УДК 004.416.6

ИСПОЛЬЗОВАНИЕ СИСТЕМ МОНИТОРИНГА СЕТИ ДЛЯ ОБНАРУЖЕНИЯ УСТРОЙСТВ

Копытов А.М., магистрант гр. ПИм-241, II курс
Научный руководитель: Пимонов А.Г., д.т.н., профессор
Кузбасский государственный технический университет имени Т.Ф. Горбачева
г. Кемерово

В современной цифровой среде локальная вычислительная сеть (ЛВС) является фундаментальной основой функционирования любого предприятия или образовательного учреждения [1]. С ростом количества подключенного оборудования остро встает проблема контроля сетевого периметра и информационной безопасности[2]. Особую актуальность данный вопрос приобретает в учреждениях со строгим регламентом доступа к сети Интернет, таких как кадетские корпуса, школы-интернаты и предприятия полузакрытого типа. В подобных инфраструктурах одной из главных угроз безопасности является использование несанкционированного оборудования (концепция Shadow IT – «теневые ИТ»), когда пользователи самовольно подключают личные маршрутизаторы, коммутаторы или портативные компьютеры к корпоративной сети.

Традиционные методы контроля доступа, такие как привязка по MAC-адресам (Port Security) или внедрение протокола 802.1X, требуют значительных административных ресурсов на этапе развертывания и поддержки, а также не всегда поддерживаются бюджетным коммутационным оборудованием уровня доступа. В связи с этим возникает необходимость разработки альтернативных, проактивных методов выявления сторонних устройств[3]. Целью данного исследования является обоснование и практическая реализация алгоритмов использования систем ИТ-мониторинга для автоматизированного обнаружения несанкционированных подключений в корпоративной сети.

В качестве инструментария для реализации поставленной задачи представляется целесообразным использовать программный комплекс корпоративного уровня Zabbix[4]. Выбор обусловлен открытым исходным кодом системы (Open Source), что исключает финансовые затраты на лицензирование, а также глубокой поддержкой протокола SNMP (Simple Network Management Protocol), позволяющего осуществлять безагентный сбор телеметрии с сетевого оборудования.

Внедрение системы мониторинга невозможно рассматривать в отрыве от организационных изменений. Для оценки эффективности предлагаемого решения было проведено моделирование бизнес-процесса «Управление сетевыми инцидентами» в двух состояниях: базовом «AS-IS» (существующий процесс) и целевом «TO-BE» (процесс после внедрения автоматизации).

Анализ процесса «AS-IS» показал, что до внедрения автоматизированного мониторинга ИТ-отдел работал по устаревшей реактивной модели. Триггером (начальным событием) для запуска процесса восстановления сети служила жалоба конечного пользователя. Типовой сценарий включал в себя следующие действия: обнаружение проблемы пользователем, телефонное оповещение администратора, выезд специалиста на объект, ручной поиск неисправного узла методом перебора и только затем устранение проблемы. Данная модель характеризовалась высоким временем реакции (MTTR) и невозможностью фиксации кратковременных нарушений безопасности, так как пользователи не сообщают о собственных попытках обхода ограничений. Схема данного процесса представлена на рисунке 1.

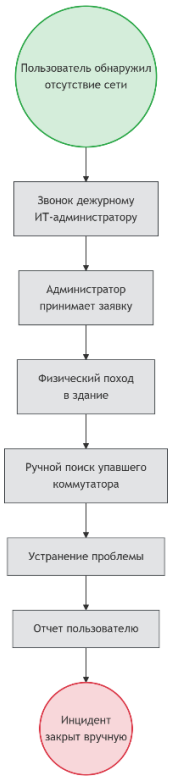

Рисунок 1 - Модель бизнес-процесса управления инцидентами «AS-IS» (реактивная модель)

После развертывания системы Zabbix архитектура бизнес-процесса трансформировалась в модель «TO-BE». Инициатором процесса теперь выступает не человек, а система мониторинга. При фиксации аномалии (падение линка, всплеск трафика) система автоматически формирует инцидент и уведомляет администратора через защищенные каналы внутренней связи. Специалист получает заявку уже с локализованной точкой сбоя (номер порта, номер коммутатора, этаж), что исключает этап ручного поиска. Целевая схема процесса представлена на рисунке 2.

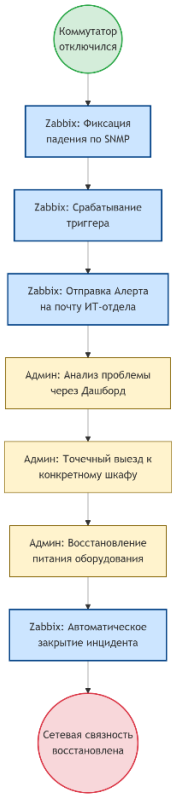

Рисунок 2 – Целевая модель бизнес-процесса управления инцидентами «TO-BE» (проактивная модель)

Техническая реализация обнаружения сторонних устройств в модели «TO-BE» базируется на косвенном анализе изменения состояния портов и аномалиях сетевого трафика. В ходе исследования была смоделирована архитектура сети, состоящая из ядра, межсетевого экрана и коммутаторов Hewlett Packard серии 1820, подключенных к серверу Zabbix версии 4.4.

Первым и наиболее эффективным методом обнаружения несанкционированных манипуляций с оборудованием является контроль метрики изменения состояния физического интерфейса коммутатора (Link Up / Link Down), известной как Port Flapping (нестабильность линка). В условиях образовательного учреждения попытка подключения стороннего устройства чаще всего сопровождается физическим извлечением кабеля (патч-корда) из авторизованного стационарного компьютера и его последующим подключением в личный ноутбук или Wi-Fi роутер пользователя.

Для автоматического выявления данного паттерна в системе Zabbix был разработан специализированный триггер, анализирующий оперативный статус порта (ifOperStatus). Логическое выражение триггера имеет следующий вид: `{Host:net.if.status[ifOperStatus.10].count(5m,2)}>3`. Данный метод позволяет выявить момент подмены устройства еще до того, как новое оборудование получит IP-адрес по протоколу DHCP.

Вторым методом обнаружения устройств выступает темпоральный анализ сетевого трафика (анализ на основе времени). Пользователи, подключаю-

щие несанкционированные маршрутизаторы для создания скрытых беспроводных сетей (Wi-Fi), генерируют нетипичный профиль нагрузки. Формализованное выражение для обнаружения аномального трафика выглядит следующим образом:

```
 {Host:net.if.in[ifInOctets.5].avg(5m)}>20M and
({Host:net.if.in[ifInOctets.5].time()}>223000 or
 {Host:net.if.in[ifInOctets.5].time()}<063000).
```

Если объем трафика превышает установленный порог (20 Мбит/с) строго в период регламентированного запрета на использование сети (с 22:30 до 06:30), администратору отправляется алерт.

Подводя итог проведенному исследованию, можно сделать вывод, что использование систем сетевого мониторинга обладает высоким потенциалом в сфере информационной безопасности. Разработанная модель, основанная на анализе состояний портов, темпоральном контроле трафика и внедрении бизнес-процесса «ТО-ВЕ», позволяет автоматизировать процесс обнаружения несанкционированных устройств без закупки дорогих аппаратно-программных комплексов[5].

Список литературы

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 6-е изд. – СПб.: Питер, 2020. – 1008 с.
2. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 2008-02-01. – М.: Стандартинформ, 2008. – 12 с.
3. Голицын А.В., Мельников В.П. Проактивные системы мониторинга как элемент корпоративной защиты // Информационные технологии и безопасность. – 2022. – № 4. – С. 45-51.
4. Официальная документация программного комплекса Zabbix 4.4. – URL: https://www.zabbix.com/documentation/4.4/ru/manual (дата обращения: 12.05.2024).
5. Бирюков А.А. Информационная безопасность: защита и нападение. 2-е изд. – М.: ДМК Пресс, 2017. -–434 с.