А.С. Южакова, Т.И. Паюсова

ФГАОУ ВО Тюменский государственный университет, г.Тюмень

УДК 004.056

ОРГАНИЗАЦИЯ СИСТЕМЫ ПРОАКТИВНОГО ПОИСКА УГРОЗ В ГАУ ТО "МНОГОФУНКЦИОНАЛЬНЫЙ ЦЕНТР ПРЕДОСТАВЛЕНИЯ ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ УСЛУГ В ТЮМЕНСКОЙ ОБЛАСТИ"

Аннотация. В статье описывается процесс организации и внедрения системы проактивного поиска угроз (Threat Hunting) в ГАУ ТО "Многофункциональный центр предоставления государственных и муниципальных услуг в Тюменской области" на базе ELK Stack.

Ключевые слова. Проактивный поиск угроз, Threat Hunting, ELK Stack, Elasticsearch, Logstash, Kibana.

Своевременное реагирование на угрозы является первостепенной задачей для специалистов по информационной безопасности. Построение комплексной системы защиты, состоящей из программных, аппаратных, организационных, криптографических и прочих элементов позволяет вовремя обнаруживать факты нападения и оказывать сопротивление злоумышленнику.

Но существует ряд угроз, которые не так легко обнаружить стандартными средствами защиты, например, атаки, построенные на уязвимостях “нулевого” дня, бэкдоры, APT-атаки, фишинг и др. По статистике подобные атаки занимают 5% от всего множества известных нападений, но именно эти 5% составляют 70% основных рисков информационной безопасности [1].

Для защиты от перечисленных 5% атак спасает процесс, который получил название Threat Hunting или проактивный поиск угроз. Threat Hunting позволяет обнаруживать нападения, которые не были зарегистрированы стандартными средствами защиты: IDS/IPS, брандмауэрами, антивирусами, SIEM, DLP и пр. Таким образом, проактивный поиск угроз осуществляется в “мирное время”, когда, казалось бы, системе ничего не угрожает, и ни одно из средств защиты не генерирует соответствующих предупреждений. Известны шуточные сравнения Threat Hunting с паранойей. Но, как известно, “если у вас паранойя, это не значит, что за вами не следят”.

Threat Hunting предполагает выдвижение гипотезы о том, что произошло нападение на систему, а далее происходит сбор доказательств для проверки гипотезы. Например, проверяется гипотеза о том, что сервер баз данных был скомпрометирован (при этом ни одно из средств защиты на это не указывает), затем осуществляется анализ лог-файлов, журналов событий, проводится поведенческий анализ действий пользователей, изучаются серверные скрипты и многое другое, чтобы доказать, что догадка о компрометации сервера является верной. Можно сказать, что проактивный поиск угроз объединил в себе приемы аудита, теста на проникновение и форензики.

Основными техниками Threat Hunting являются: базовый поиск, статистический анализ, визуализация, простые агрегации, машинное обучение и байесовские методы [2]. Все перечисленные подходы направлены на поиск доказательств сформулированной гипотезы. Источниками доказательств, например, выступают: сетевой и веб-трафик, лог-файлы, журналы событий, настройки программного обеспечения, исходные программные коды, данные из открытых источников, аномалии поведения пользователей и программ.

Компания MITRE разработала матрицу ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) (Рис. 1), содержащую описание техник атакующих и артефактов, которые остаются в системе-жертве после нападения. ATT&CK - один из самых известных и полезных инструментов для формулирования и проверки гипотез в процессе Threat Hunting [3]. Также многие другие компании, специализирующиеся на информационной безопасности, публикуют в открытых источниках свои отчеты по статистике нападений, результаты проведенных ими аудитов и тестов на проникновение. Эти материалы помогают лучше понимать логику злоумышленника и сценарии развития тех или иных атак, а также эффективнее осуществлять сбор доказательств для проверки гипотезы.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers

Рис. 1. Фрагмент матрицы ATT&CK

С технической точки зрения организация системы проактивного поиска угроз предполагает использование системы сбора данных с разнообразных источников и их анализ с помощью вышеуказанных техник Threat Hunting. Одним из возможных технических решений является стек ELK, состоящий из трех продуктов: Elasticsearch, Logstash и Kibana [4]. Logstash позволяет осуществить сбор данных, Elasticsearch – поиск данных, а Kibana ответственна за анализ данных и проведение аналитики (Рис. 2). Также для подключения к инфраструктуре Threat Hunting

конечных устройств возможно использование «легких» агентов Beats, аккумулирующих данные локально.

Рис. 2. Схема взаимодействия компонентов ELK Stack

Описанное программное решение на базе ELK Stack было реализовано и апробировано в ГАУ ТО "Многофункциональный центр предоставления государственных и муниципальных услуг в Тюменской области" (ГАУ ТО «МФЦ») для осуществления проактивного поиска угроз информационной безопасности. Система Threat Hunting была развернута в головном филиале ГАУ ТО «МФЦ» (Рис. 3) и связывала две информационные системы персональных данных (ИСПДн): ИСПДн с данными о сотрудниках ГАУ ТО «МФЦ» (ИСПДн №1) и ИСПДн с данными по обращениям граждан (ИСПДн №2). Уровни защищенности ИСПДн были определены в соответствии с Постановлением №1119: ИСПДн №1 – УЗ 3, ИСПДн №2 – УЗ 4.

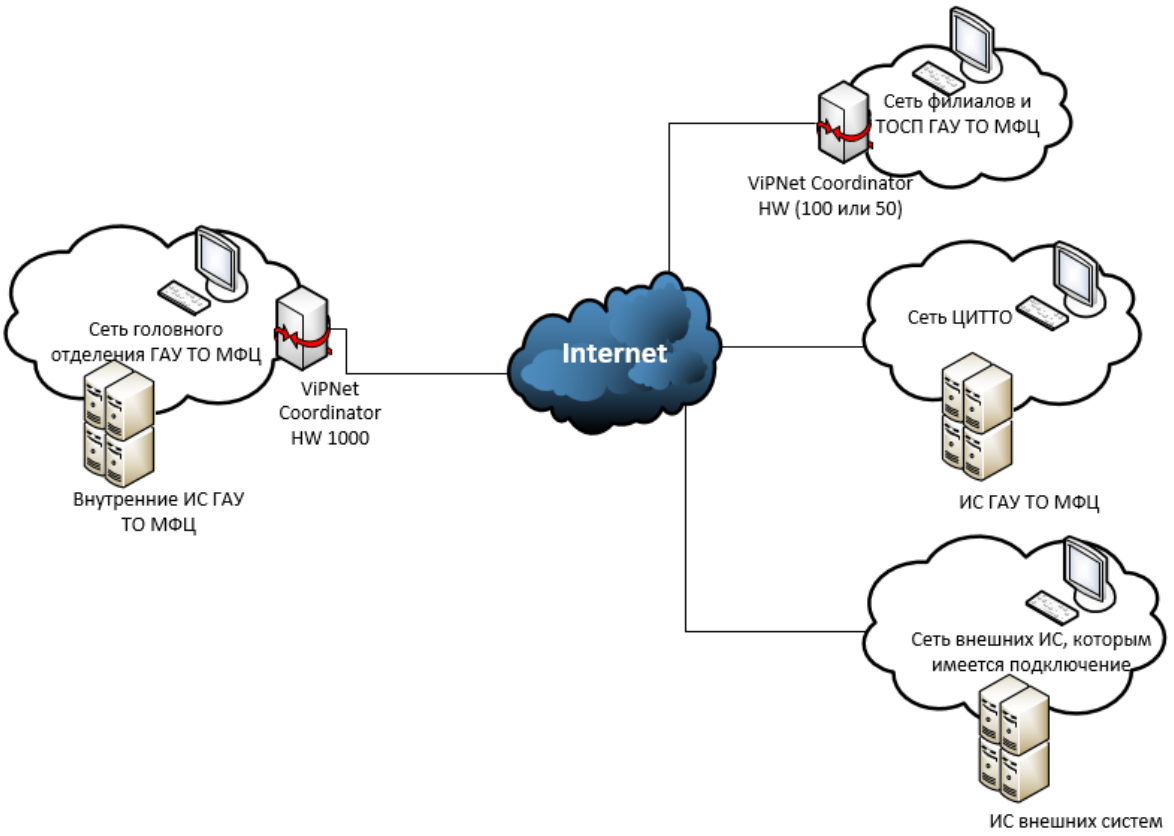

Рис. 3. Схема сети ГАУ ТО «МФЦ».

Также были построены модель злоумышленника и модель угроз для ГАУ ТО «МФЦ» (для обеих ИСПДн коэффициент исходной защищенности Y1 = 10). Из средств защиты в ГАУ ТО «МФЦ» используются смарт-карты с сертификатами ЭЦП, подписанные доверенным удостоверяющим центром, подключена DLP-система InfoWatch Traffic Monitor, функционирует система контроля защищенности и соответствия стандартам MaxPatrol 8, для подключения к серверам с наиболее критичной информацией применяются терминальные серверы, а также используется система контроля и управления доступом и проводится регулярное резервное копирование данных.

В рамках апробации рассматривался ряд гипотез, сформулированных с помощью матрицы ATT&CK. В частности, рассматривалась гипотеза о компрометации сервера баз данных. Для сбора доказательств был проведен анализ журнала событий сервера, изучены характеристики установленных

соединений за последние два месяца, а также проанализирован по ряду параметров входящий и исходящий трафик. Из техник Threat Hunting применялась визуализация, статистический анализ, в дальнейшем также планируется задействовать технику машинного обучения (построить нейросетевую модель для анализа трафика). В итоге выдвинутая гипотеза не нашла подтверждения. В ближайшее время планируется рассмотреть гипотезу о компрометации веб-сервера и учетной записи администратора системы.

Таким образом, системы Threat Hunting позволяют осуществлять проактивный поиск угроз, значительно дополняя функционал системы защиты и возможности реактивного реагирования на угрозы. Благодаря Threat Hunting специалист по информационной безопасности может действовать на опережение и иметь существенное преимущество перед злоумышленником.

СПИСОК ЛИТЕРАТУРЫ

1. Threat Hunting, или Как защититься от 5% угроз // Блог компании ГК ЛАНИТ [Электронный источник]. URL: https://habr.com/ru/company/lanit/blog/447580/ (дата обращения: 30.05.2020)
2. Обзор инструментов Threat Hunting для проактивного поиска и обнаружения угроз // Екатерина Данилова [Электронный источник]. URL https://www.anti-malware.ru/analytics/Market_Analysis/Threat-Hunting-tools-review (дата обращения: 30.05.2020)
3. ATT&CK Matrix for Enterprise // Сайт компании MITRE [Электронный источник]. URL https://attack.mitre.org/ (дата обращения: 30.05.2020)

4. The Complete Guide to the ELK Stack // Полное справочное руководство по ELK Stack [Электронный источник]. URL: https://logz.io/learn/complete-guide-elk-stack/#intro (дата обращения: 30.05.2020)