Столыпинский вестник

Научная статья

Original article

УДК 004.424

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

AUTOMATION OF VULNERABILITY MANAGEMENT

Цымбал Федор Алексеевич студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), tsybal007@rambler.ru

Tsymbal Fedor Alekseevich bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), tsybal007@rambler.ru

Аннотация: Методы управления уязвимостями основаны на тестировании, аудите и сканировании для обнаружения проблем. Эти процессы часто автоматизированы, чтобы гарантировать, что компоненты оцениваются по определенному стандарту, а уязвимости обнаруживаются как можно быстрее. Другой метод, который вы можете использовать, — это поиск угроз , который включает в себя исследование систем в режиме реального времени для выявления признаков угроз или обнаружения потенциальных уязвимостей.

Abstract: Vulnerability management methods are based on testing, auditing and scanning to detect problems. These processes are often automated to ensure that components are evaluated to a certain standard and vulnerabilities are found as quickly as possible. Another method you can use is Threat Scanning, which

involves real-time examination of systems to look for signs of threats or discover potential vulnerabilities.

Ключевые слова: информационная безопасность, уязвимости, автоматизация информационной безопасности

Keywords: information security, vulnerabilities, information security automation

Управление уязвимостями — это практика, направленная на снижение неотъемлемых рисков в приложении или системе. Идея этой практики заключается в обнаружении и устранении уязвимостей до того, как проблемы будут обнаружены или использованы. Чем меньше уязвимостей в компоненте или системе, тем в большей безопасности ваша информация и ресурсы.

Аварийное восстановление

Стратегии аварийного восстановления защищают вашу организацию от потерь или ущерба в результате непредвиденных событий. Например, программы-вымогатели, стихийные бедствия или отдельные точки отказа. Стратегии аварийного восстановления обычно учитывают, как вы можете восстановить информацию, как вы можете восстановить системы и как вы можете возобновить работу. Эти стратегии часто являются частью плана управления непрерывностью бизнеса (BCM), разработанного, чтобы позволить организациям поддерживать операции с минимальным временем простоя.

Руководители по информационной безопасности (CISO) — это люди, ответственные за управление и обеспечение защиты информации организации. Эта роль может быть отдельной позицией или входить в обязанности вице-президента (VP) по безопасности или главного сотрудника по безопасности (CSO).

В обязанности директора по информационной безопасности входит управление:

– Операции по обеспечению безопасности — включают в себя мониторинг, анализ и сортировку угроз в режиме реального времени.

– Киберриск и кибербразведка — включает в себя поддержание текущих знаний об угрозах безопасности и информирование руководства и совета директоров о потенциальном влиянии рисков.

– Потеря данных и предотвращение мошенничества — включает в себя мониторинг и защиту от внутренних угроз.

– Архитектура безопасности — включает в себя применение передовых методов обеспечения безопасности при приобретении, интеграции и эксплуатации аппаратного и программного обеспечения.

– Управление идентификацией и доступом — включает в себя обеспечение надлежащего использования мер аутентификации, мер авторизации и предоставления привилегий.

– Управление программой — включает в себя обеспечение упреждающего обслуживания аппаратного и программного обеспечения посредством проверок и обновлений.

– Расследования и судебная экспертиза — включает сбор доказательств, взаимодействие с властями и обеспечение проведения вскрытия.

– Управление — включает в себя проверку бесперебойной работы всех операций по обеспечению безопасности и служит посредником между руководством и операциями по обеспечению безопасности.

Центр управления безопасностью (SOC) — это набор инструментов и членов команды, которые постоянно отслеживают и обеспечивают безопасность организации. SOC служат единой базой, с помощью которой команды могут обнаруживать, исследовать, реагировать и устранять угрозы безопасности или уязвимости. В частности, SOC призваны помочь организациям предотвращать угрозы кибербезопасности и управлять ими.

Основная идея SOC заключается в том, что централизованные операции позволяют командам более эффективно управлять безопасностью,

обеспечивая всестороннюю видимость и контроль над системами и информацией. Эти центры сочетают решения в области безопасности и человеческий опыт для выполнения или руководства любыми задачами, связанными с цифровой безопасностью.

Для реализации SOC используются три основные модели:

- Внутренний SOC — состоит из преданных своему делу сотрудников, работающих внутри организации. Эти центры обеспечивают высочайший уровень контроля, но имеют высокие первоначальные затраты и могут быть трудными для персонала из-за трудностей с набором персонала с нужным опытом. Внутренние SOC обычно создаются корпоративными организациями со зрелыми стратегиями в области ИТ и безопасности.
- Виртуальный SOC — используйте управляемые сторонние сервисы, чтобы обеспечить покрытие и экспертизу для операций. Эти центры просты в настройке, легко масштабируются и требуют меньших первоначальных затрат. Недостатком является то, что организации зависят от поставщиков и имеют меньшую видимость и контроль над своей безопасностью. Виртуальные SOC часто используются малыми и средними организациями, в том числе теми, у которых нет собственных ИТ-отделов.
- Гибридный SOC — объединение внутренних команд с внешними командами. Эти центры используют управляемые услуги, чтобы заполнить пробелы в охвате или опыте. Например, обеспечить круглосуточный мониторинг без организации внутренних ночных смен. Гибридные SOC могут позволить организациям поддерживать более высокий уровень контроля и видимости без ущерба для безопасности. Недостатком этих центров является то, что затраты часто выше, чем у виртуальных SOC, а координация может быть сложной.

Общие риски информационной безопасности

В вашей повседневной работе многие риски могут повлиять на вашу систему и информационную безопасность. Некоторые распространенные риски, о которых следует знать, перечислены ниже.

Атаки социальной инженерии

Социальная инженерия включает в себя использование психологии, чтобы обманом заставить пользователей предоставить информацию или доступ к злоумышленникам. Фишинг — это один из распространенных видов социальной инженерии, обычно осуществляемый по электронной почте. При фишинговых атаках злоумышленники выдают себя за надежные или законные источники, запрашивая информацию или предупреждая пользователей о необходимости принять меры. Например, электронные письма могут просить пользователей подтвердить личные данные или войти в свои учетные записи по включенной (вредоносной) ссылке. Если пользователи соблюдают требования, злоумышленники могут получить доступ к учетным данным или другой конфиденциальной информации.

Расширенные постоянные угрозы (APT)

APT — это угрозы, при которых отдельные лица или группы получают доступ к вашим системам и остаются в них в течение длительного периода времени. Злоумышленники осуществляют эти атаки для сбора конфиденциальной информации с течением времени или в качестве основы для будущих атак. APT-атаки осуществляются организованными группами, которым могут платить конкурирующие государства, террористические организации или конкуренты в отрасли.

Внутренние угрозы

Внутренние угрозы — это уязвимости, созданные отдельными лицами в вашей организации. Эти угрозы могут быть случайными или преднамеренными и включать злоумышленников, злоупотребляющих «законными» привилегиями для доступа к системам или информации. В случае случайных угроз сотрудники могут непреднамеренно поделиться или раскрыть информацию, загрузить вредоносное ПО или украсть свои учетные данные. С помощью преднамеренных угроз инсайдеры преднамеренно повреждают, сливают или крадут информацию для личной или профессиональной выгоды.

Криптоджекинг

Криптоджекинг, также называемый крипто-майнингом , — это когда злоумышленники злоупотребляют вашими системными ресурсами для майнинга криптовалюты. Злоумышленники обычно добиваются этого, обманом заставляя пользователей загружать вредоносное ПО или когда пользователи открывают файлы с включенными вредоносными сценариями. Некоторые атаки также выполняются локально, когда пользователи посещают сайты, содержащие сценарии майнинга.

Распределенный отказ в обслуживании (DDoS)

DDoS-атаки происходят, когда злоумышленники перегружают серверы или ресурсы запросами. Злоумышленники могут выполнять эти атаки вручную или через ботнеты, сети скомпрометированных устройств, используемые для распространения источников запросов. Цель DDoS-атаки — запретить пользователям доступ к службам или отвлечь службы безопасности, пока происходят другие атаки.

Программы-вымогатели

Атаки программ-вымогателей используют вредоносное ПО для шифрования ваших данных и удержания их с целью получения выкупа. Как правило, злоумышленники требуют информацию, чтобы были предприняты какие-то действия, или оплату от организации в обмен на расшифровку данных. В зависимости от типа используемой программы-вымогателя вы не сможете восстановить зашифрованные данные. В этих случаях вы можете восстановить данные, только заменив зараженные системы чистыми резервными копиями.

Атака «человек посередине» (MitM)

Атаки MitM происходят, когда сообщения отправляются по незащищенным каналам. Во время этих атак злоумышленники перехватывают запросы и ответы, чтобы прочитать содержимое, манипулировать данными или перенаправить пользователей.

Существует несколько типов атак MitM, в том числе:

– Перехват сеанса — при котором злоумышленники подменяют свой собственный IP-адрес законным пользователям, чтобы использовать их сеанс и учетные данные для получения доступа к системе.

– IP-спуфинг — при котором злоумышленники имитируют надежные источники для отправки вредоносной информации в систему или запроса информации обратно.

– Атаки с прослушиванием — при которых злоумышленники собирают информацию, передаваемую при общении между законными пользователями и вашими системами.

Технологии информационной безопасности

Создание эффективной стратегии информационной безопасности требует применения различных инструментов и технологий. Большинство стратегий используют некоторую комбинацию следующих технологий.

Брандмауэры

Брандмауэры — это уровень защиты, который можно применять к сетям или приложениям. Эти инструменты позволяют фильтровать трафик и передавать данные о трафике в системы мониторинга и обнаружения. Брандмауэры часто используют установленные списки одобренного или неутвержденного трафика и политики, определяющие скорость или разрешенный объем трафика.

Литература

1. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.
2. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
3. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 400 с.
4. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 476 с.

5. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.
6. Баранова, Е.К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. - М.: Риор, 2008. - 400 с.
7. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.
8. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.
9. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: Инфра-М, 2018. - 64 с.

References

1. Babash, A.V. Information security: Laboratory workshop / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2019. - 432 p.
2. Babash, A.V. Information Security. Laboratory workshop: Textbook / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2013. - 136 p.
3. Baranova E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2017. - 400 p.
4. Baranova E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2017. - 476 p.
5. Baranova E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2018. - 400 p.
6. Baranova E.K. Information Security. History of special methods of cryptographic activity: Textbook / E.K. Baranova, A.V. Babash, D.A. Larin. - M.: Rior, 2008. - 400 p.
7. Biryukov, A.A. Information security: protection and attack / A.A. Biryukov. - M.: DMK Press, 2013. - 474 p.
8. Gafner, V.V. Information Security: Textbook / V.V. Gafner. - Rn / D: Phoenix, 2010. - 324 p.

9. Glinskaya E.V. Information security of computer structures and systems: Textbook / E.V. Glinskaya, N.V. Chichvarin. - M.: Infra-M, 2018. - 64 p.

Для цитирования: Цымбал Ф.А. АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ// *Научный сетевой журнал «Столыпинский вестник» №4/2022.*