Литература:

1. Безопасность гидротехнических сооружений в Центральной Азии. Создание потенциала и региональное сотрудничество. 2021. – 66 с. – URL: https://unece.org/sites/default/files/2021-07/Dam%20Safety%20Review_RU.pdf (дата обращения 15.09.2023).

2. *Кукшинов М.С.* Водохранилища и безопасность. Некоторые аспекты проблемы / Проблемы гидрометеорологического обеспечения хозяйственной деятельности в условиях изменяющегося климата: материалы Международной научн. конф., 5-8 мая 2015 г. – Минск: Издательский центр БГУ, 2015. – 337 с. – URL: https://elib.bsu.by/handle/123456789/118300 (дата обращения 10.09.2023).

3. *Агасандян Г.А., Гасанов И.И., Ерешко Ф.И.* Новые подходы в проблеме комплексного управления водными ресурсами. – М.: ВЦ РАН, 2003. – 54 с.

4. *Агасандян Г.А.* Некоторые вопросы управления водохранилищами. – М.: ВЦ АН СССР, 1986. – 40 с.

DOI: 10.25728/iccss.2023.51.41.036

Синцов М.И.

Проблемы выявления угроз, связанных с эксплуатацией уязвимостей в программном обеспечении, через ретроспективный анализ событий информационной безопасности

Аннотация: В современном мире, где цифровые технологии все глубже проникают во все сферы нашей жизни, вопрос информационной безопасности становится все более актуальным. В постпандемическом мире гибридный режим работы (сочетание работы в офисе и удаленной работы) стал не только нормой, но и предпочтительной ситуацией для многих. Эта среда, стремительное внедрение новых технологий, повсеместная цифровизация бизнес-процессов приводят к появлению новых возможностей и расширению площади атаки, представляют собой уникальные и обширные возможности для киберпреступников. В работе рассмотрены проблемы

выявления угроз, связанных с уязвимостями в программном обеспечении, исследованы подходов к выработке соответствующих правил корреляции и определены направления дальнейших исследований в целях совершенствования механизмов ретроспективного анализа.

Ключевые слова: информационная безопасность, угрозы, эксплуатация уязвимостей, ретроспективный анализ, система мониторинга событий информационной безопасности

1. Тенденции развития угроз информационной безопасности в мире

В современном мире, где цифровые технологии все глубже проникают во все сферы нашей жизни, вопрос информационной безопасности становится все более актуальным. В постпандемическом мире гибридный режим работы (сочетание работы в офисе и удаленной работы) стал не только нормой, но и предпочтительной ситуацией для многих. Эта среда, стремительное внедрение новых технологий, повсеместная цифровизация бизнес-процессов приводят к появлению новых возможностей и расширению площади атаки, представляют собой уникальные и обширные возможности для киберпреступников.

Анализ современных исследовательских работ и аналитических отчетов, в том числе, таких вендоров как McAfee, Trend Micro, Лаборатории Касперского позволяет определить основные тренды развития угроз информационной безопасности на ближайшее будущее.

Первой и, пожалуй, наиболее значимой тенденцией (по мнению автора) является увеличение количества и уникальности кибератак. Бурное развитие технологий позволяет злоумышленникам все эффективнее и умнее атаковать информационные системы. Они могут использовать дефекты и уязвимости в программном обеспечении, социальную инженерию, фишинг и множество других методов для первоначального доступа внутрь ИТ-инфраструктуры организации. Такие атаки могут иметь огромные последствия не только для организаций, но и для обычных граждан.

Второй важной тенденцией является усиление международного характера киберугроз. Если ранее кибератаки в основном проводились отдельными группами хакеров или киберпреступниками, то сегодня наблюдается возрастающая активность со стороны государств и преступных структур. Киберпространство стало новым полем для информационной войны, шпионажа и манипулирования общественным мнением.

Третьей тенденцией является распространение шпионского ПО. С появлением и развитием мобильных устройств и интернета вещей, доступ к информации становится все шире и глубже. Злоумышленники активно используют шпионское ПО для получения доступа к частной информации пользователей, воровства личных данных, финансовых мошенничеств и других преступлений в сфере кибербезопасности. Данная тенденция создает серьезные угрозы для безопасности как отдельных личностей, так и организаций.

Четвертой тенденцией является развитие кибервоенных технологий. Современные войска все больше осознают значимость киберпространства и инвестируют в развитие кибервойск. Это включает в себя создание кибероружия, массовых атак на крупные информационные системы противника, разработку специализированных программ для ведения информационной войны. Такие разработки могут иметь серьезные последствия для сферы обороны, политики и экономики государства.

И наконец, пятой тенденцией является развитие атак на цепочки поставок, в рамках которых злоумышленники проникают в инфраструктуру целевой организации через сторонние компании. Как правило, данные атаки осуществляются по двум направлениям: атаки поставщиков услуг или подрядчиков, которые сотрудничает с целевой организацией, либо атаки на разработчиков программного обеспечения, когда в продукт внедряется вредоносный код, который вместе с легитимным софтом попадает внутрь ИТ-инфраструктуры целевой организации.

При этом, стоит отметить, что позиция вендоров касательно важности тех или иных тенденций различаются. Так, McAfee [1], [2] в первую очередь акцентирует внимание на безопасность личных данных пользователей, кибергигену внутри семьи, защиту

мобильных устройств (общий тренд на защиту от шпионского ПО) и облачных технологий.

Trend Micro [3] рекомендует сконцентрироваться вокруг защиты гибридного режима работы пользователей (постоянное перемещение рабочих устройств между зонами безопасности: от защищенного офисного помещения до общей домашней сети), а также в отношении информационной безопасности поставщиков услуг (разработка программного обеспечения, услуги IaaS/SaaS).

Отчеты Лаборатории Касперского [4] указывают на уязвимости в ПО как на одну из основных угроз, что при дальнейшем развитии атаки приводит к утечкам чувствительной информации. Кроме того, компания отмечает увеличение количества вирусов-вымогателей.

Вместе с тем, стоит отметить, что прогнозирование трендов развития является достаточно сложной задачей. Тем не менее, основываясь на огромных объемах информации, которой обладают перечисленные выше вендоры (о различных видах вирусного программного обеспечения, типах атак, наиболее часто используемых злоумышленниками тактиками и техниками, особенностями активных хакерских группировок), а также используя методы ретроспективного анализа, можно делать те или иные предположения и прогнозы.

2. Трудности выявления атак на ИТ-инфраструктуру организаций, использующих уязвимости в программном обеспечении

Одним из часто используемых методов первоначального проникновения в ИТ-инфраструктуру организаций является использование уязвимостей в программном обеспечении, в том числе 0-day уязвимостей, особенно на ресурсах доступных из сети Интернет. При этом выявление подобных атак, является сложной задачей, даже при наличии в организации максимально возможных средств защиты подобных ресурсов: Систем периметральной защиты, Межсетевых экранов уровня приложений, Систем предотвращений вторжений и, в том числе, и Систем мониторинга событий информационной безопасности.

Ниже перечислены несколько причин, обосновывающие сложность в выявлении таких.

1. Отсутствие обновлений: 0-day уязвимости — это те, которые еще неизвестны производителям программного обеспечения, в отличие от киберпреступников, которые денные уязвимости целенаправленно выискивают.

2. Отсутствие сигнатур: Средства защиты информации, как правило, используют сигнатуры, основанные на известных уязвимостях, техниках и инцидентах для обнаружения атак. Однако, если атака использует новую уязвимость или до сих пор неизвестные методы (в том числе поведенческие), сигнатуры могут не сработать, и атака может остаться незамеченной.

3. Сложность выявления: Атаки на ИТ-инфраструктуру могут быть изощренными и сложными для обнаружения. Злоумышленники могут использовать различные методы для скрытия своей активности, маскировки трафика или использовать специализированные инструменты, которые затрудняют обнаружение.

4. Объем данных: Огромное количество данных из различных источников – средств защиты информации и элементов ИТ-инфраструктуры, включая журналы безопасности, трафик с сетевых устройства – все это значительно увеличивает время отклика систем мониторинга, а также количество ложных срабатываний, что, в свою очередь может приводить к пропуску атак.

5. Ложные срабатывания: Средства защиты информации могут срабатывать на ложные события или нормальную и повседневную пользовательскую активность, что может быть ошибочно идентифицировано как атака. Что, в свою очередь может вести к массовым ложным срабатываниям и перегрузке команды безопасности.

3. Исследование подходов к выработке правил корреляции для выявления атак с использованием ретроспективного анализа

С учетом изложенных выше проблем, при выявлении соответствующих атак, предлагается рассмотреть возможные их решения.

Опишем основные шаги выявления инцидента информационной безопасности.

1. Получение события информационной безопасности – фиксирование некоторого действия, которое представляет из себя интерес с точки зрения информационной безопасности (например, «Вход пользователя в систему»).

2. Выявление нарушения политики информационной безопасности организации – фиксирование некоторого действия (набора действий), которое представляет из себя нарушение существующих в организации правил/процедур (например, в конце рабочего дня пользователь должен разлогиниться из системы, соответственно отсутствие события «Выхода пользователя из системы», при наличии события «Вход пользователя в систему» может являться нарушением политики).

3. Выявление нарушения информационной безопасности – фиксирование некоторого действия (набора действий), которое представляет из себя нарушение существующих в организации правил/процедур и могут привести к некоторым негативным последствиям для организации.

4. Выявление инцидента информационной безопасности – фиксирование некоторого действия (набора действий), которое представляет из себя нарушение существующих в организации правил/процедур, которые привели к некоторым негативным последствиям в организации (т.е. к ущербу).

5. Выявление киберпреступления (в данной работе мы не рассматриваем переход инцидента в киберпреступление, поэтому описание предоставлено справочно) – фиксирование некоторого действия (набора действий), которое представляет из себя нарушение существующих в организации правил/процедур, которые привели к некоторым негативным последствиям в организации (т.е. к ущербу), а у субъекта, совершившего соответствующие действия, был мотив.

Ключевую роль в выявлении инцидентов информационной безопасности играют Системы мониторинга событий информационной безопасности, которые консолидируют информацию от различных источников событий, обрабатывают ее и с помощью правил корреляции выявляют соответствующие нарушения политик информационной безопасности. Выявление инцидентов информационной безопасности осуществляется к в онлайн режиме (на потоке поступающих событий), так и в

ретроспективе (по событиям, которые ранее поступили в систему и уже в ней хранятся какое-то время). При этом, когда речь идет о ретроспективном анализе, как правило подразумевают поиск инцидентов по следующим индикаторам компрометации: IP адреса, URL-ссылки, Hash, Email-адреса. Вместе с тем, для выявления атак, связанных с использованием уязвимостей в программном обеспечении данные индикаторы являются малоинформативными и как правило под каждую уязвимость необходима индивидуальная разработка правил, включая [5]:

1) изучение уязвимости (эксплоитов, при их наличии), выявление индикаторов компрометации;

2) определение логики правила корреляции;

3) определение перечня событий, в которых могут встречаться индикаторы компрометации;

4) разработку правил и их тестирование.

В среднем на весь цикл разработки правила корреляции под одну уязвимость требуется от 3-5 рабочих дней. При десятках тысячах уязвимостей в год данная задача является очень трудоемкой (даже если рассматривать только уязвимости на ИТ-инфраструктуре, доступной из сети Интернет).

4. Направления дальнейших исследований в целях совершенствования механизмов по выявлению атак на ИТ-инфраструктуру через ретроспективный анализ событий информационной безопасности

Учитывая высокую трудоемкость задачи по разработку правил корреляции, направленных на выявление атак с использованием уязвимостей в программном обеспечении предлагается следующий вариант ее оптимизации.

1. Использование алгоритмов машинного обучения для автоматического сбора данных об уязвимостях, последующий их анализ и парсинг в целях вычленения индикаторов компрометации. Это позволит повысить охват исследуемых неструктурированных данных при сборе аналитической информации, а также значительно снизит трудозатраты на изучение уязвимостей. В дальнейшем развитие данного направления позволит также выявлять образцы поведения злоумышленников, которые могут быть упущены при традиционных методах анализа.

2. Использование универсальных средств разработки правил (например проект Sigma) [6]. Это унифицированный механизм описания правил корреляции, который позволяет разрабатывать правила, используя унифицированный синтаксис, а затем с помощью специального конвертера получить правило в синтаксисе поддерживаемой SIEM-системы. Это позволит минимизировать трудозатраты как на определении логики правил, так и на разработку правил под конкретные SIEM системы (а в случае необходимости и их миграцию).

3. Применение аналитики поведения пользователей: использования паттернов из систем анализа поведения пользователей в информационной среде, в качестве базового элемента при разработке правил корреляции событий информационной безопасности. Например, может быть использована технология профилирования поведения пользователей, на которую уже будут накладываться различные сопутствующие события информационной безопасности. При этом, под поведением пользователя, с точки зрения ИТ-инфраструктуры следует рассматривать не только действия непосредственно работников организации под своими учетными записями, но и действия, выполняемые под сервисными учетными записями, в том числе, в автоматическом режиме. В данном случае выявление эксплуатации уязвимости предлагается рассматривать не через поиск индикаторов компрометации, характерных для данной уязвимости, а через призму поведения пользователя/службы/сервиса, которые не являются характерными для данной ситуации [7].

4. Оптимизации существующих алгоритмов поиска. Использование методов ретроспективного анализа является достаточно ресурсоемким, особенно в случае невозможности формализации индикаторов компрометации и их поиска не в нормализованных полях, а в сырых событиях, что в свою очередь требует наличие больших мощностей и оптимизированных алгоритмов поиска.

Литература:

1. Отчет McAfee об угрозах для мобильных устройств потребителей. – URL: https://media.mcafeeassets.com/content/dam/

npcld/ecommerce/en-us/docs/reports/rp-mobile-threat-report-feb-2023.pdf (дата обращения 26.10.2023).

2. Отчет McAfee киберзапугивание у всех на виду. – URL: https://media.mcafeeassets.com/content/dam/npcld/ecommerce/en-us/docs/reports/rp-cyberbullying-in-plain-sight-2022-global.pdf (дата обращения 26.10.2023).

3. Отчет об угрозах по электронной почте: Тактика киберпреступников, методы, которые необходимо знать организациям. – URL: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/annual-trend-micro-email-threats-report (дата обращения 26.10.2023).

4. Природа инцидентов информационной безопасности, Аналитический отчет. – URL: https://content.kaspersky-labs.com/se/media/ru/business-security/Analytical%20Report%20 Kaspersky%20IR_RU.pdf (дата обращения 01.09.2023).

5. *Королев И.Д., Попов В.И., Коноваленко С.А.* Методика аналитической обработки распределенных во времени инцидентов информационной безопасности // Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. № 5. – С. 53-61. – DOI: 10. 36724/2409-5419-2020-12-5-53-61. – URL: https://cyberleninka.ru/ article/n/metodika-analiticheskoy-obrabotki-raspredelennyh-vo-vremeni-intsidentov-informatsionnoy-bezopasnosti (дата обращения 01.09.2023).

6. Проект Sigma. – URL: https://github.com/SigmaHQ/sigma?ysclid=lonznn6tpr426357953 (дата обращения 01.09.2023).

7. *Беззатеев С.В., Елина Т.Н., Мыльников В.А., Ливщиц И.И.* Методика оценки рисков информационных систем на основе анализа поведения пользователей и инцидентов информационной безопасности // Научно-технический вестник информационных технологий, механики и оптики. – 2021. – Т. 21. № 4. – DOI: 10.17586/2226-1494-2021-21-4-553-561. – URL: https://cyberleninka.ru/ article/n/metodika-otsenki-riskov-informatsionnyh-sistem-na-osnove-analiza-povedeniya-polzovateley-i-intsidentov-informatsionnoy-bezopasnosti (дата обращения 01.08.2023).