УДК 004.056

В.Л. ЕВСЕЕВ, В.А. ПЕЧЕРСКИЙ

Национальный исследовательский ядерный университет «МИФИ», Москва

ЦЕЛЕСООБРАЗНА ЛИ ВИЗУАЛИЗАЦИЯ БЛОКИРОВОК СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ?

В докладе сделан акцент на анализ необходимости формирования уведомлений пользователям при блокировке их действий средствами защиты информации. Основное внимание уделено вопросам значительного снижения объема передаваемой информации об элементах защиты и дифференцированию событий безопасности по критичности.

Введение

В современных информационных системах (ИС) средства защиты информации (СЗИ) способны полностью блокировать действия клиента в случае обнаружения угроз. В таких ситуациях возникает вопрос о целесообразности информирования пользователей о блокировке по средствам соответствующих окон и создания событий безопасности в СЗИ. В связи со значительным потоком информации об инцидентах, которые требуется решить специалистам по информационной безопасности [1], в докладе проанализирован процесс информирования пользователей, а также детально рассмотрены возникающие при этом последствия.

Постановка задачи

Задача состоит в повышении эффективности работы администраторов СЗИ и уменьшении количества открытых данных об элементах защиты ИС путем определения инцидентов, в которых уведомления о блокировках пользователям избыточны.

Пути решения задачи

В ходе исследования был проведен анализ порядка 100 инцидентов информационной безопасности, зарегистрированных в течение 30 дней. Рассмотрены такие параметры, как тип инцидента, последствия и вероятность его возникновения. Для обработки данных использовался метод кластерного анализа, позволяющий разделить инциденты на группы по критичности. В частности, применен метод k-средних, который позволил выделить кластеры малокритичных и критичных инцидентов. Для подтверждения устойчивости кластеров применялись различные

методы валидации, включая «статистику Хопкинса», что позволило оценить тенденцию данных к группировке [2]. В вычислениях использовались инструменты на языке программирования R.

В результате проведенного исследования 12% событий были отнесены к группе малокритичных инцидентов, характеризующихся высокой вероятностью возникновения и низкими последствиями для ИС. Для событий данного типа предложена скрытая блокировка без отображения уведомлений, при которой действия пользователя прерываются без оповещения специалистов по ИБ. Данный фактор позволяет снизить нагрузку на администраторов безопасности и минимизировать риск утечек информации о работе СЗИ, что особенно актуально с учетом последних тенденций [3]. Напротив, для инцидентов с более серьезными последствиями, которые определены в 23% случаев, уведомления для пользователей и администраторов наиболее существенны, так как позволяют ускорить процесс реагирования на угрозы и минимизировать возможные негативные последствия для информационной системы.

Заключение

Исследование показало, что информирование пользователей о блокировках СЗИ должно носить дифференцированный характер в зависимости от критичности инцидента. Внедрение данного подхода может существенно повысить эффективность работы администраторов СЗИ, минимизировать количество открытой информации об используемых средствах защиты в ИС, а также улучшить пользовательский опыт. Разделение инцидентов по критичности позволяет снизить нагрузку на специалистов по ИБ, автоматизировать обработку некритичных инцидентов, и одновременно обеспечить оперативное реагирование на серьёзные угрозы, что в конечном итоге значительно повысит безопасность ИС.

Список литературы

1. Селютина А.А. Реагирование на инциденты информационной безопасности: научная статья / Селютина А.А. – СПб.: Изд-во СПбГЭУ, 2023. – 72 с.

2. Шитиков В.К., Мастицкий С.Э. Классификация, регрессия, алгоритмы Data Mining с использованием R [Электронный ресурс]. Режим доступа: https://github.com/ranalytics/data-mining, свободный (дата обращения 14.09.2024).

3. Стоделов Д.Н. Вопросы поиска информации об организациях по открытым источникам / Д.Н. Стоделов, Н.Г. Милославская // Кибернетика и информационная безопасность «КИБ-2023»: Сборник научных трудов Всероссийской научно-технической конференции, Москва, 18–19 октября 2023 года. – М.: НИЯУ МИФИ, 2023. – С. 82–83. – EDN IBCWQR.