RISKS OF MASS DATA UPDATES: HOW TO PREVENT DATA LOSS AND LEAKS

Polyakov A.A.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: artpol2001@gmail.com

Mass data updates are crucial for keeping information current in large companies and organizations. However, these processes can carry risks, such as data loss, integrity violations, and information leaks. The article examines the main hidden threats associated with mass data updates and offers protection methods, including access management, data backup, and integrity checks, to mitigate risks.

Keywords: mass data updates, data leakage, data loss, security, backup, access management, data integrity.

Введение

В эпоху цифровой трансформации массовые обновления данных стали необходимостью для организаций, стремящихся поддерживать актуальность и точность информации. Эти процессы, затрагивающие огромные объёмы данных, часто включают модификацию, удаление или добавление записей, что помогает компаниям оставаться конкурентоспособными и соответствовать постоянно меняющимся бизнес-требованиям. Однако масштабные изменения данных нередко сопряжены с рисками, которые могут привести к нарушению конфиденциальности, потере данных или их повреждению.

Риски, возникающие при массовых обновлениях, зачастую остаются незамеченными, особенно когда процесс плохо управляется или недостаточно защищён. Эти угрозы могут быть связаны с несанкционированным доступом, ошибками персонала или техническими

сбоями. Без соответствующих мер безопасности последствия могут быть серьёзными: от утраты критически важной информации до утечек, способных нанести значительный вред репутации компании. Введение в процесс обновления надёжных методов управления, таких как контроль доступа, автоматическое резервное копирование и регулярные проверки целостности, поможет снизить риск потерь и утечек данных, что становится всё более актуальным в условиях возросших требований к безопасности.

Скрытые риски массовых обновлений данных

Массовое обновление данных — это процесс, который требует тщательной координации и надёжного управления, поскольку даже минимальная ошибка может привести к серьёзным последствиям. Например, если на этапе обновления будет нарушена целостность данных, это способно негативно отразиться на работе всех зависимых систем. В случае массовых обновлений в базе данных ошибка в одной записи может распространиться на тысячи других, вызывая проблемы с обработкой транзакций, выводом отчётности и даже влияя на аналитические данные, что, в свою очередь, может привести к принятию ошибочных бизнес-решений[1].

Одна из серьёзных угроз при массовых обновлениях — это риск потери данных. Потеря информации может произойти как из-за случайных ошибок, так и из-за недосмотра сотрудников, а также из-за технических проблем, таких как сбои в работе серверов или сетевые неполадки. В случае отсутствия актуальных резервных копий восстановление данных может стать крайне трудоёмким процессом или даже невозможным. Чтобы избежать подобных проблем, компании должны использовать продуманные стратегии резервного копирования, включая создание дублирующих копий данных перед началом массового обновления. Эти резервные копии необходимо хранить в надёжном месте и периодически проверять на соответствие актуальному состоянию данных[2].

Другой важный аспект защиты данных при массовых обновлениях — это управление доступом. Не все сотрудники должны иметь возможность изменять или удалять данные, и ограничение прав доступа в зависимости от должностных обязанностей является важным шагом для предотвращения несанкционированного вмешательства. Использование ролевой модели управления доступом помогает контролировать, кто именно может вносить изменения, снижая риск случайных ошибок и потенциальных утечек. При этом, чем больше людей имеют доступ к данным, тем выше вероятность ошибки или преднамеренного нарушения безопасности. В дополнение к этому, рекомендуется использовать двухфакторную аутентификацию и регистрацию всех действий, связанных с изменениями данных, что позволит отслеживать каждый шаг процесса и оперативно выявлять подозрительные активности[3].

Помимо угроз потери данных и нарушений доступа, массовое обновление может представлять риск для конфиденциальности информации. В случае ошибки при обновлении чувствительная информация может быть случайно отправлена в неподходящее место, что приведёт к утечке данных и возможным юридическим последствиям. Этого можно избежать, используя проверенные и надёжные методы шифрования данных, что особенно важно при обработке персональных и финансовых данных. Дополнительно, компании могут внедрить протоколы безопасности, которые будут обеспечивать автоматическое сканирование на

наличие ошибок и недопустимых изменений перед финальным обновлением данных в системе[4].

Для обеспечения целостности данных также необходимо проводить регулярные проверки и тестирование на контрольных средах. Это позволит своевременно выявить и устранить ошибки до того, как они нанесут серьёзный ущерб. Кроме того, перед каждым обновлением необходимо провести тестовые испытания на отдельном сервере, чтобы убедиться, что процесс обновления не создаст конфликтов в системе. Таким образом, компании могут минимизировать риски, связанные с массовыми изменениями, и предотвратить сбои, которые могут нарушить рабочие процессы и привести к финансовым потерям[5].

Многие компании всё ещё недооценивают важность регулярных проверок и анализа данных после массовых обновлений. Эти проверки должны проводиться автоматически, чтобы сравнивать состояния данных до и после обновления. Если выявлены какие-либо отклонения или несовпадения, процесс может быть остановлен до тех пор, пока проблема не будет решена. Эти меры контроля помогут сохранить целостность данных и предотвратить возможные утечки. Кроме того, автоматизация процессов обновления и мониторинга данных также играет ключевую роль в снижении риска человеческих ошибок и повышении эффективности системы безопасности.

Заключение

Массовое обновление данных — это сложный и многогранный процесс, сопряжённый с рядом скрытых угроз, таких как потеря данных, утечка информации и нарушение целостности. Для минимизации этих рисков компаниям необходимо внедрять надёжные системы управления данными, использовать продуманные протоколы резервного копирования и шифрования, а также контролировать доступ на основе должностных обязанностей. Введение регулярных проверок целостности данных и тестирования обновлений на контрольных серверах перед массовым применением поможет предотвратить крупные сбои и минимизировать вероятность утечек.

Эффективная защита данных требует систематического подхода, который учитывает все этапы процесса обновления, от подготовки до завершения. В условиях, когда утечки и потери данных могут нанести серьёзный ущерб компании, внедрение комплексной стратегии защиты данных становится критически важным. Массовые обновления данных могут быть выполнены безопасно только при условии, что компании обеспечат высокий уровень контроля и защиты, что позволит избежать множества потенциальных проблем и защитить конфиденциальные данные от потерь и утечек.

Список литературы

1. Свидетельство о государственной регистрации программы для ЭВМ № 2020664289 РФ. Программа обеспечения системы компьютерного зрения на основе библиотеки OpenCV : № 2020663625 : заявл. 03.11.2020 : опубл. 11.11.2020 / И.Е.Пестов, А.М.Гельфанд, Н.Н.Лансере, И.И.Фадеев, заявитель ФГБОУ ВО «С-Пб-кий гос.университет телекоммуникаций им. проф. М.А. Бонч-Бруевича». – EDN PKSCLB.

2. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
3. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 72-76.
4. Пестов И. Е. МЕТОДИКА АВТОМАТИЗИРОВАННОГО ПРОТИВОДЕЙСТВИЯ НЕСАНКЦИОНИРОВАННЫМ ВОЗДЕЙСТВИЯМ НА ИНСТАНСЫ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ С ИСПОЛЬЗОВАНИЕМ БЕЗАГЕНТНОГО МЕТОДА СБОРА МЕТРИК.
5. Шемякин С. Н., Ахметшина М. Э., Катасонов А. И. Поиск функций, обладающих наилучшими характеристиками в классе от 4 переменных //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 61-65.

References

1. Certificate of state registration of the computer program No. 2020664289 Russian Federation. The program for providing a computer vision system based on the OpenCV library : No. 2020663625 : application 03.11.2020 : publ. 11.11.2020 / I. E. Pestov, A.M. Gelfand, N. N. Lancere, I.I. Fadeev ; applicant Federal State Budgetary Educational Institution of Higher Education "St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch- Bruevich." – EDN PKSCLB.
2. Lesnova E. M., Pestov I. E. Development of a method of error detection and correction for a distributed information network based on big data //Regional informatics and information security. – 2018. – pp. 236-240.
3. Pestov I. E. Methodology for developing control effects on cloud infrastructure instances //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2020. – No. 4. – pp. 72-76.
4. Pestov I. E. METHOD OF AUTOMATED COUNTERACTION TO UNAUTHORIZED IMPACTS ON CLOUD INFRASTRUCTURE INSTANCES USING AN AGENTLESS METHOD OF COLLECTING METRICS.
5. Shemyakin S. N., Akhmetshina M. E., Katasonov A. I. Search for functions with the best characteristics in a class of 4 variables //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2020. – No. 4. – pp. 61-65.