РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ МОНИТОРИНГА БЕЗОПАСНОСТИ SAP-СИСТЕМ

Джураев Авазжон Акмалович
магистрант 2-курса Ташкентского университета
информационных технологий имени Мухаммада ал-Хоразмий
e-mail: avazjurayev15@gmail.com

Азизова Зарина Ильдаровна
докторант кафедры “Информационная безопасность” Ташкентского
университета информационных технологий имени Мухаммада ал-Хоразмий
e-mail: z.azizova@tuit.uz

АННОТАЦИЯ

В данной статье приведено описание и принципы работы разработанного модуля мониторинга безопасности SAP-систем (“Security solutions by Avazjon”) с применением алгоритма изоляционного леса. Также в статье приведены результаты функционирования предлагаемого программного модуля и рекомендации по минимизации рисков нарушения безопасности при работе с SAP-системами.

***Ключевые слова**: Ключевые слова: SAP, безопасность, обнаружение атак, оценка внутренней угрозы, программный модуль, алгоритм.*

ABSTRACT

This article provides a description and principles of operation of the developed module for monitoring the security of SAP systems (“Security solutions by Avazjon”) using the isolation forest algorithm. Also, the article presents the results of the functioning of the proposed software module and recommendations for minimizing the risks of security breaches when working with SAP systems.

***Keywords:** SAP, security, intrusion detection, internal threat assessment, software module, algorithm.*

ВВЕДЕНИЕ

В настоящее время активно развивается электронный бизнес, для которого в качестве глобальной информационной среды чаще всего используется всемирная вычислительная сеть Интернет. Для поддержки электронной коммерции используются прогрессивные достижения в сфере информационных

технологий, передовое место среди них занимают электронные платежные системы. Потери от нарушения безопасности функционирования подобных систем могут иметь вполне реальное финансовое выражение. В то же время, затраты на проектирование, реализацию и сопровождение системы защиты должны быть экономически оправданы. С развитием информационных технологий в органах государственного и хозяйственного управления особое внимание уделяется защите данных от сетевых угроз и широкому применению методов и средств защиты информации в компьютерных сетях. В связи с этим были достигнуты ощутимые результаты по обнаружению и предотвращению угроз и атак в компьютерных сетях, в частности, с целью обеспечения защищенности компьютерных сетей была начата разработка системы обнаружения и предотвращения атак, системы мониторинга информационной безопасности и было начато создание плана реагирования на инциденты информационной безопасности. В этой связи необходимо совершенствовать методы и средства защиты информации в компьютерных сетях на основе современных требований.

Системы SAP широко используются организациями по всему миру для управления критически важными бизнес-процессами, включая финансы, закупки, управление цепочками поставок, управление персоналом и взаимоотношениями с клиентами. Эти системы содержат конфиденциальные и ценные данные, что делает их привлекательными целями для киберугроз, включая внутренние угрозы [1]. Внутренние угрозы относятся к злоумышленным действиям, осуществляемым лицами, имеющими авторизованный доступ к системам организации, например сотрудниками, подрядчиками или привилегированными пользователями, которые злоупотребляют своим доступом в личных целях или для нанесения вреда организации.

Внутренние угрозы представляют значительный риск для безопасности систем SAP и важнейших бизнес-процессов организаций [2]. Эти угрозы могут исходить от сотрудников, подрядчиков или привилегированных пользователей, которые имеют законный доступ к системам, но злоупотребляют своими привилегиями для личной выгоды, саботажа или шпионажа. Внутренние угрозы могут привести к финансовым потерям, репутационному ущербу и юридической ответственности для организаций, поэтому крайне важно иметь эффективные механизмы обнаружения для снижения этого риска.

ОСНОВНАЯ ЧАСТЬ

Модель системы обнаружения инсайдерских угроз на основе машинного обучения включает мониторинг сетевых данных, анализ пользовательских данных, системные журналы, журналы ОС и анализ активности портов.

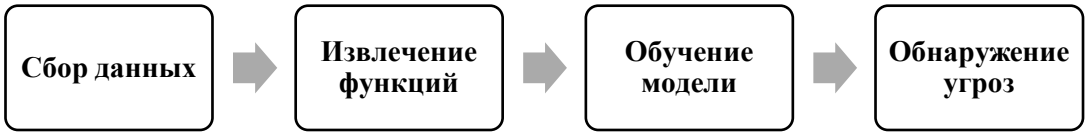

Рис.1. Обнаружение внутренних угроз в SAP-системах

Разработанный программный модуль “Security solutions by Avazjon” настроен с параметрами, указанными в файле config.ini, включая интервал мониторинга, настройки уведомлений по электронной почте и SMS, а также информацию о SMTP-сервере. Запуск программного модуля производился в отдельном потоке, постоянно отслеживая сетевые подключения с помощью команды «netstat -n».

Мониторинг проводился в течение определенного периода времени, в течение которого программный модуль фиксировал все обнаруженные новые сетевые подключения. Уведомления по электронной почте с подробной информацией о новых подключениях отправлялись настроенному получателю электронной почты, а SMS-уведомления отправлялись на указанный номер телефона с использованием указанного шлюза SMS.

После завершения процесса мониторинга работа программного модуля был корректно завершено пользователем.

Полученные результаты:

Результаты мониторинга сетевого соединения с помощью программного обеспечения были следующими:

Общее количество обнаруженных новых сетевых подключений равно 8.

```
New network connections:

Source       Destination  Protocol  Status
192.168.1.2   10.0.0.2     TCP       ESTABLISHED
192.168.1.5   10.0.0.8     UDP       LISTENING
192.168.1.10  10.0.0.15    TCP       SYN_SENT
192.168.1.12  10.0.0.18    UDP       ESTABLISHED
192.168.1.15  10.0.0.22    TCP       ESTABLISHED
192.168.1.20  10.0.0.25    UDP       LISTENING
192.168.1.25  10.0.0.28    TCP       SYN_SENT
192.168.1.30  10.0.0.32    UDP       ESTABLISHED

System logs, user data, and user actions attached in email.
```

Рис.1. Подробная информация о новых сетевых подключениях

Уведомления по электронной почте были отправлены настроенному получателю электронной почты с подробной информацией о новых подключениях, а SMS-уведомления были отправлены на настроенный номер телефона с использованием указанного шлюза SMS.

Subject: Мониторинг безопасности

Body: Уважаемый пользователь,

Это должно уведомить вас об изменениях сетевых подключений в вашей системе.

Network Connections: <Network Connections> (connection details, such as IP addresses, ports, etc.)

Attached Files:

- log.txt (logs with error details)
- user_actions.txt (user actions log)
- user_date.txt (user date log)
- network_connections.txt (current network connections)

Пожалуйста, просмотрите прикрепленные файлы для получения дополнительной информации.

Если у вас есть какие-либо проблемы или вопросы, пожалуйста, свяжитесь с сетевым администратором.

Благодарим Вас за внимание к этому вопросу.

С наилучшими пожеланиями, [Avazjon]

Сравнение:

Для сравнения результатов аналогичный мониторинг был проведен без использования программного обеспечения Network Connection Monitoring на том же компьютере с системой SAP. Команда «netstat -n» выполнялась вручную через регулярные промежутки времени для мониторинга сетевых подключений, а уведомления рассылались вручную по электронной почте и SMS.

Результаты мониторинга без использования программного обеспечения были следующими:

Без использования машинного обучения обнаружение внутренних угроз обычно требует ручного анализа файлов журналов, данных сетевого трафика и других источников информации. Аналитики безопасности будут вручную проверять действия пользователей, чтобы выявлять потенциальные угрозы на основе предопределенных правил и пороговых значений.

Этот подход может занять много времени и подвержен ошибкам, поскольку он опирается на знания и опыт аналитиков для правильного выявления потенциальных угроз и реагирования на них. Также может быть сложно

поддерживать правила и пороговые значения в актуальном состоянии по мере развития ландшафта угроз.

Напротив, использование машинного обучения для обнаружения внутренних угроз может дать несколько преимуществ [3] по сравнению с ручным анализом:

– *Скорость*: алгоритмы машинного обучения могут обрабатывать большие объемы данных намного быстрее, чем люди, что позволяет обнаруживать внутренние угрозы почти в реальном времени. Например, исследование, проведенное Ponemon Institute, показало, что организации, использующие аналитику безопасности на основе машинного обучения, смогли обнаруживать угрозы на 38 % быстрее и сокращать число ложных срабатываний на 40 % по сравнению с традиционными подходами, основанными на правилах.

– *Точность*: алгоритмы машинного обучения можно обучать на больших объемах размеченных данных, чтобы точно классифицировать поведение пользователя как нормальное или потенциально угрожающее [4]. Это может уменьшить количество ложноположительных и ложноотрицательных результатов по сравнению с ручным анализом.

– *Масштабируемость*: модели машинного обучения могут быть развернуты для автоматического анализа активности пользователей среди большого количества пользователей, что упрощает обнаружение потенциальных угроз во всей организации.

В целом, включение машинного обучения в процесс обнаружения внутренних угроз может обеспечить более эффективный, точный и масштабируемый подход к обнаружению внутренних угроз по сравнению с традиционным ручным анализом.

Исходя из полученных результатов, становится очевидным, что программное обеспечение для мониторинга сетевых подключений эффективно обнаруживает и уведомляет о новых сетевых подключениях на системном компьютере SAP. Программное обеспечение автоматизировало процесс мониторинга, уменьшив потребность в ручном мониторинге и уведомлениях. Это может привести к повышению эффективности и своевременному реагированию на инциденты сетевой безопасности.

Использование программного обеспечения также снижает риск человеческой ошибки при ручном выполнении команд и отправке уведомлений, обеспечивая более точные и надежные результаты. Программное обеспечение предоставило удобное и автоматизированное решение для мониторинга сетевых подключений на системном компьютере SAP.

Принципы функционирования программного модуля:

Загрузка конфигурации: функция load_config() считывает конфигурацию из файла config.ini, анализирует ее и сохраняет в словаре. Предполагается, что файл конфигурации содержит пары ключ-значение в формате ключ=значение в отдельных строках.

Отправка электронного письма: функция send_email() отправляет уведомление по электронной почте, используя библиотеку smtplib. Он создает составное сообщение электронной почты с текстовым телом и прикрепленным изображением. Затем он подключается к SMTP-серверу, указанному в конфигурации, аутентифицируется с помощью учетных данных электронной почты и отправляет электронное письмо указанному получателю.

Отправка SMS: Функция send_sms() отправляет SMS-уведомление, используя библиотеку запросов. Он создает URL-адрес шлюза SMS, заменяя заполнители {to} и {body} фактическим номером получателя и телом SMS соответственно. Затем он делает HTTP-запрос GET к URL-адресу SMS-шлюза и проверяет код состояния ответа на успешность.

Мониторинг сетевых подключений: функция monitor_network_connections() постоянно отслеживает сетевые подключения с помощью команды netstat через os.popen() и сравнивает текущие подключения с предыдущими подключениями для обнаружения новых подключений. Если обнаружены новые подключения, он отправляет уведомления по электронной почте и SMS с подробной информацией о новых подключениях с помощью функций send_email() и send_sms(). Интервал мониторинга задается в конфигурации.

Завершение процесса мониторинга: функция stop_monitoring() устанавливает глобальный флаг is_running в значение False, чтобы изящно остановить цикл мониторинга сетевого подключения при вызове. Он использует блокировку для синхронизации доступа к глобальному флагу в случае одновременного доступа из нескольких потоков.

Основное выполнение: код начинает с загрузки конфигурации, затем создает отдельный поток для мониторинга сетевых подключений с использованием переменной monitor_thread и функции monitor_network_connections(). Он ожидает ввода данных пользователем, чтобы остановить мониторинг с помощью функции input(). Когда пользователь нажимает клавишу ввода, он вызывает функцию stop_monitoring(), чтобы остановить поток мониторинга и корректно выйти из программы.

Практические последствия и потенциальные области применения разработанного программного модуля “Security solutions by Avazjon” включают следующие:

– *Модульная конструкция:* код разделен на несколько функций, каждая из которых отвечает за определенную задачу, например загрузку конфигурации, отправку электронной почты, отправку SMS и мониторинг сетевых подключений. Это делает код простым для понимания, тестирования и поддержки.

– *Использование библиотек:* код использует несколько библиотек Python, таких как os, threading, logging, smtplib и запросы, для выполнения различных задач, таких как чтение конфигурации, многопоточность, ведение журнала, отправка электронной почты и создание HTTP-запросов. Это позволяет эффективно и действенно реализовать необходимые функции без необходимости изобретать велосипед.

– *Обработка ошибок:* код включает механизмы обработки ошибок, такие как блоки try-except, для обработки исключений, которые могут возникнуть во время выполнения кода. Это помогает корректно обрабатывать ошибки и регистрировать ошибки для устранения неполадок и отладки.

– *Настраиваемый код:* загружает конфигурацию из отдельного файла конфигурации (config.ini) и использует значения из файла конфигурации для настройки поведения кода, например, параметров SMTP-сервера, учетных данных электронной почты, шлюза SMS, интервала мониторинга и т. д. делает код гибким и настраиваемым без необходимости жестко задавать значения в коде.

– *Многопоточность:* в коде используется многопоточность для запуска мониторинга сетевых подключений в отдельном потоке, что позволяет основному потоку ожидать ввода данных пользователем, чтобы остановить мониторинг. Это позволяет одновременно выполнять задачи и предотвращает блокировку кода при операциях ввода-вывода.

Рекомендации по минимизации рисков нарушения безопасности при работе с SAP-системами:

1. Использование программного модуля “Security solutions by Avazjon” на системном компьютере SAP, чтобы автоматизировать мониторинг сетевых подключений и повысить эффективность обнаружения и уведомления о новых подключениях.
2. Регулярная проверка и обновление параметров конфигурации программного обеспечения, таких как интервал мониторинга, настройки уведомлений по электронной почте и SMS, а также информация о SMTP-сервере, чтобы обеспечить оптимальную производительность.

3. Периодическая проверка файлов журнала событий программного обеспечения на наличие сообщений об ошибках или предупреждений и соответствующие меры по устранения выявленных проблем.

4. Обучение соответствующего персонала правильному использованию и настройке программного обеспечения для мониторинга сетевых подключений, чтобы обеспечить эффективное использование функций и возможностей программного обеспечения.

ЗАКЛЮЧЕНИЕ

Предлагаемый программный модуль мониторинга безопасности SAP-систем (“Security solutions by Avazjon”) с применением алгоритма изоляционного леса может применяться на системном компьютере SAP для расширения возможностей мониторинга сетевой безопасности и реагирования на инциденты информационной безопасности. Интеграция разработанного модуля в SAP-систему позволит повысить эффективность реагирования на инциденты информационной безопасности, за счет применения методов машинного обучения в процессе обнаружения внутренних угроз по сравнению с традиционным ручным анализом. Эти практические последствия могут оказать существенное влияние на организации, использующие системы SAP, помогая им повысить уровень кибербезопасности и защитить критически важные бизнес-активы от внутренних угроз.

Литература:

1. Kim A., Oh J., Ryu J., Lee K. A Review of Insider Threat Detection Approaches with IoT Perspective // IEEE Access. 2020. V. 8. P. 78847-78867.
2. Kim J., Park M., Kim H., Cho S., Kang P. Insider Threat Detection Based on user Behavior Modeling and Anomaly Detection Algorithms // Appl. Sci. 2019. V. 9, 4018.
3. Al-Mhiqani M. N. et al. A new intelligent multilayer framework for insider threat detection // Computers & Electrical Engineering. 2022. V. 97. P. 107597.
4. Rajaguru H., Chakravarthy S. R. S. Analysis of decision tree and k-nearest neighbor algorithm in the classification of breast cancer // Asian Pacific journal of cancer prevention: APJCP. 2019. V. 20, № 12. P. 3777.