СИСТЕМА МОНИТОРИНГА БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ НА ОСНОВЕ АНАЛИЗА СОБЫТИЙ

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

Сороко М.В.

Астровский И.И. – к.т.н., доцент

Любая корпоративная компьютерная сеть, даже небольшая, требует постоянного внимания к себе. Как бы хорошо она ни была настроена, насколько бы надежное ПО не было установлено на серверах и клиентских компьютерах – нельзя полагаться лишь на внимание системного администратора; необходимы автоматические и непрерывно действующие средства контроля состояния сети и своевременного оповещения о возможных проблемах. Также особое внимание необходимо уделять постоянному мониторингу событий, связанных с безопасностью информационных систем.

Системы защиты постоянно развиваются и адаптируются к новым видам угроз. Количество источников информации, из которых поступают данные по текущему состоянию защищенности, растет с каждым днем. Когда инфраструктура слишком сложна, невозможно уследить за общей картиной происходящего в ней. Если своевременно не реагировать на возникающие угрозы и не предотвращать их, толку не будет даже от сотни систем безопасности. На помощь приходят системы управления событиями информационной безопасности – Security Information and Event Management (SIEM) [1].

SIEM - это технология, которая помогает в мониторинге, предупреждает администратора, коррелирует события журналов безопасности, позволяет расследовать инциденты, позволяет строить отчетность. SIEM может служить, как хранилище журналов для дальнейшего анализа.

Система управления событиями может помочь компании в повседневном оперативном мониторинге сетевых устройств, компьютеров, серверов, веб-сайтов, службы каталогов (Active Directory) и других устройств, которые используются в корпоративных сетях. Таким образом с помощью системы управления событиями можно построить единый центр реагирования в компании – Security Operation Center(SOC), который станет основным инструментом для анализа и поддержания состояния безопасности на достаточно высоком уровне [2].

Для внедрения данных систем необходимо провести ряд первоначальных мероприятий:

-Оценить инфраструктуру предприятия

-Определить количество источников, с которых будут собираться журналы безопасности

-Определить способы и протоколы передачи журналов на сервер

-Рассчитать среднее количество событий в минуту со всех источников

Главным этапом в построении систем мониторинга является правильный выбор источников событий. Рассмотрим основные источники:

-Сервера управления доступом — для мониторинга контроля доступа к информационным системам и использования привилегий

-Журналы событий серверов и рабочих станций

-Сетевое оборудование, маршрутизаторы, межсетевые экраны

-Системы предотвращения вторжений

-Сервера антивирусной защиты. События о работоспособности ПО, баз данных, изменении конфигураций и политик, вредоносных программах

-Сканеры уязвимостей

-Системы предотвращения утечек информации, антифрода

-Netflow и системы учета трафика

Заключительным этапом внедрения SIEM систем является настройка правил безопасности, так как корректно настроенные правила позволяют администраторам реагировать на инциденты в минимально кратчайшие сроки.

Список использованных источников:
1. SIEM [Электронный ресурс] – Режим доступа: https://www.securitylab.ru/analytics/430777.php
2. CISSP All-In-One Exam Guide // Шон Харрис – 2011