СИСТЕМА СИТУАЦИОННОГО УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННОГО ПЕРИМЕТРА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Судакевич А. А.

Утин Л. Л. – к.т.н, доцент

Безопасность информационного периметра отдельных организаций обеспечивается множеством межсетевых экранов, систем обнаружения вторжений и антивирусных средств. Однако в подавляющем большинстве случаев множество проблем информационной безопасности остаются нерешенными. Использование системы управления и мониторинга информационной безопасности с возможностью анализа информационных событий является одним из направлений решения отдельных аспектов информационной безопасности.

В настоящее время все больше внимания уделяется повышению эффективности системы управления информационной безопасностью. Это обусловлено тем, что применение для защиты информационного периметра отдельных организаций только межсетевых экранов, систем обнаружения вторжений и антивирусных средств уже не гарантирует обеспечение сохранности, целостности, конфиденциальности и доступности информационных систем. Увеличение количества устройств защиты при отсутствии программно-технических решений по их управлению или мониторингу и корреляции событий от установленных технических средств, может приводить к конфигурационным ошибкам, снижению возможности по проведению анализа информационных потоков и ослаблению уровня защиты всей системы.

Умение распознавать определенные типы поведения, выраженные сотрудниками, которые готовятся к информационной атаке, может помочь предотвратить потенциальную угрозу. Согласно исследованиям [1] большинство атак планируется заранее, а, следовательно, шаги потенциальных нарушителей могут быть предотвращены:

- у 80% нарушителей, которые совершали нападения на свои компании, было негативное поведение до инцидента;
- 92% нарушителей сталкивались с негативом на работе, например, понижение в должности или предупреждение об увольнении;
- 57% нарушителей были восприняты другими как недовольные;
- для выполнения большинства нападений использовался удаленный доступ;
- наиболее распространенным мотивом была месть.

Информационная безопасность компании обычно строится не только на использовании технологических средств защиты, но использует и организационно-юридические возможности. При этом общие принципы обеспечения безопасности остаются неизменны и должны учитывать разграничение прав доступа и контроль за соответствием служебных обязанностей сотрудников и доступной им информации.

Инфраструктура современных корпоративных информационных систем постоянно развивается, становится все более сложной и разнообразной и приобретает распределенный характер. Внутри такой распределенной системы, состоящей из серверов приложений, сетевого оборудования, средств и систем безопасности, пользователи корпоративной сети ежедневно генерируют миллионы событий. В таких условиях остро встает вопрос контроля текущего состояния и обеспечения информационной безопасности.

Системы мониторинга и управления информационной безопасностью осуществляют сбор и анализ событий от разнородных приложений, операционных систем, сетевых устройств, телекоммуникационного оборудования. Их обычно разделяют на три класса решений:

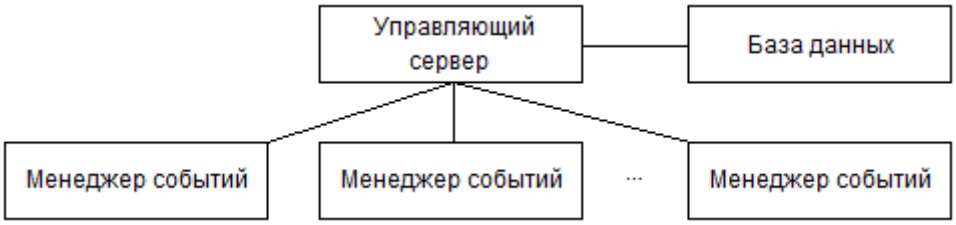
- Security Information Management (SIM) – системы, которые в первую очередь ориентированы на сбор, анализ и долгосрочное хранение событий безопасности от приложений, операционных систем, баз данных и в меньшей степени на сбор данных от сетевого и серверного оборудования
- Security Event Management (SEM) – системы, которые в первую очередь ориентированы на сбор и анализ событий аудита от телекоммуникационного оборудования и в меньшей мере на сбор данных от пользовательских и серверных приложений
- Security Information and Event Management (SIEM) – системы, сочетающие в себе функционал и SIM, и SEM решений

В настоящее время на рынке систем мониторинга и управления информационной безопасностью преобладают SIEM решения, предназначенные для решения следующих задач:

- оперативное обнаружение нарушений политики информационной безопасности;
- мониторинг, выявление и приоритезация в режиме реального времени событий от разных устройств и инцидентов информационной безопасности;
- автоматическое реагирование на инциденты информационной безопасности;
- формирование базы знаний по инцидентам информационной безопасности;
- проведение расследований инцидентов информационной безопасности.

Системы мониторинга, анализа и управления информационной безопасностью, разворачиваемые поверх корпоративной сети, в общем случае состоят из менеджеров событий, управляющего сервера и базы данных, рисунок 1. Менеджеры событий осуществляют сбор событий информационной безопасности и

выполняют их первоначальную обработку и фильтрацию, после чего передают на анализ серверу приложений, который является основой системы. Сервер приложений анализирует собранную с помощью агентов информацию и преобразует ее в более высокоуровневое и удобное для анализа представление. Вся информация, собранная агентами, а также результаты анализа ее сервером приложений сохраняются в базе данных. Для обработки и анализа событий информационной безопасности можно использовать механизмы нормализации, фильтрации, классификации, агрегации, корреляции и приоритезации событий.



Внедрение системы мониторинга событий информационной безопасности позволяет обеспечить централизованное управление, увеличить скорость выявления, расследования и реагирования на инциденты информационной безопасности, а также повысить эффективность управления рисками информационной безопасности

Список использованных источников:

3. Яфизов Р. А. Защита от внутренних угроз // Information Security/ Информационная безопасность – 2008 – Номер 1.
4. Башлыков М. А. Предотвращение утечки конфиденциальной информации // Information Security/ Информационная безопасность – 2010 – Номер 3.
5. Поспелов Д .А. Ситуационное управление. Теория и практика / Д. А. Поспелов. – Москава: Наука, 1986 – 285 с.