Эксперт рассказал, какие уязвимости чаще всего есть в ИТ-системах интернет-магазинов

По данным компании «Нейроинформ», в первом квартале 2025 года число уязвимостей в безопасности среди российских ритейлеров возросло на 28% по сравнению с аналогичным периодом прошлого года. Генеральный директор компании Александр Дмитриев отметил, что среди самых распространённых уязвимостей на первом месте оказалось нарушение контроля доступа к важным данным и ресурсам. Эта проблема составила 34% всех обнаруженных инцидентов, в то время как 26% пришлось на отсутствие блокировки при переборе паролей в веб-приложениях, а 21% — на проблемы с аутентификацией на API-вызовах.

По словам экспертов, нарушение контроля доступа является одной из самых опасных уязвимостей, поскольку оно напрямую угрожает безопасности всей инфраструктуры компании. Специалисты компании обнаруживали утечку внутренних данных, таких как IP-адреса и ключи доступа, которые могут быть размещены в публичных материалах или конфигурационных файлах, доступных из интернета. Также встречаются случаи хранения учётных данных пользователей в метаданных, изображений и скриптах, что даёт злоумышленникам возможность легко получить доступ к системам и начать целенаправленные атаки.

Отсутствие блокировки при переборе паролей остаётся серьёзной угрозой для веб-приложений. Этот тип уязвимости позволяет преступникам с помощью автоматизированных инструментов подбирать пароли, используя слабые или стандартные комбинации. В сочетании с отсутствием двухфакторной аутентификации, это открывает двери для компрометации административных панелей и дальнейших атак на серверы и внутренние сети компаний. Наконец, отсутствие аутентификации на API-вызовах, по мнению аналитиков, становится новой, но критической угрозой для бизнеса. Без правильной защиты API-сервисы становятся уязвимыми для атак, что может привести к утечке данных и даже регуляторным штрафам.