ных на снижение вероятности реализации угроз хакерских атак или ущерба от них;

– исключение возможности проведения атаки за счёт изменения схемы информационного потока и архитектуры информационной системы;

– минимизация негативного действия риска за счет применения мер по страхованию;

– уменьшение риска до таких значений, при которых он перестает представлять опасность для информационной системы.

Таким образом, внутренний аудит информационной безопасности организации является наиболее эффективным инструментом, позволяющим получить объективные сведения о текущем уровне защищенности информационной системы. План аудита информационной безопасности должен учитывать все возможные риски компрометации системы, только в этом случае экспертиза принесет реальную пользу.

Литература

1. АйТи. Система ИБ. Аудит ИБ [Электронный ресурс]. – Режим доступа: http://www.it.ru/services/sub/sud_detail.php?ID=383&SUB_ID=6916.

2. ProtectMi – лаборатория безопасности. Аудит и управление ИБ [Электронный ресурс] – Режим доступа: http://www.infosecurity.ru/iprotect/audit/

3. Ситнов А.А. Организация аудита информационной безопасности [Электронный ресурс]. – Режим доступа: https://accounting.fa.ru/jour/article/viewFile/129/130.pdf.

4. Аудит состояния информационной безопасности на предприятии [Электронный ресурс]. Режим доступа: https://www.intuit.ru/studies/professional_retraining/964/courses/419/lecture/9583?page=1

Д.И. Парфёнов, В.А. Торчин, Л.С. Забродина

РАЗРАБОТКА ПОДХОДА К ПОИСКУ УЯЗВИМОСТЕЙ В СЕТЯХ ПРОВАЙДЕРОВ ТЕЛЕКОММУНИКАЦИОННЫХ УСЛУГ

(Оренбургский государственный университет)

Развитие информационных технологий предполагает появление новых угроз и возникновение необходимости разработки новых подходов к обеспечению безопасности. Это особенно актуально для операторов связи и провайдеров телекоммуникационных услуг, являющихся ключевым звеном инфраструктуры передачи данных для любой компании. Для обеспечения защиты собственной инфраструктуры и сервисов провайдерам приходится применять не тривиальные решения [1]. Инфраструктура провайдеров телекоммуникационных услуг на сегодняшний день, как правило, строится на базе автономных систем, организованных на базе мультиоблачных платформ. Такой подход позво-

ляет изолировать потоки пользователей, и сократить возможный ущерб в случае проведения атак на конкретного пользователя [2]. Для защиты от внешних и внутренних угроз операторы связи активно используют комплексные системы управления информацией и событиями, для построения которых актуально использование SIEM-технологии (Security Information and Event Management) [3].

В рамках настоящего исследования разработан подход к поиску уязвимостей в сетях провайдеров телекоммуникационных услуг, построенный на основе анализа событий в журналах различных систем, в том числе отвечающих за сетевую безопасность.

Журналы сетевых событий являются одним из важнейших средств для анализа работы компьютерных сетей, в том числе и с точки зрения оценки защищенности сети. В сети провайдеров журнал сетевых событий Журнал сетевых событий представляют собой совокупность записей о произошедших обменах данных между узлами, а также об изменениях возникших в рамках взаимодействий как отдельных узлов, так целых сегментов.

В работе рассматривается два подхода к анализу журналов сетевых событий – построение графа атаки за счет реверсивного анализа сетевых событий и промежуточного анализа аномальной активности. Для дальнейшего рассмотрения подходов, необходимо ввести ряд моделей с целью формализации алгоритмов, лежащих в основе.

Журналы сетевых событий, как правило, представляют собой совокупность последовательностей отражающих изменения, происходящие в инфраструктуре провайдера телекоммуникационных услуг с течением времени и под воздействием определенных внешних или внутренних факторов. При этом сам набор этих факторов можно разделить на две большие группы не только по источнику их возникновения, но и по влиянию, оказываемому ими на сеть провайдера. К первой группе факторов относят события, не приводящие к негативным последствиям для сетевой и физической инфраструктуры. К ним как правило относят типовые технологические операции выполняемые в рамках повседневной деятельности провайдера по организации новых каналов связи и поддержания работоспособности существующих связей в динамически изменяющейся сетевой среде, за исключением действий, вызывающих аварийные ситуации. Ко второй группе факторов относят события, которые прямо или косвенно ухудшают, или наносят вред сетевой или физической инфраструктуры. К таким событиям, как правило, относят различные виды атак, а так же аварийные ситуации на сети.

Как правило, каждая информационная или сетевая система формирует собственный лог событий, отражающий действия пользователей или иных процессов, или компонентов, влияющих на ее работу. Тем не менее, все события, происходящие в сети, независимо от вида отражаются в журнале с соответствующей меткой времени. Такой способ записи позволяет в дальнейшем расследовать инциденты сетевой безопасности и определять затронутые узлы. На практике для корреляции событий, произошедших на различных узлах провайдеру необходимо агрегировать полученные данные в едином формате, содер-

жащем базовую информацию о произошедшем событии. Для операторов связи задача сбора сведений о сетевых взаимодействиях является нетривиальной, и требует отдельного рассмотрения для каждой конкретной системы. Поэтому в рамках настоящего исследования представим запись о событии в журнале в упрощенном виде, а именно в форме вектора z следующего вида:

$$z = \{date\_time, src\_ip, dst\_ip, protocol, src\_port, dst\_port, size\}, \quad (1)$$

где date_time – момент времени, в который произошло рассматриваемое взаимодействие; src_ip – ip-адрес источника сообщения; dst_ip – ip-адрес получателя сообщения; protocol – протокол, по которому осуществлялся обмен сообщениями; src_port – номер сетевого порта источника сообщения; dst_port – номер сетевого порта получателя сообщения; size – размер пакета.

Тогда множеством $Z = \{z_1, \ldots, z_n\}$ обозначим журнал сетевых событий за определенное время, где n – последовательный набор временных меток.

Одной из задач в рамках обеспечения безопасности сетевой инфраструктуры является поиск аномалий в журналах сетевых событий.

Как правило, для выявления аномалий в сетевой активности, провайдеры используют статистические данные, накопленные за различные периоды времени. На основе накопленных данных для каждого элемента, входящего в состав сетевой инфраструктуры провайдера строится модель профиля типовой активности. Для этого из журнала сетевых событий необходимо выбрать множество записей соответствующих только выбранному элементу сети. В рамках построенной модели журнала сетевых событий такую выборку можно представить в виде множества Z_k

$$Z_k = \{z_1, \ldots, z_m\}, \forall z_j : src\_ip_j = a_k \vee dst\_ip_j = a_k \quad (2)$$

Обобщая статистически данные для каждого узла, получаем множество, которое обозначим за C_k.

Исходя из определения множества C_k, аномальную активность можно обозначить в виде множества, состоящего из записей, не подходящих к типовым профилям пользователей, формально обозначаемо в следующем виде:

$$z_r : src\_ip_r = a_k \vee dst\_ip_r = a_k, z_r \in Z \wedge z_r \notin C_k. \quad (3)$$

Построенную модель поиска аномального трафика, рассмотренную выше, можно использовать двумя способами:

-рассмотреть построение графа атаки для уже известного инцидента безопасности;

-произвести рассмотрение аномальной активности пользователей за некоторый период времени.

Работа выполнена при финансовой поддержке РФФИ проект № 18-07-01446, гранта Президента Российской Федерации для государственной поддержки молодых российских ученых — кандидатов наук (МК-860.2019.9), а так же Министерства образования Оренбургской области в рамках НИР "Интеллектуальная система идентификации источников и прогнозирования распространения инцидентов кибербезопасности для адаптивного управления механизмами защиты в среде провайдеров телекоммуникационных услуг".

Литература

1. Дойникова Е. В., Котенко И. В. Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер // Тр. СПИИРАН. — 2018. — №2 (57). — С. 211–240.

2. Парфенов Д. И. Архитектура прототипа автономной системы обеспечения кибербезопасности и качества обслуживания программно-управляемой инфраструктуре мультиоблачной платформы [Электронный ресурс] / Парфенов Д. И., Дедюрин В. В., Шардаков В. М. // Университетский комплекс как региональный центр развития образования, науки и культуры : материалы Всерос. науч.-метод. конф., 31 янв.-2 февр. 2018 г., Оренбург / М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования "Оренбургский гос. ун-т". - Электрон. дан. - Оренбург: ОГУ,2018. - . - С. 1834-1837. . - 4 с.

3. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. — 2016. — № 2 (45). — С. 207 – 244.

К.В. Пензин, Л.С. Зеленко

ФУНКЦИОНИРОВАНИЕ ПОДСИСТЕМЫ ФОРМИРОВАНИЯ ОТЧЕТОВ В СОСТАВЕ ПРОГРАММНОГО КОМПЛЕКСА «МОНИТОРИНГ ГОТОВНОСТИ»

(Самарский национальный исследовательский университет
имени академика С.П. Королёва)

Программный комплекс (ПК) «Мониторинг готовности» предназначен для автоматизации расчета показателей ПАО «РусГидро» и обеспечивает их сравнения со значениями, рассчитанными системным оператором единой энергетической системы России и загружаемыми с сайта балансирующего рынка.

ПК «Мониторинг готовности» реализован в виде web-приложения с трехзвенной клиент-серверной архитектурой. Серверная часть реализована на языке C# и работает под управлением СУБД Microsoft SQL Server 2014. Клиентская часть приложения реализована с использованием языков TypeScript и JavaScript.

Подсистема формирования отчетов интегрирована в ПК «Мониторинг готовности» с целью улучшения наглядности представления результатов расчетов показателей готовности, а также предоставления пользователям возможности формирования собственных представлений данных и отчетных форм.

Редактирование отчетов в ПК доступно администраторам со страницы «Шаблоны отчетных форм». Она предоставляет возможность редактирования перечня шаблонов (см. рисунок 1), а также отдельных отчетов. На рисунке 2 представлен пример задания параметров отчета.