УДК 004.056 EDN UUAIPT

Повышение эффективности процесса управления инцидентами информационной безопасности за счет внедрения SIEM систем

Я.О. Худолей, Е.А. Наташкина*

Центр информационных технологий, Оружейный переулок, 13, Тула, 300002, Россия

*E-mail: Elena.Natashkina@tularegion.ru

Аннотация. В данной статье рассматривается вопрос, связанный с повышением эффективности процесса управления в сфере информационной безопасности. Дается краткий экскурс об этапах внедрения SIEM систем в России. Представлены подходы, которые применялись для решения проблем внедрения SIEM систем вендорами. Первый подход направлен на обучение работников организации-заказчика эффективному использованию SIEM систем. Второй подход направлен на снижение влияния компетенций обслуживающих работников на эффективность SIEM системы. Были обозначены вопросы, касающиеся необходимости процесса сбора и оперирования объемами информации, связанными с событиями безопасности. Также был обозначен вопрос о возможности предотвращения инцидентов по результатам проведенного анализа, и о сокращении их воздействия на информационные системы. Отмечено, что наиболее популярным мотивом приобретения SIEM систем была необходимость соответствия требованиям законодательства по защите информации и требованиям регуляторов. Было уточнено, что с ростом уровня развития информационной безопасности в организациях менялось понимание целей внедрения SIEM систем. Сделаны выводы по результатам обзора требований российского законодательства в части защиты информации, а также представлены результаты обзора особенностей внедрения SIEM систем в России.

Ключевые слова: информационная безопасность, инциденты, SIEM системы, информационные технологии, обработка информации.

Improving the efficiency of the information security incident management process through the introduction of SIEM systems

Ya.O. Khudoley, E.A. Natashkina*

Center of Information Technologies, Tula, Russia

*E-mail: Elena.Natashkina@tularegion.ru

Abstract. This article discusses the issue related to improving the efficiency of the management process in the field of information security. A brief overview of the stages of the implementation of SIEM systems in Russia is given. The approaches that have been used to solve the problems of implementing SIEM systems by vendors are presented. The first approach is aimed at training the employees of the customer organization in the effective use of SIEM systems. The second approach is aimed at reducing the impact of the competencies of service workers on the effectiveness of the SIEM system. Questions were raised regarding the need for the process of collecting and operating volumes of information related to security events. The issue of the possibility of preventing incidents based on the results of the analysis and reducing their impact on information systems was also highlighted. It is noted that the most popular motive for acquiring SIEM systems was the need to comply with the requirements of information protection legislation and regulatory requirements. It was clarified that with the increasing level of information security development in organizations, the understanding of the goals of implementing SIEM systems changed. Conclusions are drawn based on the results of a review of the requirements of Russian legislation in terms of information protection, and the results of a review of the features of the implementation of SIEM systems in Russia are presented.

Keywords: information security, incidents, SIEM systems, information technology, information processing.

1. Введение

На сегодняшний день реализация текущих процессов организации деятельности региональных органов власти и предоставления услуг наделению невозможно без создания сложных, разнообразных и распределенных систем обработки информации. Для обеспечения целостности, доступности и конфиденциальности информации, обрабатываемой в таких информационных системах, должен применяться комплексный подход к выполнению требований информационной безопасности установленный действующим законодательством Российской Федерации, включающий в себя набор организационных и технических мер защиты информации. Эффективная система защиты информации не может существовать без выстроенного мониторинга событий безопасности и оперативного выявления инцидентов безопасности.

2. Цель исследования

Вследствие того, что исследование эффективности управления инцидентами информационной безопасности представляет собой актуальное направление в связи с ужесточением данных вопросов, целью исследования является определение повышения эффективности данных процессов за счет использования SIEM систем.

3. Полученные результаты

Отметим, что в процессе эксплуатации, аттестованной ИС особо остро стоит вопрос своевременного выявления инцидентов информационной безопасности возникающих в ходе реализации угроз, а также компьютерных атак на объекты обработки информации региональных органов власти. Обнаружение и идентификация инцидентов производится в процессе регистрации и анализа событий безопасности, поступающих из различных источников [1].

В случае использования больших информационных систем обработки информации, таких источников событий может быть более 1000, при этом количество производимых ими событий информационной безопасности в течение дня может достигать более 100 тыс. для одного источника. Таким образом объем получаемых событий значительно превышает возможности «ручной обработки» без использования специализированных средств и становится невозможным выявлять весь объем происходящих инцидентов и своевременно реагировать на них.

Сокращение источников событий (например, ограничить системами защиты информации) и обработка событий только от конкретного источника не дает полной

картины в отношении защищенности информации, т.к. события, полученные с единичного источника, могут быть квалифицированы как не являющиеся инцидентами, но в случае корреляции таких событий с другими источниками может быть подтвержден инцидент безопасности.

Также может возникнуть ситуация, когда в процессе расследования инцидента выявляется, что некоторыми источниками не сохранены данные о событиях, в результате чего не удается собрать достаточного объема информации по инциденту, и принять соответствующие меры.

Отдельно стоит отметить ошибочное выявление инцидента, так как расследование и устранение такого инцидента также отвлекает специалистов от плановой работы и несет за собой значительные трудозатраты.

Регулятором в области информационной безопасности ФСТЭК России также установлены меры защиты информации по регистрации, мониторингу и реагированию на события информационной безопасности.

Исходя из этих требований оператором должен осуществлять системный подход к сбору, регистрации, анализу и хранению событий информационной безопасности с целью предотвращения возможных инцидентов, а также своевременного выявления инцидентов и проведения расследования в отношении инцидентов. Но насколько необходимо собирать и оперировать такими объемами информации, связанной с событиями безопасности? Возможно ли по результатам анализа предотвратить инцидент или сократить воздействие на информационные системы?

На отечественном рынке SIEM системы стали появляться в 2012 году [2]. Первая волна внедрения SIEM систем была достаточно неудачной [3]. Причиной тому было непонимание заказчиком, какого результата он ждет от SIEM систем. Большинством организаций SIEM система приобреталась для соответствия требованиям законодательства по защите информации или требований ФСТЭК и ФСБ России. В штате организаций-заказчиков не было потребности, и, соответственно, не было специалистов, которые понимали принципы и сценарии атак на информационную систему (ИС) и инфраструктуру. Вендоры SIEM систем и их партнеры, осуществлявшие дистрибьюцию и внедрение продукта, предоставляли стандартный вариант SIEM системы с предустановленными правилами нормализации и корреляции событий из наиболее часто встречающихся источников событий безопасности. Источники, которые

поддерживала такая SIEM система, а также стандартные правила корреляции событий не учитывали структурно-функциональные особенности ИС и инфраструктуры, а также особенности процессов, происходящих в ИС и инфраструктуре. В результате, если в SIEM систему направлялось мало источников, выявление атак было крайне малоэффективным. Также в SIEM систему не вносились данные по изменениям ИС и инфраструктуры, в результате чего SIEM система видела только часть ИС и инфраструктуры. Если же в систему направлялось много источников событий безопасности, без определения приоритета событий и настройки правил корреляции событий в конкретной ИС и инфраструктуре, то SIEM система выдавала огромное количество срабатываний, подавляющее большинство которых было ложными. При таком варианте развития событий SIEM систему либо полностью отключали, либо отключали значительную часть функций, исходя из принципа «чтобы не мешало». Доработка правил корреляции SIEM системы силами вендора или партнера, проводившего внедрение, означала дополнительные существенные денежные затраты для организации-заказчика, и также не давало значимого увеличения эффективности, так как за относительно короткий период внедрения исполнитель не смог бы разобраться детально в структуре и процессах, происходящих в ИС и инфраструктуре. В итоге у организации-заказчика возникало недоумение, для чего были потрачены значительные денежные средства на систему, от которой не видно эффекта.

Несколько лет назад начала набирать популярность тема внедрения в средства защиты информации механизмов машинного обучения. Не обошла она стороной и SIEM системы. Машинное обучение в SIEM системах выросло до отдельного продукта – UBA/UEBA, которое позволяло находить аномалии в поведении пользователей. UBA-системы не заменяют SIEM, они являются либо самостоятельным продуктом, интегрируемым с SIEM системами, либо расширением SIEM систем. И даже при наличии UBA-систем, все также остается проблема с правилами корреляции событий безопасности.

Для решения проблем, возникших по итогам первой волны внедрения SIEM систем, среди вендоров выявились следующие подходы. Стоит сразу отметить, что вендоры не делают ставку только на один из указанных ниже подходов, лидеры в области SIEM систем стараются развиваться в обоих направлениях.

Первый подход направлен на обучение работников организации-заказчика эффективному использованию SIEM систем. В частности, подход предполагает обучение сотрудников организации-заказчика написанию правил корреляции под свои ИС и инфраструктуру. Для реализации данного подхода разрабатываются статьи и пособия по написанию правил, проводятся семинары и обучения. В качестве одной из реализаций данного подхода можно указать на услугу компании GroupIB Pre-IR Assessment. В рамках данной услуги проводится анализ процессов регистрации и анализа событий безопасности, выявления и реагирования на инциденты информационной безопасности (ИБ), по результатам которого организации даются рекомендации и предлагаются OpenSource-решения по настройке регистрации событий безопасности, автоматизации их анализа и выявлению инцидентов ИБ, проводится обучение сотрудников по выявлению и реагированию на определенные типы инцидентов. Данная услуга является хорошей подготовкой ко внедрению SIEM системы. Эффективность первого подхода зависит от наличия у вендоров и их партнеров серьезной экспертизы в области выявления атак и проведения пентестов, способные обнаруживать новые угрозы.

Второй подход направлен на снижение влияния компетенций обслуживающих работников на эффективность SIEM системы. Одно из направлений данного подхода предполагает внедрение не просто SIEM системы, а целого комплекса средств защиты, выявляющих атаки в специфичных областях (IPS/IDS или NGFW, WAF, сканеры уязвимостей, UBA/UEBA). Совокупность указанных средств защиты и SIEM системы образуют SOC. Например, продукт MaxPatrol SIEM включает в себя модули, проводящие сканирование сети, выявляющие элементы ИС и инфраструктуры и необходимую информацию о них (механизмы обогащения данных об активах — ключевых элементах IT-инфраструктуры), модули комплексного анализа сетевого трафика, в том числе передаваемых по сети файлов (модуль представляет собой средство обнаружения вторжений (IDS) и глубокий анализ сетевых пакетов (DPI) с дополнительным обогащением событий данными геолокации). Также данная система имеет механизмы по интеграции как с продуктами Positive Technologies, так и с специализированными продуктами других производителей.

Логика второго подхода в том, что атаки на конкретные компоненты ИС и инфраструктуру, например, веб-серверы, периметр инфраструктуры, периметр

сегментов инфраструктуры, пользователей, лучше выявляют узкоспециализированные средства защиты, нежели это сделает SIEM система из первичных данных. Таким образом удается снизить нагрузку на SIEM систему и повысить точность выявления инцидентов. Данное направление, учитывая высокую стоимость самой SIEM системы, может оказаться доступным только для крупных организаций, выделяющих значительные бюджеты на IT. Для того, чтобы данных подход был доступен большему числу организаций, в настоящее время активно продвигается услуга мониторинга инцидентов ИБ на аутсорсе (сторонние SOC). Данный вариант представляется наиболее оптимальным с точки зрения затраченных денег, времени и полученного результата. Но в данном варианте слабо учитывается специфика структуры и процессов ИС и инфраструктуры организации. Другим направлением данного подхода является создание из SIEM некой экспертной системы, наполняемой и регулярно обновляемой специалистами вендора.

Изначально наиболее популярным мотивом приобретения SIEM систем была необходимость соответствия требованиям законодательства по защите информации и требованиям регуляторов. Требования по защите персональных данных, а также требования по защите информации в государственных ИС предполагают регистрацию и анализ событий безопасности, выявление инцидентов ИБ. Данные требования возможно выполнить и без использования SIEM систем. Естественно, об эффективности выявления инцидентов при таком подходе речи не идет. Только для государственных ИС 1-го класса защиты требуется интеграция результатов мониторинга событий безопасности из разных источников и их корреляция с целью выявления инцидентов безопасности. Таким образом, если подходить строго формально, то SIEM система необходима только для государственных ИС 1-го класса защиты. Вступление в силу с 1 января 2018 года Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» и связанных с ним нормативно-правовых актов, согласно которым в России создается Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, подразумевает создание корпоративных и ведомственных центров выявления компьютерных атак [4]. Основой таких центров становится SIEM система.

С ростом уровня развития информационной безопасности в организациях менялось и понимание целей внедрения SIEM систем. В организациях с развитым

уровнем ИБ на регулярной основе проводится инвентаризация ИТ-активов, для понимания какие изменения происходят в ИС и инфраструктуре, осуществляется выявление уязвимостей ИС и инфраструктуры с помощью специализированных сканеров безопасности с последующей верификацией уязвимостей. На основании информации о выявленных уязвимостях и ценности ИТ-ресурсов и информации формируются предположения о типах нарушителей, для кого атаки на ИС и инфраструктуру будет представлять интерес, и о возможных сценариях атак. В организациях данного типа есть понимание, что выявление атак на ИС и инфраструктуру будет существенно затруднено без наличия SIEM системы. Рост уровня развития ИБ в организации практически невозможен без выделения средств на наем и обучение компетентных специалистов, а также приобретение средств защиты. Поэтому организации с развитым уровнем ИБ могут себе позволить (вернее могут убедить руководство в необходимости) приобрести, настроить и поддерживать функциональную SIEM систему, так как они понимают, что в долгосрочной перспективе SIEM система помогает снизить затраты на информационную безопасности и ИТ в целом. В данных организациях есть понимание, что SIEM системы не относятся к решениям, работающим по принципу «включил и работай» или «настроил и забыл», и что при внедрении их невозможно добиться всех поставленных целей за несколько месяцев.

4. Выводы

По результатам обзора требований законодательства Российской Федерации и подзаконных актов уполномоченных организаций в части защиты информации сделаны следующие выводы:

- регистрация событий безопасности с последующим выявлением и обработкой инцидентов безопасности являются обязательными для реализации мерами в государственных информационных системах, информационных системах персональных данных и в объектах критической информационной инфраструктуры;
- использование средств корреляции событий безопасности не является обязательным для всех классов информационных систем.

По результатам обзора особенностей внедрения SIEM систем в Российской Федерации можно отметить следующее:

- с ростом уровня зрелости процессов информационной безопасности в организациях цели внедрения SIEM смещаются от «необходимость соответствия требованиям законодательства/отечественных или зарубежных стандартов» к «SIEM – эффективное средство выявления атак»;
- непонимание целей использования SIEM, низкая компетенция специалистов по информационной безопасности являются существенным препятствием на пути эффективного использования SIEM. В связи с чем, становится популярным мнение, что SIEM – малоэффективный продукт, стоимость приобретения и внедрения которого весьма высока;
- компании, осуществляющие разработку, поставку и внедрение SIEM прилагают больше усилий (вернее предлагают дополнительные услуги), чтобы сделать использование SIEM в компаниях более эффективным.

Список литературы

1. Федеральный закон от 26.07.2017 №187 «О безопасности критической информационной инфраструктуры Российской Федерации».
2. Security Information and Event Management (SIEM). Деловой портал TAdviser.ru [Электронный ресурс]. - Режим доступа: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:Security_Information_and_Event_Management_(SIEM)#2007 (дата обращения: 26.01.2024)
3. Компании Positive Technologies. Видеотрансляция с форума Positive Hack Days 2016 [Электронный ресурс]. – Режим доступа: https://phdays.com/archive/2016/ (дата обращения: 26.01.2024).
4. Королев И.Д. Анализ проблематики системы управления информацией и событиями безопасности в информационных системах / И.Д. Королев, В.И. Попов, В.А. Ларионов // Инновации в науке. – 2018. – № 12(88). – С. 19-26.