ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СИСТЕМ МОНИТОРИНГА КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СЕТИ

Родионов Илья Викторович,
магистрант, Уральский государственный экономический университет
Россия, г. Екатеринбург
007Rodionov@rambler.ru

Аннотация

В статье рассматриваются вопросы, связанные с проведением мониторинга корпоративной информационной сети. Отдельное внимание уделено содержанию мониторинга и основным функциям, которые соответствующие системы должны выполнять. Кроме того, обозначены наиболее популярные решения и методы отслеживания состояния корпоративной сети и анализа активности пользователей. Также в статье представлены результаты сравнения некоторых распространенных инструментов мониторинга корпоративной информационной сети с учетом их ключевых характеристики и возможностей применения на практике.

Ключевые слова: корпоративная сеть, мониторинг, атака, трафик, активность, пользователь.

COMPARATIVE ANALYSIS OF CORPORATE INFORMATION NETWORK MONITORING SYSTEMS

Rodionov Ilya Viktorovich,
master's student, Ural State Economic University
Russia, Ekaterinburg
007Rodionov@rambler.ru

ABSTRACT

The article deals with the issues related to the monitoring of corporate information network. Special attention is paid to the content of monitoring and the main functions that the corresponding systems should perform. In addition, the most popular solutions and methods of tracking the state of the corporate network and analyzing user activity are outlined. The article also presents the results of comparison of some common tools for monitoring the corporate information network, taking into account their key characteristics and possibilities of application in practice.

Keywords: corporate network, monitoring, attack, traffic, activity, user.

Корпоративная информационная сеть образует важную инфраструктурную основу современного предприятия. Она соединяет несколько рабочих площадок, устройств и систем для обеспечения бесперебойной работы онлайн-операций. Все, начиная от присутствия пользователей в Интернете, до виртуального сотрудничества и разработки приложений, зависит от сети [1]. Когда компьютерная сеть выходит из строя, это имеет далеко идущие последствия для бизнеса. Например, однодневный сбой в работе Facebook в 2019 году стоил около 90 млн. дол. дохода. В результате компании пришлось срочно убеждать пользователей в том, что их данные находятся в надежных руках, и пытаться сохранить ценность своего бренда.

Сегодняшние технологии динамичны и это отражается на корпоративных информационных сетях. Сеть может постоянно меняться и трансформироваться благодаря виртуализации и внедрению облачных технологий. Киберпреступники всегда ищут и усовершенствуют способы проникновения в сеть, чтобы добраться до основных критически важных ресурсов. Поскольку в бизнес поступает больше потребительских данных, чем когда-либо прежде, отраслевые регуляторы обязали компании защищать конфиденциальную информацию.

Для решения большей части проблем, которые возникают при функционировании корпоративной информационной сети, используются системы мониторинга и управления. Этот класс решений обеспечивает инвентаризацию и расширенную диагностику компьютерных сетей; постоянный контроль функционирования используемого сетевого оборудования, прикладных систем и сетевых сервисов; сбор статистики и визуализацию ключевых показателей производительности и операционных параметров сетевой инфраструктуры; оптимизацию нагрузки на сетевое оборудование и серверы и т.д. [2].

В тоже время необходимо отметить, что сегодня доступно множество видов решений для сетевого мониторинга, каждое из них имеет свои достоинства и недостатки, отличительные особенности, поэтому их подробное изучение и сравнение является в настоящее время актуальной задачей, которая и обуславливает выбор темы данной статьи.

Современные методы аудита и мониторинга в задачах защиты информации описывают в свои трудах Ковцур М.М., Коновалова В.В., Мисливский Б.С., Акилов М.В., Leonardo Alfonso, Arnold Lobbrecht.

Специфика отслеживания важнейших параметров корпоративных сетей предприятий на основе разных систем диагностики и технологий агрегации оповещений нашла свое отражение в публикациях Истратовой Е.Е., Смирнова А.Е., Глинина Е.В., Веревкина С.А., Paul Hudak, Hugo A. Loaiciga, F. Andrew.

В тоже время, несмотря на широкое число работ и внимание ученых к разрабатываемой тематике, ряд вопросов в данной предметной плоскости остается открытым и требует более детальной проработки. Так, отдельного внимания заслуживают методы интеграции систем мониторинга с существующей ИТ-инфраструктурой предприятия. Кроме того, в уточнении нуждаются способы выявления ранних индикаторов компрометации корпоративной сети.

Таким образом, цель статьи заключается в проведении сравнительного анализа систем мониторинга корпоративной информационной сети.

Прежде всего, необходимо отметить, что мониторинг корпоративной информационной сети — это ИТ-процесс, который непрерывно отслеживает и оценивает компьютерную сеть и ее активы. Система мониторинга сети заранее выявляет и устраняет медленный сетевой трафик или неадекватные сетевые компоненты, чтобы обеспечить обнаружение вторжений или других аномалий с целью поддержания целостности сети [3]. В свою очередь системы мониторинга корпоративной информационной сети — это программные платформы, которые подключаются к сетевым компонентам и другим ИТ-

системам для измерения, анализа и создания отчетов о топологии, производительности и состоянии сети.

В процессе выбора и анализа системы мониторинга корпоративной информационной сети необходимо обратить внимание на ее способность выполнять ключевые функции (см. рис. 1).

Рис. 1 Ключевые функции системы мониторинга корпоративной сети

Рассмотрим приведенные на рис. 1 функции более подробно.

1. Подробная аналитика. Аналитика и отчеты о данных являются основой мониторинга сети. Выбранный инструмент должен оценивать производительность сети по таким ключевым показателям, как задержка и скорость. Он также должен генерировать информацию о местоположении и устройствах с точным отображением тенденций.

2. Широкая совместимость. Инструмент должен быть совместим с максимально возможным разнообразием сетей и компонентов ИТ-инфраструктуры. Сюда входят программные приложения и аппаратные сетевые устройства. Кроме того, должна быть предусмотрена возможность отслеживать сетевое подключение и статус подключения в режиме реального времени для виртуальных машин.

3. Оптимизированные панели инструментов. Приборные панели — это то, с помощью чего можно ежедневно просматривать информацию о состоянии и производительности сети. В то время как отчеты о данных могут быть длинными и подробными, приборные панели должны представлять информацию в сжатом виде, чтобы ее можно было понять с первого взгляда.

4. Настраиваемые оповещения. Инструмент управления и мониторинга сети должен отправлять оповещения при каждом необычном сетевом событии, нарушении порога или отключении устройства. Сетевой администратор должен иметь возможность настраивать оповещения, чтобы получать только ту информацию, которая необходима.

5. Несколько пользовательских интерфейсов. Эта функция становится все более важной для современных предприятий [4].

Хочу отметить, что сегодня на практике системные администраторы используют очень много разнообразных инструментов, которые позволяют проводить мониторинг корпоративной информационной сети. Ниже представлена описание некоторых наиболее популярных технологий.

Обнаружение вторжений: эта технология позволяет контролировать сеть и определять, когда хакеры или злоумышленники её атакуют. Сегодня на рынке есть самые разнообразные программные средства, благодаря которым можно достаточно просто выявить атаки на сеть.

Прослушивание пакетов: данная технология позволяет проверять каждый блок или каждый пакет информации, которые циркулируют в сети. Цель данной технологии выявить незаконное программное обеспечение, которое установили хакеры, чтобы следить за сетью [5].

Отслеживание уязвимостей: эти системы на регулярной основе проводят проверку корпоративной сети чтобы выявить её узкие места. Хочу отметить, что данный метод отличается от обнаружения вторжений тем, что благодаря его использованию можно определить, где слабое место сети ещё до того, как на неё будет произведена хакерская атака.

Тестирование на проникновение: это очень интересная технология, поскольку она предполагает, что системные администраторы сами пробуют использовать те методы, которые хакеры намерены применять чтобы взломать сеть. И в результате таких действий можно найти уязвимости и слабые места сети, о которых злоумышленники могут знать, но которые не удалось найти с помощью других средств мониторинга.

Сегодня на рынке можно приобрести самое различные программное обеспечение, чтобы проводить мониторинг корпоративной сети на предприятии. Есть очень много производителей они предлагают широкий ассортимент. В таблице 1 представлена сравнительная характеристика некоторых из них.

Таблица 1 Сравнение распространенных инструментов мониторинга корпоративной информационной сети

Инструмент мониторинга / Критерии оценки	OpenView Network Node Manager 4.1	Spectrum Enterprise Manager	NetView forAIX SNMP Manager	Solstice Enterprise Manager
Определение имени хоста через DNS - сервер	+	+	+	+
Распознавание сетевых топологий	Любые сети на TCP/IP	Ethernet, распределенные сети	Распознавание по интерфейсам устройств	Ethernet, распределенные сети
Поддержка баз данных	Oracle	Файлы	Oracle, Sybase	Informix, Oracle, Sybase
Наличие серверов	+	+	+	+
Количество клиентов	До 15	Неограничено	30	Неограничено
Поддержка SNMP	+	+	+	+
Поддержка ОС	HPUX, Solaris	HPUX, IBM, Win NT	Win NT	Solaris

Максимальное число обслуживаемых узлов	3000	Ограничение отсутствует	Ограничение отсутствует	10000-50000

В качестве вывода хотелось бы отметить, что вопрос управления и мониторинга корпоративных сетей является очень важным. Для осуществления мониторинга нужно выбирать наиболее подходящую программу и стратегию которые будут удовлетворять требования предприятия с точки зрения масштабов, квалификации персонала и имеющихся в распоряжении средств.

Список литературы:

1. Ковцур М.М. Разработка методики удаленного мониторинга трафика в корпоративных сетях // Заметки ученого. 2021. № 6-1. С. 27-31.
2. Тлеугалиев Е.У., Сагиндыков К.М. Система мониторинга для обеспечения информационной безопасности в корпоративной сети // Annali d'Italia. 2022. № 31. С. 139-141.
3. Зиненко О.А. Главные угрозы безопасности корпоративных сетей и как от них защититься // Защита информации. Инсайд. 2021. № 3. С. 4-7.
4. Кокурин Е.А. Разработка архитектуры информационной системы информационной безопасности программного обеспечения корпоративных сетей предприятий // Тенденции развития науки и образования. 2022. № 83-2. С. 103-107.
5. Битуреева Д.Е. Разработка комплексной модели управления информационной безопасностью с применением dlp-системы // Вестник молодых ученых Санкт-Петербургского государственного университета технологии и дизайна. 2021. № 4. С. 33-38.

References:

1. Kovtsur, M.M. Development of the remote traffic monitoring methodology in corporate networks // Notes of the scientist. 2021. No 6-1. Pp. 27-31.
2. Tleugaliev, E.U.; Sagindykov, K.M. Monitoring system for information security in a corporate network // Annali d'Italia. 2022. No 31. Pp. 139-141.
3. Zinenko O.A. The main threats to the security of corporate networks and how to protect from them // Information Protection. Insight. 2021. No 3. Pp. 4-7.
4. Kokurin, E.A. Development of the architecture of the information system of information security software of corporate networks of enterprises // Tendencies of science and education development. 2022. No 83-2. Pp. 103-107.
5. Bitureyeva D.E. Development of a complex model of information security management with the use of dlp-system // Bulletin of young scientists of St. Petersburg State University of Technology and Design. 2021. No 4. Pp. 33-38.