5. *Лаврова Д.С., Зегжда Д.П., Зайцева Е.А.* Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам // Вопросы кибербезопасности. – 2019. – № 2 (30). – С. 13-20.

6. *Афанасьев М. Я., Федосов Ю. В., Крылова А. А., Шорохов С. А.* Организация киберфизических производственных систем с использованием технологий блокчейн и смарт-контрактов // Известия высших учебных заведений. Приборостроение. – 2019. – Т. 62. № 3. – С. 226-234.

Изотова И.А., Мысак М.Ю., Фейзов В.Р.

Технология кибербразведки как инструмент выстраивания проактивной защиты

Аннотация: Работа посвящена актуальной на сегодняшний день проблеме низкого уровня осведомленности организаций о технологии кибербразведки и вопросам применения данных о киберугрозах при выстраивании системы обеспечения кибербезопасности. В работе проанализированы методы применения данных кибербразведки в целях повышения уровня защищенности организации путем выстраивания проактивной защиты. Вопросы, изучаемые в работе, заинтересуют руководителей служб информационной безопасности (ИБ), а также центров мониторинга и реагирования организаций кредитно-финансового сектора.

Ключевые слова: кибербразведка, данные о киберугрозах, кибербезопасность, повышение уровня защищенности, кредитно-финансовый сектор

Современный мир невозможно представить без информационных технологий, и финансовая сфера не стала исключением. Пандемия лишь ускорила процесс цифровизации в кредитно-финансовом секторе, что сместило приоритеты в сторону дистанционного обслуживания клиентов и организации удаленных рабочих мест для сотрудников. Это было бы невозможно без достижений в области информационных технологий, которые стали неотъемлемой частью финансовых услуг. Распространение сфер

применения цифровых сервисов влечет необходимость пересмотра и усиления мер обеспечения кибербезопасности.

Только по информации Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) в 2020 году через Автоматизированную систему обработки инцидентов ФинЦЕРТ от участников информационного обмена в процессе информирования о компьютерных атаках было получено 968 сообщений о фактах распространения вредоносного программного обеспечения (ВПО), содержавших 1300 образцов ВПО [1]. Большинство случаев – распространение различного ВПО с использованием электронной почты. Сравнение структуры исследованного объема ВПО с данными 2019 года позволяет выделять смещение векторов применяемого ВПО. Своевременное выявление и реагирование на большое количество сложных направленных атак невозможно без глубокого изучения особенностей атаки и принятия соответствующих превентивных защитных мер. Проблема низкой осведомленности об актуальных угрозах распространена как внутри отдельных компаний, так и внутри всей отрасли. Несмотря на общий высокий уровень защищенности организаций финансового сектора, обмен и применение данных о киберугрозах развивается медленнее остальных направлений кибербезопасности.

К финансовым организациям Банком России предъявляется ряд требований, включая требования к содержанию базового состава мер защиты информации в соответствии со стандартом ГОСТ Р 57580.1-2017 «Защита информации финансовых организаций» [2]. Одной из целей указанного нормативного документа является достижение адекватности состава и содержания мер защиты информации, применяемых финансовыми организациями, актуальным угрозам безопасности информации и уровню принятого финансовой организацией операционного риска (риск-аппетиту). В целях выполнения указанных требований организации вынуждены обратить особое внимание на применяемые процессы мониторинга и реагирования на компьютерные атаки.

Стоит отметить, что в процессе реагирования на кибератаки, организации часто сталкиваются с проблемой повышенной нагрузки на работников, вызванной разбором инцидентов, созданных на основании некачественных и несвоевременно

поступивших данных. Кроме того, приходится тратить много времени на поиск и обогащение данных из инцидента дополнительным контекстом. Все это приводит к увеличению времени реагирования и снижению качества разбора инцидентов, являющихся реальными угрозами, увеличению числа ошибок первого и второго рода при принятии решения об актуальности угрозы, увеличению наносимого ущерба или даже к нарушению требований и сроков оповещения внешних регуляторов. Применение технологии кибербразведки позволяет применять знания об угрозах в целях автоматизации мониторинга и выстраивания проактивной защиты от целенаправленных атак, что снижает нагрузку на работников центра мониторинга и реагирования, облегчает процесс разбора инцидентов и минимизирует возможный ущерб.

Существуют три основных типа данных кибербразведки: стратегические, тактические и операционные. Все они важны при построении кибербезопасности и их грамотное применение помогает минимизировать затраты на реализацию системы обеспечения кибербезопасности при повышении общего уровня защищенности. Стратегические данные включают информацию о текущих тенденциях, целях и мотивации злоумышленников. Потребителями данной информации чаще являются руководство и топ-менеджмент организации. Тактические включают более подробную информацию о конкретных готовящихся или проводимых атаках, техники, тактики и процедуры атакующих. Потребителями тактических данных чаще являются Руководители служб ИБ, центров мониторинга и реагирования, работники ИТ-подразделений. Операционные включают в себя индикаторы компрометации и индикаторы конкретных атак. Потребителями такой информации являются работники центра мониторинга и реагирования.

Примерами собираемых данных кибербразведки служит следующая информация: индикаторы, включая хэш-суммы вредоносных файлов, IP адреса, домены, URL-адреса, артефакты, правила, инструменты, данные утечек, информация о злоумышленниках из новостей, отчетов и других доступных источников. Источниками получения данных могут являться:

- бюллетени внешних регуляторов;

- открытые сообщества обмена данными об угрозах;
- коммерческие потоки данных об угрозах;
- интернет, включая социальные сети;
- СМИ;
- внутренний трафик;
- собственные средства защиты информации;
- результаты разбора внутренних инцидентов.

Важно, чтобы данные о киберугрозах, поступающие от внешних источников, были актуальные, своевременные, точные и, желательно, обогащенные контекстом. При выборе источников стоит руководствоваться репутацией поставщика, анализировать его возможности по своевременному сбору и поддержанию актуальности данных кибербразведки, релевантности предоставляемых им данных к конкретной инфраструктуре и не стоит гнаться за количеством подключаемых источников и собранных данных. Хранение данных кибербразведки лучше реализовывать совместно с соответствующими контекстными данными. Данные, которые записываются об угрозах, в основном можно разделить на пять групп.

1. Информация об индикаторе:
   - тип;
   - значение;
   - дата добавления;
   - дата последнего обновления;
   - вес.
2. Счетчик срабатываний:
   - количество подтвержденных выявлений в инфраструктуре;
   - количество ложных срабатываний;
   - даты первого и последнего срабатывания.
3. Данные источника:
   - название источника;
   - название поставщика;
   - тип;
   - достоверность;
   - дата добавления;

– дата последнего обновления.

4. Контекст угрозы:

– название;

– категория;

– уровень критичности;

– даты первого и последнего упоминания об угрозе.

5. Дополнительная информация.

Отдельной сложной математической задачей является скоринг данных кибербразведки, зависящий от множества меняющихся во времени параметров, относящихся как к самой информации, так и к источнику, контексту угрозы: дата получения данных, достоверность источника, дата последнего обновления данных от источника, рейтинг, релевантность угрозы и т.д. Например, параметры индикаторов, являющихся хэш-суммой вредоносного файла (значение хэш-суммы файла со временем не изменяется), будут с течением времени изменяться иначе, нежели IP-адреса контрольно-командных серверов, которые злоумышленники склонны менять.

Для эффективного выстраивания проактивной защиты процесс кибербразведки необходимо имплементировать в действующие процессы обеспечения кибербезопасности, такие как управление уязвимостями, поиск угроз, мониторинг и реагирования на инциденты. Без должного уровня зрелости в организации перечисленных процессов внедрение технологии кибербразведки может быть неоправданным и не принести должного положительного эффекта.

В свою очередь, процесс кибербразведки является композицией следующих основных этапов [3]:

- этап планирования, включающий определение целей и требований к собираемым данным об угрозах;
- этап сбора актуальных данных, удовлетворяющих целям и требованиям, структурирования и нормализации данных;
- этап обработки, включая унификацию;
- этап подготовки данных;
- этап распространения.

После разбора составляющих процесса кибербразведки встает вопрос о механизмах автоматизации обработки данных об угрозах.

Неспециализированные инструменты обмена данными об угрозах, такие как электронные таблицы, почта и др. не могут обеспечить требуемого уровня гибкости. Threat Intelligence Platform (TIP) или платформа кибербразведки позволяет собирать, нормализовать, коррелировать и анализировать данные об угрозах, полученные из различных источников. В статьях [4,5] выполнен сравнительный анализ основных платформ обмена данными о киберугрозах. При выборе платформы необходимо руководствоваться требованиями и потребностями конкретной организации. В случае наличия большого числа потребностей, не закрывающихся продуктами, представленными на рынке, стоит рассмотреть возможность разработки собственной платформы кибербразведки.

Внедрение платформы кибербразведки даст следующие основные преимущества:

- обеспечение единой точки управления данными кибербразведки всех типов;
- использование данных об угрозах в процессе мониторинга;
- повышение эффективности работы средств защиты за счет предоставления актуальных данных;
- обогащение контекстом, ведущее к облегчению принятия решения относительно реакции на угрозу или потенциальную угрозу;
- раннее выявление подозрительной сетевой и хостовой активности.

Таким образам, знания об актуальных угрозах, методах и инструментах злоумышленников позволяют выстраивать систему обеспечения кибербезопасности с учетом оценки релевантности угроз для конкретной отрасли и региона, приоритизировать риски и выстроить проактивную защиту от актуальных угроз. Выявление кибератак на ранних стадиях поможет значительно снизить, а то и вовсе предотвратить нанесение ущерба организации.

Литература:

1. Банк России. Основные типы компьютерных атак в кредитно-финансовом секторе в 2019-2020 годах. – URL: http://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf (дата обращения 10.10.2021).

2. Стандарт Банка России ГОСТ Р 57580.1-2017 «Защита информации финансовых организаций». – URL: https://docs.cntd.ru/document/1200146534 (дата обращения 11.10.2021).

3. *Туманов Д., Абрамов Е.* Разработка системы анализа и верификации индикаторов компрометации (IoC) / Материалы 12-й Международной научной конференции «Безопасность информации и компьютерных сетей» (SIN 2019). – Сочи: Сочинский государственный университет, 2019. – С. 54-57.

4. Краткий анализ рынка Threat Intelligence Platforms . – URL: http://www.volgablob.ru/blog/?p=1842 (дата обращения 08.10.2021).

5. *Вульфин А.* Система управления данными киберразведки // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9. №(1). – С. 1-18.

Фейзов В.Р.

Цветные революции и безопасность коммуникаций и данных в условиях существования современных олигополий

Аннотация: Интенсивный процесс перехода человечества к цифровому обществу позволил реализовать множество возможностей, одновременно с положительным эффектом возникли как новые этические вопросы, так и угрозы политического характера. В работе рассматриваются некоторые аспекты потенциально возможного деструктивного воздействия транснациональных корпораций на граждан и политическую систему отдельных стран. Рассмотренные в работе вопросы могут заинтересовать специалистов по защите информации и информационной безопасности.

Ключевые слова: цветные революции, безопасность данных, средства массовой информации, социальные сети, рекомендательные системы

В настоящее время проводится большое количество исследований посвященных анализу проблем, связанных с демонтажом политических режимов в современных государствах и ролью в этом процессе технологий цветных революций. Еще не так