Исследование возможности разработки системы автоматизированного анализа компьютерных инцидентов

А. П. Теленьга, email: telenga@mail.ru
Н. С. Евсеенков, email: Sailor797@yandex.ru

Краснодарское высшее военное орденов Жукова и Октябрьской Революции краснознамённое училище имени генерала армии С.М. Штеменко

Аннотация. *Рассматриваются понятия автоматизированного анализа инцидентов информационной безопасности и его преимущества. Приводится описание прецедентного анализа, его архитектура и математическое представление.*

Ключевые слова: *автоматизированная система, информационная безопасность, прецедентный анализ, инцидент, прецедент.*

Введение

Важнейшей чертой нашего времени является всеобщее информационное слияние сетей, заложенное на построении компьютерных сетей в огромном масштабе на уровне предприятия и их объединение через Интернет.

Сложность организации сетей приводит к различным трудностям при решении задач защиты сетей и управления. В результате использования компьютерных сетей администраторам необходимо защищать сетевые ресурсы от несанкционированной деятельности злоумышленников, воздействий вредоносного программного обеспечения и т.п., т.е. обеспечивать их целостность, доступность и конфиденциальность.

При решении данной задачи главным вопросом является своевременное выявление состояний сети, приводящих к частичной или полной потере её работоспособности, искажению, уничтожению или краже информации, являющихся следствием сбоев случайного характера, отказов или результатом получения злоумышленником несанкционированного доступа к сетевым ресурсам и других угроз информационной безопасности. Быстрое обнаружение таких состояний дает возможность администраторам своевременно предотвратить возможные критические последствия, а также выявить и устранить их причину.

Для их обнаружения используют различные варианты специализированных систем, одна из таких является система обнаружения атак, в основе которой заложены принципы прецедентного анализа.

1. Автоматизированный анализ компьютерных инцидентов.

Целесообразно сразу отметить, что мы будем придерживаться терминологии в рамках выписки из концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации утвержденная Президентом Российской Федерации от 12 декабря 2014 г. № К 1274, а именно п.20 б)

Начнем с определений. Чтобы понять, что такое автоматизированный анализ, для начала рассмотрим сам процесс добычи информации, ее нормализации и непосредственно анализа. Вопрос автоматизированного анализа является актуальным, так как с всё большим объемом данных нужны более продвинутые технологии для обработки информации, и человек сам уже не может справиться без участия средств автоматизации.

Автоматизация – одно из направлений научно-технического прогресса, использующее саморегулирующие технические средства и математические методы с целью освобождения человека от участия в процессах получения, преобразования, передачи и использования энергии, материалов, изделий или информации, либо существенного уменьшения степени этого участия или трудоёмкости выполняемых операций.

Теперь вернемся к вопросу, что же из себя представляет анализ компьютерных инцидентов. Согласно Федеральному закону от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", ст. 2 компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки; Исходя из этого анализ компьютерных инцидентов – это ряд технических мероприятий, направленный на предупреждение, предотвращение, а также расследование аномальных действий в информационной системе, с целью выявить угрозу, которая может нанести существенный ущерб организации, а также деятельность злоумышленников, пытающаяся

добыть информацию и в дальнейшем использовать её в своих корыстных целях.

Для выявления компьютерных инцидентов в виде сетевых атак используют захват и хранение своего же трафика через так называемые брокеры сетевых пакетов. Они направляют трафик в системы индексации сетевых пакетов, таких как Arkime, в которых в дальнейшем мы сможем наблюдать всю активность в нашей сети. На рис.1 показаны подзадачи системы анализа сетевого трафика.

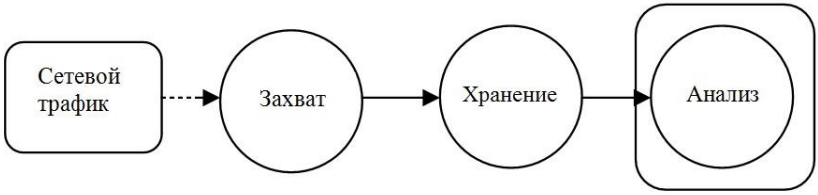

Рис. 1. Подзадачи системы анализа сетевого трафика.

После захвата и записи сетевого трафика мы должны провести его анализ для выявления аномалий и поиска вредоносной активности внутри содержимого сетевых пакетов. Существует большое количество разных подходов, но у всех них есть ряд фактов, показывающий, что без средств автоматизации никак не обойтись:

1. Объем данных. Если над процессом анализа работает только человек, то очевидно, что справиться с таким потоком данных он может только при больших временных затратах, что приводит к снижению эффективности информационной безопасности.
2. Потребность в высококвалифицированных специалистах. Для анализа трафика информационной системы и выявления компьютерных инцидентов без участия автоматизации нужны высококвалифицированные работники, хорошо разбирающимися во многих аспектах ИБ, что влечет дополнительные финансовые затраты.

На сегодняшний день уже создано большое количество различных программных продуктов, которые могут выступать как в роли системы поддержки принятия решений, так и осуществлять автоматизированный анализ событий информационной безопасности.

Рассмотрим типовую архитектуру системы анализа трафика, представленную на рис.2.

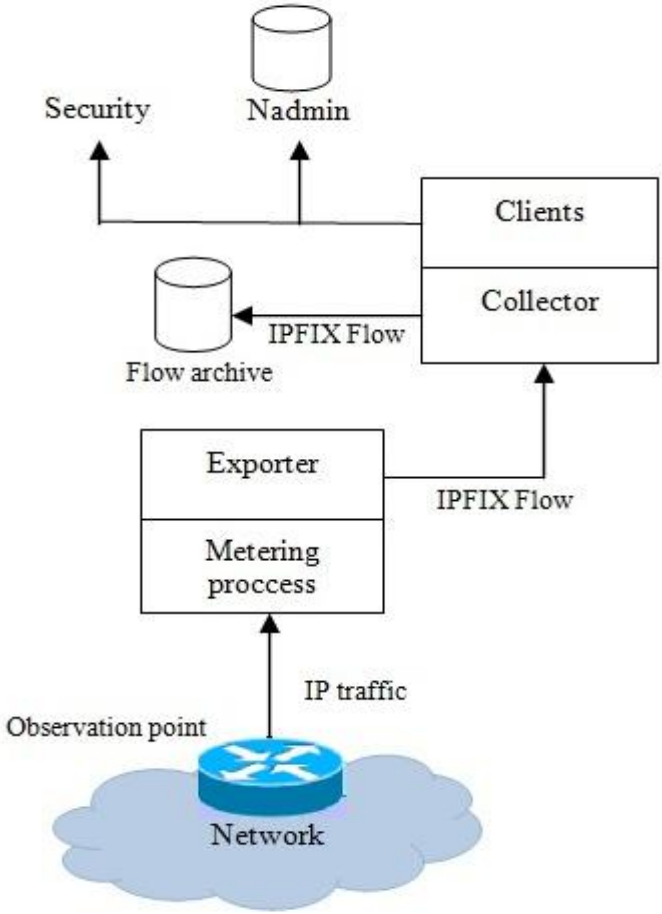

Рис. 2. Архитектура системы анализа трафика.

В ней можно выделить процессы измерения трафика, сбора сетевых потоков и параллельного анализа средствами безопасности и сетевого управления. Опираясь на неё, можно построить систему автоматизированного анализа компьютерных инцидентов.

2. Подходы к автоматизированному анализу компьютерных инцидентов.

Существует несколько путей обнаружения инцидентов и их предотвращения. В данной статье мы затронем подробнее прецедентный

анализ. Данный вопрос считается актуальным, так как на данный момент есть ряд проблем, связанные с оперативным реагированием на возникающие инциденты, а именно:

- не всегда классификация инцидентов средствами защиты производится корректно (ошибки 1-го и 2-го рода);
- по мере развития ИТ-инфраструктуры выявляются новые типы ранее неизвестных инцидентов, которых нет в базе прецедентов;
- нет единого решения реагирования для происшествий определенного класса, так как каждый инцидент является индивидуальным.

Для решения этих проблем мы будем использовать метод правдоподобного рассуждения, который позволит решить проблему реагирования на инциденты путем применения систем на основе прецедентов (Case-Based Reasoning, CBR) в качестве интегрированных средств автоматизации процесса управления. Рассмотрим, что из себя представляет прецедентный анализ.

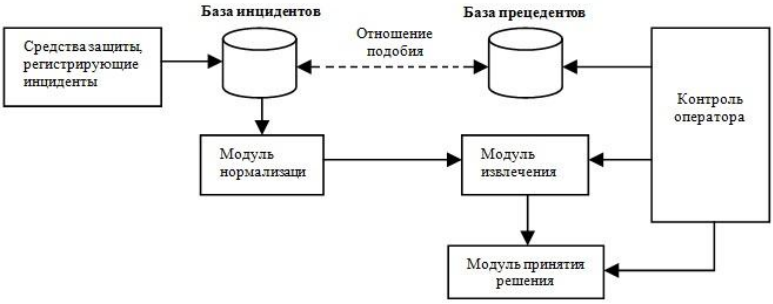

Рис. 3. Архитектура системы прецедентного анализа.

В данной архитектуре можно выделить 5 компонентов, а также процессов, которые будут происходить при обнаружении происшествия:

1. База инцидентов, хранение в себе происшествий, которые ожидают обработку.
2. Модуль нормализации, процесс преобразования зарегистрированных инцидентов в соответствии с базой прецедентов.
3. Модуль извлечения, происходит расчет сходства инцидентов и прецедентов.

4. Модуль принятия решений, определяется результат прошедших двух пунктов выше, если инциденту соответствует один или несколько прецедентов, тогда на этот случай будет уже готовый сценарий решения угрозы, в противном случае, возникают так называемые аномалии, для решения которых, нужен более углубленный анализ с участием человека.
5. Консоль оператора, коррекция процесса анализа и адаптации выработанной стратегии под ранее неизвестные условия.

Также прецедентный анализ можно представить в виде математической модели, основная идея которой заключается в функции подобия, в которой определяется сходство инцидента и прецедента.

Тогда прецедент будет выглядеть в следующем образе

$$CASE = \left(x_1, x_2, ..., x_p, R \right) \tag{1}$$

где $x_1, x_2, ..., x_p$ – параметры, описываемой данным прецедентом;

R – одно или несколько решений данной угрозы.

Извлечение прецедентов основополагается на определении функции подобия F, значение которой определяет схожесть прецедента и текущей ситуации. В пространстве признаков определяется точка, соответствующая целевой проблеме, и в рамках используемой метрики выбирается ближайший прецедент. Формально аналогия прецедента $g = (x_{g1}, x_{g2}, ..., x_{gp})$ и текущей ситуации $k = (x_{k1}, x_{k2}, ..., x_{kp})$ описывается функцией вида

$$SIM\ (g, k) = F\left(sim\left(x_{g1}, x_{k1} \right), ..., sim\left(x_{gp}, x_{kp} \right) \right) \tag{2}$$

где $sim\left(x_{gi}, x_{ki} \right)$ – локальная схожесть значений i-го признака прецедента g и i-го признака текущей ситуации (инцидента) k. Функция F выражает полную схожесть прецедента с текущей ситуацией.

С учетом происшествий, которых нет в стратегии реагирования, прецедентный анализ сводится к классификации инцидентов на нормальные и аномальные, исходя из количества найденных аналогий: $G = \{ g_1, ..., g_n \}$ – множество прецедентов; $g_i = (x_1, ..., x_p, r)$ – единичный прецедент; $K = \{ K_1, ...K_m \}$ – множество зарегистрированных

инцидентов; $k_j = (x_1, ..., x_p)$ – единичный инцидент; $F(g_i, k_j)$ – функция подобия; $G_l = \{ g_i : F(g_i, k_j) \le d_{\lim} \}$ – множество подобных прецедентов. Таким образом, условие отнесение инцидента к множеству прецедентов формулируется следующим образом: $k_j \in G \Leftrightarrow G_l \ge p_{\lim}$. Как видно, результат классификации напрямую зависит от предельного расстояния $d_{\lim}$ и предельного количества аналогий $p_{\lim}$.

Заключение

Таким образом, рассмотренная возможность применения прецедентного анализа и его автоматизации при реализации различных стратегий реакции на выявленные инциденты информационной безопасности позволяет нам накапливать базу прецедентов, что впоследствии сокращает время поиска решения для последующих аналогичных происшествий, а также снижает вмешательство человека в процедуру анализа компьютерных инцидентов, тем самым уменьшая риски ошибок 1-го и 2-го рода и повышая защищенность информационной системы в целом.

Литература

1. Маркин Ю. В. Обзор современных инструментов анализа сетевого трафика. / Ю. В. Маркин, А. С. Санаров // Препринты ИСП РАН – 2014 – № 27.

2. Жуков В. Г. Прецедентный анализ информационной безопасности / В. Г. Жуков, А. А. Шаляпин. // Вестник СибГАУ –2013 – № 2 – С. 19-23.

3. Шаляпин А. А. Модельно-алгоритмическое обеспечение системы прецедентного анализа инцидентов информационной безопасности / А. А. Шаляпин // Решетневские чтения – 2015 – С. 304-306.