МСЭ, время проверки значительно сокращается.

Разработана методика автоматизированного обнаружения отсутствующих правил на межсетевых экранах. Она преобразует пользовательские запросы в структурированные параметры через LLM, определяет нужный МСЭ по подсети источника и проверяет наличие правила. Время диагностики сокращается с минут до секунд, что позволяет быстро выявлять причину проблем и восстанавливать доступ к сервисам.

Список использованных источников

1.Кривец, А. С. Анализ систем искуственного интелекта применяемых для работы систем обнаружения вторжений / А. С. Кривец, С. И. Штеренберг // Технологии информационного общества : Сборник трудов XVIII Международной отраслевой научно-технической конференции, Москва, 27–28 февраля 2024 года. – Москва: Московский технический университет связи и информатики, 2024. – С. 99-101. – EDN MQZRNG.

2.Разработка концепции определения нелегитимного трафика dns. Платонов А.Е., Ковцур М.М., Ушаков И.А. В книге: Региональная информатика (РИ-2024). Материалы XIX Санкт-Петербургской международной конференции. Санкт-Петербург, 2024. С. 412-413.

3.Организация защищенного взаимодействия распределенных сетевых устройств. Ковцур М.М., Браницкий А.А., Казаков Н.И. В книге: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 51-й Международной конференции. Москва, 2023. С. 37-39.

Махмутова Нурия Фаритовна, магистрант, iromup9898@gmail.com
Алькаттан Самех, магистрант, sameh.kt94@gmail.com.
Ковцур Максим Мхайлович, к.т.н., доцент каф. ЗСС, kovcur.mm@sut.ru
Ушаков Игорь Александрович, и.о. зав. каф. ИБКС, к.т.н., доцент, доцент каф. ИКС

УДК 004.056.53

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕХАНИЗМОВ ЗАЩИТЫ ОТ АТАК ЛОКАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ СИСТЕМНЫХ СЛУЖБ ASTRA LINUX SE И КЛАССИЧЕСКИХ GNU/LINUX-ДИСТРИБУТИВОВ

Д. Е. Гилева, А. М. Гельфанд, М. М. Ковцур
СПбГУТ им проф. М. А. Бонч-Бруевича, г. Санкт-Петербург

Ключевые слова: информационная безопасность, Astra Linux Special Edition, GNU/Linux, мандатный контроль целостности.

Защита системных служб от атак локальных пользователей —важная задача обеспечения безопасности операционный систем (ОС). Безопасность системных служб в классических дистрибутивах основана на комбинации механизмов, ядром которой является дискреционное управление доступом (права UNIX). Управление правами для множества служб децентрализовано,

что усложняет верификацию и контроль целостности политик [1].

Systemd обеспечивает изоляцию через Namespaces, создавая «песочницу», что минимизирует риски, но не исключает их. AppArmor (Ubuntu) — профили на основе путей или SELinux (RHEL) — политики на основе меток реализуют мандатное управление доступом с тонкими политиками, однако политики по умолчанию носят общий характер и требуют нетривиальной адаптации для жёсткого ограничения служб. В Debian/RHEL используется подсистема аудита ядра Linux. Она предназначена для отслеживания критичных с точки зрения безопасности системных событий [1].

Astra Linux SE выделяется среди ОС благодаря мандатной сущностно-ролевой ДП-модели (МРОСЛ ДП). В этой модели субъекты делятся на доверенные и недоверенные. Считается, что после настройки системы доверенными субъектами, работа недоверенных не должна нарушать политики безопасности. Это обеспечивает изоляцию пользовательских сессий от системных служб [2].

Мандатное управление доступом (МУД) является основой Astra Linux SE. Все субъекты и объекты помечаются мандатными метками, включающими уровень конфиденциальности и набор категорий. Доступ разрешён по правилу «не ниже» для чтения и «не выше» для записи. Системная служба имеет фиксированную метку, и её доступ к ресурсам жёстко ограничен политикой даже при root-правах [2].

Наличие мандатного контроля целостности (МКЦ) в ОС Astra Linux SE дозволяет создавать изолированные «песочницы» с пониженным уровнем целостности для недоверенного ПО. Это обеспечивает защиту системы: даже при атаке или заражении вредоносное ПО не влияет на доверенные приложения (рис. 1) [2].

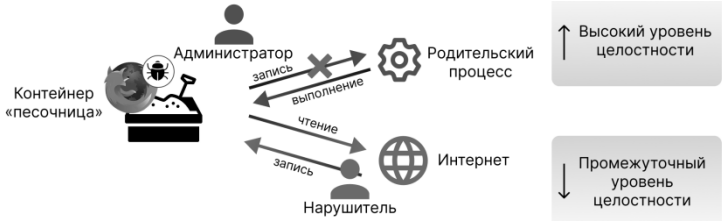

Рисунок 1 - Безопасный запуск процессов в ОС Astra Linux SE

Astra Linux SE включает механизм Киоск-2 для ограничения прав непривилегированных пользователей. Вместе с МКЦ и защитой от информационных закладок он предотвращает типовые угрозы. Гибкость обеспечивается профилями безопасности с ограничениями доступа к файлам — можно назначать несколько профилей или не назначать ни одного [3]. Система аудита PARSEC интегрирована с МУД и МКЦ: события безопасности фиксируются в защищённых журналах с привязкой к

мандатным меткам, что упрощает анализ инцидентов. Настройка аудита централизованная, через графическую утилиту, с привязкой к пользователям и группам [2].

Анализ показал принципиально разные подходы к безопасности. Классические дистрибутивы (Debian, RHEL) используют адаптивную модель на базе дискреционного доступа: она гибка, но требует ручной настройки администратором, иначе система уязвима даже для root. Astra Linux SE реализует проактивную модель, где защита изначально встроена в архитектуру на основе формальной модели МРОСЛ.

Список использованных источников

1. Оценка стойкости механизма, реализующего мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства GNU Linux / А. И. Катасонов, С. И. Штеренберг, А. Ю. Цветков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – № 2. – С. 50-56. – DOI 10.46418/2079-8199_2020_2_8. – EDN EUMWWI

2. Преимущества использования СЗИ в ОС Astra Linux Special Edition [Электронный ресурс] // habr.com. – URL: https://habr.com/ru/companies/astralinux/articles/670060/

Гилева Дарья Евгеньевна, бакалавриат СПбГУТ, daryagileva.2004@yandex.ru.
Гельфанд Артем Максимович, стар. препод. каф. ЗСС, gelfand.am@sut.ru
Ковцур Максим Михайлович, к.т.н., доцент, доцент каф. ИБКС, kovcur.mm@sut.ru

УДК 004.7.056; 004.7:004.8

СИСТЕМА ОБНАРУЖЕНИЯ АНОМАЛИЙ НА ОСНОВЕ АНАЛИЗА ЖУРНАЛА СОБЫТИЙ

Е.А. Атарская, А.М. Вульфин, А.Д. Кириллова
Уфимский университет науки и технологий, г. Уфа

Ключевые слова: интеллектуальный анализ данных, машинное обучение, анализ логов, межсетевые экраны.

Растущее число кибератак и появление новых уязвимостей требуют комплексных и адаптивных подходов к защите. Для обеспечения безопасности применяются различные системы и подходы, в том числе межсетевые экраны уровня веб-приложений (WAF).

Внедрение алгоритмов машинного обучения (МО) в WAF значительно расширяет возможности защиты веб-приложений, позволяя автоматизировать обнаружение аномалий и новых векторов атак, позволяет сократить количество ложных срабатываний и адаптироваться к меняющимся условиям работы, что повышает точность обнаружения угроз и снижает нагрузку на специалистов по информационной безопасности.