УДК 004.056.53

Анализ систем мониторинга и управления

информационной безопасностью

Н.В. Абрамченко (SPIN 7288-6400), 1Р.И. Садыков

Финансовый университет при правительстве России (Омский филиал), Россия

1СибАДИ, г. Омск, Россия

*Аннотация. Системы мониторинга и управления информационной безопасностью способны значительно повысить эффективность комплексной системы защиты данных. Авторами рассмотрены законы и стандарты по информационной безопасности и выделены ряд требований, обязательных для исполнения в государственных информационных системах и информационных системах персональных данных. Проведен сопоставительный анализ широкого спектра программных систем мониторинга и управления событиями информационной безопасности на предмет выполнения данных требований.*

*Ключевые слова. Системы мониторинга и управления информационной безопасностью. Защита данных. Информационные системы.*

В связи с широким применением информационных технологий в современном обществе актуальным требованием является обеспечение защиты информации. Однако, вместе с ростом количества средств защиты существенно увеличивается и объём информации, которую должен обработать администратор безопасности. Это обусловливает то, что в настоящее время на первый план выходят задачи по мониторингу событий информационной безопасности и оперативному реагированию на инциденты. Для крупной компании оперативный доступ к данным мониторинга безопасности, своевременное отслеживание и разрешение инцидентов в режиме реального времени – неоценимый вклад в повышение эффективности и управляемости системы ИБ в целом.

Все больше предприятий и организаций имеют целый комплекс средств по защите информации. Зачастую, чтобы проанализировать все входящие данные, за день или даже за час работы систем по обеспечению информационной безопасности, требуются не только огромные затраты времени и многочисленный штаб персонала, но и должная квалификация сотрудников. Не каждое предприятие имеет возможность и желание постоянно расширять отдел информационных технологий. Системы мониторинга и управления информационной безопасностью (СМУИБ) решают проблему анализа входящих данных, и помогают быстро реагировать на различные угрозы информационной безопасности, а также повысить эффективность принятия управленческих решений за счет оперативности представления информации.

В состав системы мониторинга включаются следующие компоненты:

* агенты мониторинга, предназначенные для сбора информации, поступающей от различных средств защиты;
* сервер событий, обеспечивающий централизованную обработку информации о событиях безопасности, которая поступает от агентов. Обработка осуществляется в соответствии с правилами, которые задаются администратором безопасности;
* хранилище данных, содержащее результаты работы системы, а также данные, полученные от агентов;
* консоль управления системой, позволяющая в реальном масштабе времени просматривать результаты работы системы, а также управлять её параметрами.

В системах мониторинга выделяют подкласс продуктов, называемый «Системы мониторинга и управления событиями информационной безопасности» (SIEM). Такие системы реализуют комплексный подход к решению задач сбора, анализа и контроля событий, поступающих от различных средств защиты. Она помогает решить следующие задачи:

**•** управление большим объемом событий ИБ;

**•** получение полной картины происходящего в информационной системе с точки зрения ИБ;

**•** мониторинг текущего уровня обеспечения безопасности (контроль достижения заданных показателей эффективности, KPI);

**•** своевременное обнаружение инцидентов ИБ;

**•** получение реальных данных для анализа и оценки рисков;

**•** принятие обоснованных решений по управлению безопасностью;

**•** выполнение отдельных требований законодательства и нормативных актов в области мониторинга событий ИБ (ISO/IEC 27001:2005, PCI DSS, СТО БР ИББС, Федеральный закон № 152 «О персональных данных» и др.)

Система мониторинга собирает лог-файлы от средств обеспечения ИБ. Сбор журналов событий возможен благодаря агентам, устанавливаемым на автоматизированные рабочие места со средствами защиты информации, или технологиям типа WMI (Windows Management Instrumentation, инструментарий управления Windows). Данные передаются на сервер с помощью различных протоколов, PRC (Remote Procedure Call, удаленный вызов процедур), FTP (File Transfer Protocol, протокол передачи файлов), TFTP (Trivial File Transfer Protocol, простой протокол передачи файлов), и т.д. После доставки лог-файлов они должны быть нормализованы. Каждый производитель оборудования и программного обеспечения сам решает, в каком формате и какие данные хранить в журнале. Поэтому журналы событий могут быть очень различными.

Для того чтобы система мониторинга могла понимать все входящие логи, они приводятся к некому стандарту. Журналы разбиваются на свойства и «привязываются» к полям формата IDMEF (Intrusion Detection Message Exchange Format, формат обмена данными между компонентами IDS). Также данные системы имеют в своем распоряжении множество различных средств анализа журналов. Это свойство является важнейшим. Системы мониторинга и управления событиями информационной безопасности способны коррелировать:

а) описанную правилами корреляции угрозу;

б) угрозу на базе типового общего шаблона;

в) аномалию в случае отклонения от «baseline»;

г) отклонение от политики по принципу «все, что не разрешено - запрещено» (реализовано не во всех SIEM);

д) причинно-следственную связь [7].

Таким образом, системы мониторинга и управления событиями информационной безопасности решают очень важную задачу: это агрегация и анализ данных, собираемых от множества программно-аппаратных средств защиты информации, что особо актуально для разросшейся инфраструктуры современных информационных систем.

В данном исследовании интерес представляют государственные информационные системы и информационные системы персональных данных, для которых реализация комплексной защиты данных является неотъемлемым условием существования [2,3]. С целью обеспечения таковой следует изучить:

1) требования по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные в приказе ФСТЭК России №17;

2) требования к защите информации из ГОСТ Р 51583-2014;

3) меры по обеспечению защиты персональных данных (ПДн), утвержденные в приказе ФСТЭК России №21;

4) требования к защите ПДн при их обработке в ИСПДн, утвержденные в постановлении Правительства Российской Федерации №1119 [1,4-6].

Анализ перечисленных документов с одной стороны, а также функций и состава систем мониторинга и управления событиями информационной безопасности с другой стороны, позволил определить ряд требований к средствам защиты данного класса (СМУИБ), если их предполагается использовать в системах защиты данных в государственных информационных системах и информационных системах персональных данных:

1. патентная чистота;
2. возможность создания аналитических отчетов;
3. возможность визуализации данных;
4. возможность создания собственных правил;
5. возможность резервного копирования данных;
6. хранение данных с использованием РСУБД;
7. возможность использования русского или английского языка;
8. наличие графического интерфейса;
9. возможность оповещения об инциденте;
10. наличие сертификата ФСТЭК России по защите от НСД;
11. наличие сертификата ФСТЭК России об отсутствии НДВ;
12. хранение информации в течение установленного срока;
13. возможность безагентного сбора данных;
14. возможность создания собственных коннекторов для подключения стороннего продукта.

На соответствие этим требованиям были проверены ряд программ (HP ArcSight ESM, RSA Security Analytics, IBM QRadar SIEM, McAfee ESM, Splunk, Symantec SIM, AlienVault OSSIM, LogRhythm, КОМРАД «НПО «Эшелон»), проведен их сравнительный анализ (см. таблицу 1).

*Таблица 1. Сравнительный анализ систем мониторинга и управления информационной безопасностью*

| **№ п/п** | **Требования** | **HP ArcSight** | **RSA Security Analytics** | **IBM QRadar SIEM** | **McAfee ESM** | **Splunk** | **SSIM** | **AlienVault OSSIM** | **LogRhythm** | **КОМРАД «НПО «Эшелон»** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Патентная чистота | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 2 | Возможность создания аналитических отчетов | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 3 | Возможность визуализации данных | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 4 | Возможность создания собственных правил | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ? | ✓ |
| 5 | Возможность резервного копирования данных | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 6 | Хранение данных с использованием РСУБД | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ |
| 7 | Возможность использования русского или английского языка | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 8 | Наличие графического интерфейса | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 9 | Возможность оповещения об инциденте | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 10 | Наличие сертификата ФСТЭК России по защите от НСД | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ |
| 11 | Наличие сертификата ФСТЭК России об отсутствии НДВ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ |
| 12 | Хранение информации в течение установленного срока | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 13 | Возможность безагентного сбора данных | ✗/✓ | ✗/✓ | ✗/✓ | ✗/✓ | ✗/✓ | ✗ | ✗/✓ | ✗/✓ | ✗/✓ |
| 14 | Возможность создания собственных коннекторов для подключения стороннего продукта | ✓ | ✓ | ✓ | ✗ | ✓ | ✗/✓ | ✓ | ✗ | ✗ |

Примечание: ✓ – требование выполняется; ✗ – требование не выполняется; ✗/✓ – требование выполняется, но с нюансом; ? – не удалось найти информацию.

Следует упомянуть, что такие продукты как IBM QRadar и Symantec SIM сняты с продаж из-за того, что они не могут конкурировать с новыми продуктами компаний, к примеру, McAfee и RSA. Рынок СМУИБ динамичен, и поэтому компании выпускают новые решения и используют новые технологии в программах. В ходе анализа было выявлено, что всем требованиям наиболее полно соответствуют только два продукта, McAfee ESM и КОМРАД (поставляются в виде программно-аппаратного комплекса), не уступающие по функциональности продукту компании HP. Возможно, HP занимает большую долю рынка из-за того, что заняла нишу на рынке СМУИБ одной из первых компаний.

Но, если решения, предоставляемые в продукте HP ArcSight ESM доступны лишь коммерческим организация или предприятиям, к примеру, заказчиками HP ArcSight ESM являются:

а) Центральный банк РФ;

б) ОАО «Россельхозбанк»;

в) ОАО «Газпромбанк»;

г) ОАО Национальный банк «Траст»;

д) ОАО «Собинбанк»;

е) ОАО «ТрансКредитБанк»;

ж) и т.д.;

то сертифицированная система КОМРАД является поставщиком для таких государственных и унитарных организаций и предприятий как:

а) блок силовых министерств и федеральных служб;

б) Федеральная налоговая служба России (ФНС России);

в) Федеральная служба Российской Федерации по контролю за оборотом наркотиков (ФСКН России);

г) Министерство финансов Московской области;

д) ФГУП «Ростовский-на-Дону научно-исследовательский институт радиосвязи» (ФГУП «РНИИРС»), г. Ростов-на-Дону;

е) ФГУП «Центральный научно-исследовательский институт химии и механики» (ФГУП "ЦНИИХМ");

ж) ОАО «Институт сетевых технологий» (ОАО «ИСТ»), СПб;

з) и т.д.

Таким образом, можно сделать вывод, что для государственных информационных систем, в которых обрабатывают персональные данные, следует выбирать именно McAfee ESM или КОМРАД, данные продукты не уступают по функциональности HP ArcSight ESM, но имеют сертификаты ФСТЭК.

В заключение отметим, что на сегодняшний день всё больше и больше компаний приходят к пониманию того, что использование систем мониторинга позволяет значительно повысить эффективность процесса обнаружения и реагирования на инциденты информационной безопасности. Это обеспечивается за счет автоматизации процесса сбора и анализа информации, которая регистрируется в автоматизированной системе компании. При этом применение систем мониторинга также позволяет значительно повысить эффективность уже установленных в организации средств защиты.

Библиографический список

1. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения [текст]: ГОСТ Р 51583 – 2014.
2. О персональных данных [текст]: федер. закон от 27 июля 2006 г. №152-ФЗ.
3. Об информации, информационных технологиях и о защите информации [текст]: федер. закон от 27 июля 2006 г. №149-ФЗ.
4. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [текст]: приказ ФСТЭК России от 18 февраля 2013 г. №21.
5. Об утверждении Требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [текст]: приказ ФСТЭК России от 11.02.2013 г. №17.
6. Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных [текст]: постановление правительства РФ от 1 ноября 2012 г. №1119.
7. Шелестова, О. SIEM и (или) сканер уязвимостей [интернет-ресурс] – (http://www.securitylab.ru/analytics/430782.php)