Столыпинский вестник

Научная статья

Original article

УДК 004.424

МОНИТОРИНГ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ

MONITORING PRIVILEGED USERS

Багдасаров Даниэль Михайлович, студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), baggggdass@rambler.ru

Bagdasarov Daniel Mikhailovich, bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), baggggdass@rambler.ru

Аннотация. Возможности привилегированных пользователей отличается от простых, что влияет на целостность данных и на их приоритет в организации безопасности информационной системы. В данной статье описаны возможные способы решения для защиты самого пользователя, так и данных в самой системе.

Abstract. The capabilities of privileged users differ from simple ones, which affects the integrity of data and their priority in organizing the security of an information system. This article describes possible solutions to protect the user himself and the data in the system itself.

Ключевые слова: информационная безопасность, привилегированные пользователи, риски, сохранность данных.

Keywords: information security, privileged users, risks, data safety.

Привилегированным пользователям — обычно администраторам баз данных, сетевым инженерам, специалистам по безопасности, хранителям облачных вычислений — для выполнения своей работы требуется неограниченный доступ к серверам, сетям, устройствам, приложениям или базам данных. С этим доступом привилегированные пользователи могут многое. Вносить изменения в серверы, сети, приложения, корпоративные устройства (включая ноутбуки, USB-устройства и внешние жесткие диски), приложения и базы данных. Управление профилями пользователей и привилегиями. Просматривайте конфиденциальные данные, включая интеллектуальную собственность, код, юридические данные, а также личную информацию сотрудников и клиентов, находящиеся в поддерживаемых ими базах данных. Изменить или удалить данные. Реагируйте на предупреждения системы безопасности, просматривая, изменяя или удаляя журналы аудита.

Однако их действия часто выполняются незаметно за пределами актива, над которым они работают. Что произойдет, если они намеренно или случайно поставят под угрозу конфиденциальность, целостность или доступность данных организации? Без эффективного мониторинга привилегированные пользователи могут причинить значительный ущерб, даже не будучи обнаруженными.

Опасности привилегированных учетных записей пользователей. Глобальный охват ИТ-активов (включая облачные технологии, виртуализацию и большие данные) создал потребность в более привилегированных пользовательских ролях для управления активами. В результате неограниченные привилегии пользователей часто широко назначаются ролям и отдельным лицам, чтобы упростить процесс управления пользователями и гарантировать, что они могут выполнять свою работу, не вызывая предупреждения системы безопасности или блокируя доступ к необходимым ресурсам.

Как это ни парадоксально, существуют опасности, связанные с учетными записями привилегированных пользователей. Совместное использование учетных данных. Некоторые организации назначают роль привилегированной учетной записи пользователя, а не конкретному пользователю. Это снижает возможность отслеживания личной ответственности в случае преднамеренного или случайного изменения данных или актива.

Нарушения отраслевых стандартов и стандартов соответствия. Привилегированный пользователь может намеренно или случайно нарушить стандарты доступности, целостности и конфиденциальности (AIC) следующим образом:

Проблема доступности. Привилегированные пользователи могут неправильно настроить компонент, тем самым заблокировав доступ к веб-сайту или другому ресурсу. Они также могли менять пароли, тем самым блокируя авторизованных пользователей.

Проблема целостности. Привилегированные пользователи могут изменять или удалять данные, включая журналы аудита, которые выявляют преднамеренные или случайные изменения данных.

Проблема конфиденциальности. Привилегированные пользователи могут получить доступ к личной идентификационной информации (PII) или другим конфиденциальным данным, даже если этот доступ не требуется для выполнения их работы.

Литература

1. Ван Хайтао Исследование системы осведомленности об информационной безопасности на основе технологий больших данных и искусственного интеллекта, Технологии и приложения сетевой безопасности, 2018 (3): 60-63.
2. Чжэн Яньфан Исследования и практика применения искусственного интеллекта и технологий анализа в системе ситуационной осведомленности информационной безопасности Мир цифровых коммуникаций, 2018, № 160 (4): 229.

3. Чжэн Фан Информационная безопасность в эпоху искусственного интеллекта, Исследования в области информационной безопасности, 2017, 3 (11): 966-967.
4. Дэн Вэньбинь Проблемы и меры противодействия надзору за информационной безопасностью в эпоху искусственного интеллекта Информационная безопасность Китая, 2018 г., 106 (10): 106-108.

References

1. Wang Haitao Research on Information Security Situation Awareness System Based on Big Data and Artificial Intelligence Technology, Network Security Technology and Application, 2018 (3): 60-63.
2. Zheng Yanfang Research and Practice of Artificial Intelligence Application and Analysis Technology in Information Security Situational Awareness System Digital Communication World, 2018, No.160 (4):229.
3. Zheng Fang Information Security in the Age of Artificial Intelligence, Information Security Research, 2017, 3 (11): 966-967.
4. Deng Wenbing Challenges and Countermeasures for Information Security Supervision in the Age of Artificial Intelligence China Information Security, 2018, 106 (10): 106-108.

© Багдасаров Д.М., 2022 Научный сетевой журнал «Столыпинский вестник», номер 4/2022.

Для цитирования: Багдасаров Д.М. Мониторинг привилегированных пользователей// Научный сетевой журнал «Столыпинский вестник», номер 4/2022.