WWW.PTSECURITY.RU / EMAIL: PT@PTSECURITY.RU / TEL.: +7 (495) 744 01 44

Система контроля защищенности и соответствия стандартам на базе MaxPatrol 8

Москва, 2014

Оглавление

1 Общие сведения

1.1 Назначение Системы

Распределенная информационно-аналитическая Система предназначена для получения объективной оценки состояния защищенности IT-инфраструктуры в целом, а также отдельных подразделений, узлов и приложений. Применение такой системы для контроля защищенности ИС позволит:

- сократить трудозатраты,
- минимизировать влияние человеческого фактора,
- использовать единый подход при проведении работ.

Поиск и устранение уязвимостей и ошибок конфигурации ИС позволяют взять под контроль базовые угрозы ИБ, характерные для ИС и ее компонентов, — нарушение конфиденциальности, целостности и доступности. Применение Системы позволит избежать негативных последствий для бизнеса компании, вследствие реализации угроз, приводящих к:

- нарушению законов или требований подзаконных актов,
- финансовым потерям,
- снижению эффективности бизнеса,
- негативному воздействию на репутацию.

Контроль защищенности, реализуемый Системой, относится к категории превентивных защитных механизмов. Его главное назначение — своевременно обнаружить слабые места (уязвимости) ИС и тем самым предотвратить возможные атаки с использованием этих уязвимостей.

Для организации эффективной защиты ИС важно также контролировать ее соответствие стандартам безопасности. Контроль соответствия стандартам позволяет обеспечить выполнение требований российских регулирующих органов, международных и отраслевых стандартов, корпоративных регламентов.

1.2 Задачи, решаемые Системой

Для достижения поставленной цели Система обеспечивает решение следующих задач, которые соответствуют ключевым этапам контроля защищенности:

- инвентаризация компонентов ИС и планирование контроля защищенности;
- поиск уязвимостей и ошибок конфигурации компонентов ИС, а также несоответствий фактических настроек ИС установленным требованиям (внутренним политикам, стандартам и «лучшим практикам»);
- анализ результатов контроля защищенности, формирование отчетов;
- устранение уязвимостей и ошибок конфигурации компонентов ИС;
- оценка эффективности контроля защищенности и действий, связанных с устранением нарушений безопасности.

Дополнительно Система обеспечивает автоматизацию и централизацию процессов поиска уязвимостей, контроля состояния информационной безопасности и соответствия стандартам в ИС различного масштаба.

2 Описание предлагаемой Системы

2.1 Общие сведения

Система для выполнения поставленных задач реализует следующие функциональные возможности:

- тестирование на проникновение,
- системные проверки,
- контроль соответствия стандартам,
- выявление признаков компрометации системы,
- оценка эффективности процессов ИБ.

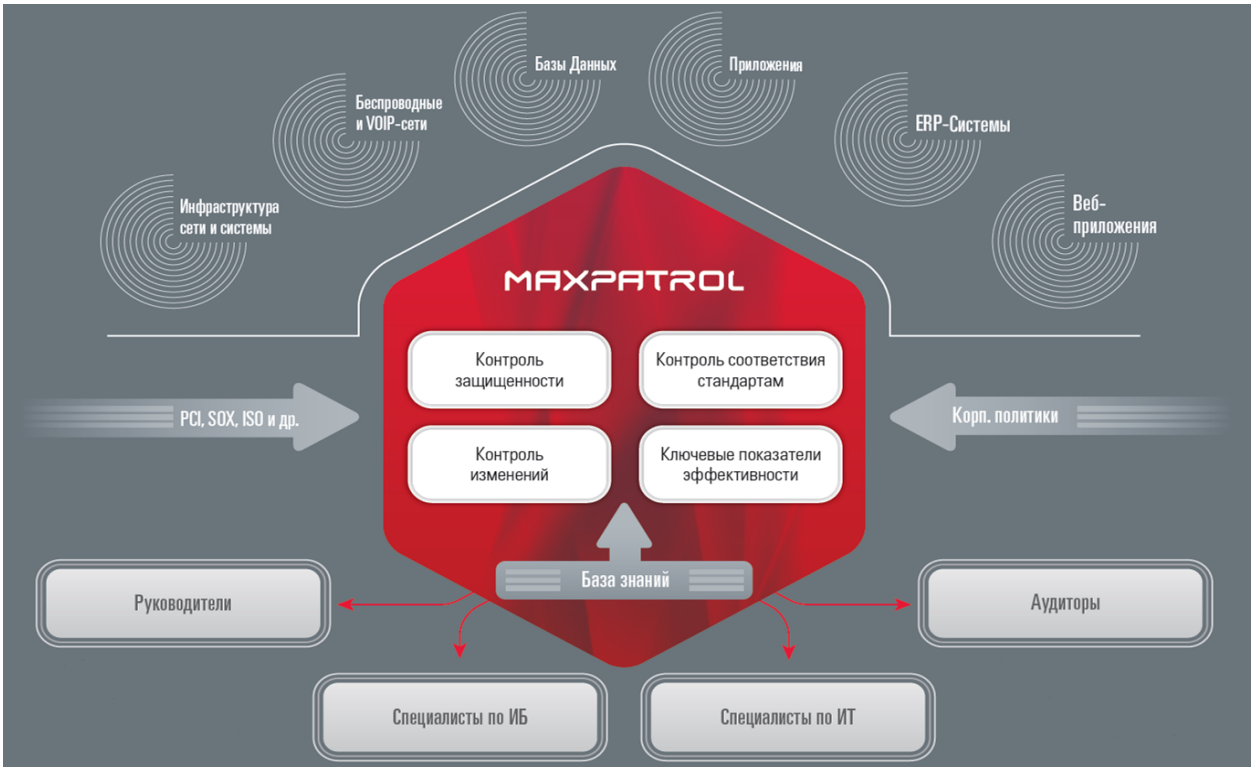

Рис. 1. Система контроля защищенности и соответствия стандартам

Механизм тестирования на проникновение реализует проверки, типичные для сканера сетевого уровня: «баннерные» проверки, «эксплойты», подбор учетных записей. Он ориентирован на использование минимальных привилегий в тестируемой системе. Система содержит также специализированные проверки, направленные на анализ защищенности веб-приложений и СУБД.

Механизм проведения системных проверок позволяет выполнять проверки посредством удаленного доступа к объектам сканирования. Используются протоколы, позволяющие получить удаленный доступ к исследуемой системе (NetBIOS, SSH, WMI и т. п.) и учетные записи. Механизм системных проверок может быть использован для контроля обновлений, анализа конфигураций, локальной оценки стойкости паролей. Отличием Системы при выполнении системных проверок является отсутствие необходимости в наличии агента на исследуемом объекте.

Механизм контроля соответствия стандартам позволяет обрабатывать результаты проведения системных проверок с учетом требований различных стандартов. При этом могут быть учтены как простые технические требования, например, о длине или периоде действия паролей, так и более сложные, например, об отсутствии устаревшего программного обеспечения.

В базу знаний Системы входит широкий набор технических стандартов, каждый из которых определяет набор требований к настройке программных и программно-аппаратных средств. При этом администратору системы доступны механизмы изменения заложенных в Систему стандартов, а также создания собственных, с использованием встроенного инструментария.

Существуют разнообразные технические меры, призванные в режиме реального времени анализировать данные сетевых журналов и другие подобные источники информации, но несмотря на наличие средств автоматизации, своевременное обнаружение следов компрометации системы остается задачей эксперта в области информационной безопасности. Предлагаемая Система является удобным инструментом в руках такого эксперта, позволяя провести экспресс-расследование в соответствии с поставленной задачей на большом количестве компьютеров, объединенных в локальную или глобальную сеть.

Система обеспечивает оценку эффективности процессов ИБ в организации с использованием набора специальных показателей, как технических (например, доля узлов, не удовлетворяющих требованиям парольной политики), так и высокоуровневых (к примеру, процент выполнения филиалом требований по безопасности в сравнении с другими филиалами на протяжении определенного времени).

Механизмы отчетности Системы позволяют отслеживать изменения в защищенности отдельных узлов и подразделений, а также демонстрировать общей уровень защищенности ИТ-инфраструктуры.

2.2 Состав Системы

2.2.1 Подсистема контроля защищенности

Подсистема анализа защищенности реализует два механизма контроля защищенности: сетевое сканирование (PenTest) и системное сканирование (Audit).

Механизм сетевого сканирования производит оценку защищенности сетевых служб сканируемого узла. В этом режиме Система использует возможности, доступные внешнему по отношению к защищаемой информационной системе потенциальному нарушителю, при этом используются следующие механизмы выявления уязвимостей:

- определение ПО или сервиса по особенностям их реализации,
- проверка наличия уязвимости путем ее частичной эксплуатации,
- проверка уязвимости веб-приложения путем анализа контента.

Механизм сетевого сканирования обеспечивает возможность получения:

- общих сведений о сетевых ресурсах (серверах, рабочих станциях, активном сетевом оборудовании, принтерах), включая сетевые адреса, тип операционной системы, доступные сетевые приложения и сервисы;
- данных о выявленных уязвимостях (включая ошибки конфигурации) в реализации идентифицированных сетевых приложений, уязвимости в доступные по протоколу HTTP в веб-приложениях, обусловленных ошибками, допущенными при разработке этих приложений;
- подобранных учетных записей с простыми паролями или паролями по умолчанию.

Механизм системного сканирования производит оценку защищенности как серверных, так и клиентских (локальных) компонентов сканируемого узла. В этом режиме система использует возможности, доступные внутреннему потенциальному нарушителю, имеющему санкционированный доступ к сканируемому узлу. Система проводит сбор сведений о конфигурации программного и аппаратного обеспечения в объеме, достаточном для выявления уязвимостей (обусловленных, в частности, ошибками

конфигурации): аппаратная конфигурация, файлы настроек сетевых устройств, списки установленного ПО, пользователи и роли доступа.

Для операционных систем Microsoft Windows, например, доступно получение информации о лицензионном ключе операционной системы, а также сбор сведений о фактах подключения (в том числе, несанкционированных) модемов, беспроводных устройств, внешних USB-устройств.

2.2.2 Подсистема контроля соответствия стандартам

Подсистема контроля соответствия стандартам обеспечивает оценку соответствия сканируемого объекта требованиям профилей защиты, реализованных в Системе. При этом проводятся как проверки, реализованные в режиме системного сканирования, включающие идентификацию установленного программного обеспечения контролируемого узла, так и дополнительные проверки, необходимые для принятия решения о соответствии сканируемого объекта требованиям профилей защиты.

Подсистема может быть дополнительно настроена с учетом требований международных или корпоративных стандартов в области ИБ (PCI DSS, ISO 27001, SOX 404, NIST, МОРАС, Федеральные законы № 152-ФЗ и 161-ФЗ, СТО БР ИББС, СТО Газпром). Для этого в нее встроены более ста постоянно обновляемых и дополняемых технических стандартов для сетевого оборудования, операционных систем, СУБД, сетевых приложений, веб-служб, почтовых систем, ERP-приложений, АСУ ТП, созданных на основе рекомендаций ведущих мировых производителей и опыта экспертов компании Positive Technologies.

Кроме того, Система обеспечивает контроль выполнения требований законов и нормативных документов регулирующих органов[1].

2.2.3 Подсистема обнаружения следов компрометации

Подсистема обеспечивает проведение расследований инцидентов ИБ в соответствии с поставленной задачей без приостановки основных бизнес-процессов компании.

Подсистема обнаружения следов компрометации ИС обеспечивает:

- поиск следов атаки, связанных с подбором паролей;
- поиск нелегитимного ПО (программ, запрещенных корпоративными политиками);
- обнаружение закладок;
- проверку системы разграничения доступа и аутентификации (проверку прав доступа, наличия «дополнительных» пользователей с максимальными привилегиями);
- контроль целостности;
- обнаружение подозрительной активности (анализ журналов событий, поисковых запросов пользователей, подозрительных загрузок и т. п.);
- идентификацию злоумышленника (эвристические методики определения адреса источника атак).

Для классификации защитных мер, принимаемых в сложных информационных системах, можно использовать так называемую пятиуровневую модель информационной системы, которая выделяет: уровень пользователей, уровень приложения, уровень СУБД, уровень ОС и уровень сетевых служб.

[1] Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Система проверяет ИС на всех перечисленных уровнях кроме уровня пользователя, предоставляя специалистам практически всю информацию, которую можно собрать автоматизированными средствами. Подсистема обнаружения следов компрометации, в свою очередь, работает на всех пяти уровнях ИС.

2.2.4 Подсистема консолидации данных

Подсистема консолидации данных аккумулирует информацию от различных серверных компонентов Системы. В качестве хранилища информации при этом используется встроенная база данных Системы или корпоративная СУБД.

Собранные сведения используются в дальнейшем для анализа, построения отчетов, а также передачи данных в подсистему аналитической отчетности для получения целостной картины защищенности ИС.

2.2.5 Подсистема аналитической отчетности

Подсистема аналитической отчетности консолидирует и отображает настроенные показатели эффективности процессов ИБ по инфраструктуре компании в целом, с возможностью детализации по отдельным структурным и территориальным формированиям.

При этом обеспечивается получение данных:

- о текущем уровне защищенности инфраструктуры и его динамике;
- динамике устранения уязвимостей в разные периоды времени;
- состоянии Системы и ее компонентов в части работоспособности, необходимости обновления, активации лицензий;
- инвентаризации и контроле установленного ПО, соблюдении лицензионной политики и контроле использования запрещенного оборудования (USB-модемы, внешние накопители, мобильные устройства);
- состоянии и динамике прохождения проверок на соответствие техническим и внутренним стандартам компании.

Применение подсистемы аналитической отчетности обеспечивает следующие преимущества для бизнеса:

- возможность построения единой системы консолидированной отчетности для множества ИС,
- сокращение временных затрат на получение данных любого уровня и их анализ,
- возможность быстрого решения бизнес-задач,
- кардинальное снижение уровня затрат на разработку отчетов,
- интеграция с мобильными устройствами.

Подсистема аналитической отчетности, используя результаты работы Системы, позволяет проводить оперативный анализ данных о любой части инфраструктуры компании любого уровня детализации и за любой временной промежуток, помогает выстраивать процессы контроля защищенности, контроля эффективности ИБ, управления активами и соответствия стандартам.

2.2.6 Подсистема обновления

Подсистема обновления обеспечивает централизованное обновление всех компонентов Системы, получая данные от глобальных серверов обновления Системы.

Применение подсистемы обновлений позволяет:

- оптимизировать систему обновлений базы знаний и исполняемых модулей Системы;
- ограничить внешний интернет-трафик;
- провести обновление компонентов Системы в сетях, изолированных от сети Интернет.

Подсистема обновлений является важным компонентом Системы. Еженедельно по всему миру обнаруживаются и устраняются десятки уязвимостей, и команда Positive Technologies делает все возможное, чтобы поддерживать базу знаний в актуальном состоянии.

2.2.7 Подсистема управления

Подсистема управления предоставляет графический интерфейс управления Системой администраторам, операторам и пользователям Системы.

С ее помощью выполняются все действия в Системе:

- настройка компонентов Системы,
- управление процессом контроля защищенности,
- обработка результатов.

Подсистема управления обеспечивает идентификацию и аутентификацию пользователей Системы по уникальному идентификатору и паролю, а также ролевое управление доступом, при котором каждой роли назначается выполнение определенного набора задач в Системе.

2.3 Архитектура и компоненты системы

Логическая архитектура Системы, приведенная выше, реализована в виде отдельных программных компонентов.

MaxPatrol Server (MP-SRV)

MaxPatrol Server — это основной компонент Системы, выполняющий все основные функции распределенного сканера безопасности, а именно:

- сканирование,
- сбор данных и их обработку,
- сохранение результатов в базе данных,
- формирование отчетов.

MaxPatrol Server обеспечивает поддержку механизмов контроля защищенности, реализованных в Системе.

MaxPatrol Mobile Server (MP-M)

Компонент MaxPatrol Mobile Server — это специализированная версия MaxPatrol Server, оптимизированная для работы на мобильных компьютерах. Мобильный сервер поддерживает функцию удаленного управления с помощью MaxPatrol Console и выгрузки данных в MaxPatrol Consolidation Server.

Мобильный сервер имеет следующие отличительные особенности:

- лицензируется для использования только на мобильных компьютерах,
- имеет встроенную поддержку консолидации данных,
- поддерживает хранение данных только во встроенной СУБД,
- не имеет возможности подключения внешних сканеров.

MaxPatrol Mobile Server подходит, например, для проведения тестов на проникновение и аудита внешними консультантами.

MaxPatrol Scanner (MP-SCN)

В состав каждого MaxPatrol Server входит модуль MaxPatrol Scanner (сканирующее ядро), который выполняет собственно сканирование. Однако при необходимости к MaxPatrol Server могут быть добавлены дополнительные сканеры — для достижения необходимой производительности или для учета топологии сети при сканировании.

MaxPatrol Offline Scanner

Компонент предназначен для сканирования узлов, изолированных от локальной сети. Он позволяет произвести сканирование Windows-систем.

Установка компонента не требуется, его работа производится с Flash-носителя.

MaxPatrol Consolidation Server (MP-CS)

Сервер консолидации (MaxPatrol Consolidation Server), как было упомянуто ранее, аккумулирует информацию различных серверов MaxPatrol Server и позволяет строить целостную картину защищенности крупной распределенной информационной системы.

Между MaxPatrol Server и MaxPatrol Consolidation Server достаточно устанавливать связь периодически (результаты сканирования можно также передавать на съемных носителях).

MaxPatrol Report Portal (MP-RP)

Портал аналитической отчетности основан на платформе класса business intelligence, предоставляющей бизнес-аналитикам помощь в обработке поступающей информации. Инструменты BI, встроенные в портал аналитической отчетности, позволяют анализировать большие объемы данных, заостряя внимание пользователей лишь на мониторинге Системы и ключевых показателях эффективности.

MaxPatrol Local Update Server (MP-LUS)

Локальный сервер обновлений используется как единая точка поддержки базы знаний и исполняемых модулей компонентов в актуальном состоянии.

При использовании локального сервера обновлений можно загружать новые версии компонентов MaxPatrol из сети Интернет только на данный сервер. Благодаря MP-LUS обновления становятся доступными для других компонентов системы MaxPatrol.

MaxPatrol Console (MP-CON)

Консоль управления — неотъемлемый компонент Системы, представляющий собой инструмент для выполнения всех действий в системе MaxPatrol.

Пример развертывания Системы

Состав компонентов Системы, их количество и расположение варьируются в зависимости от множества факторов и являются предметом проектирования Системы.

Пример развертывания системы приведен на рис. 2.

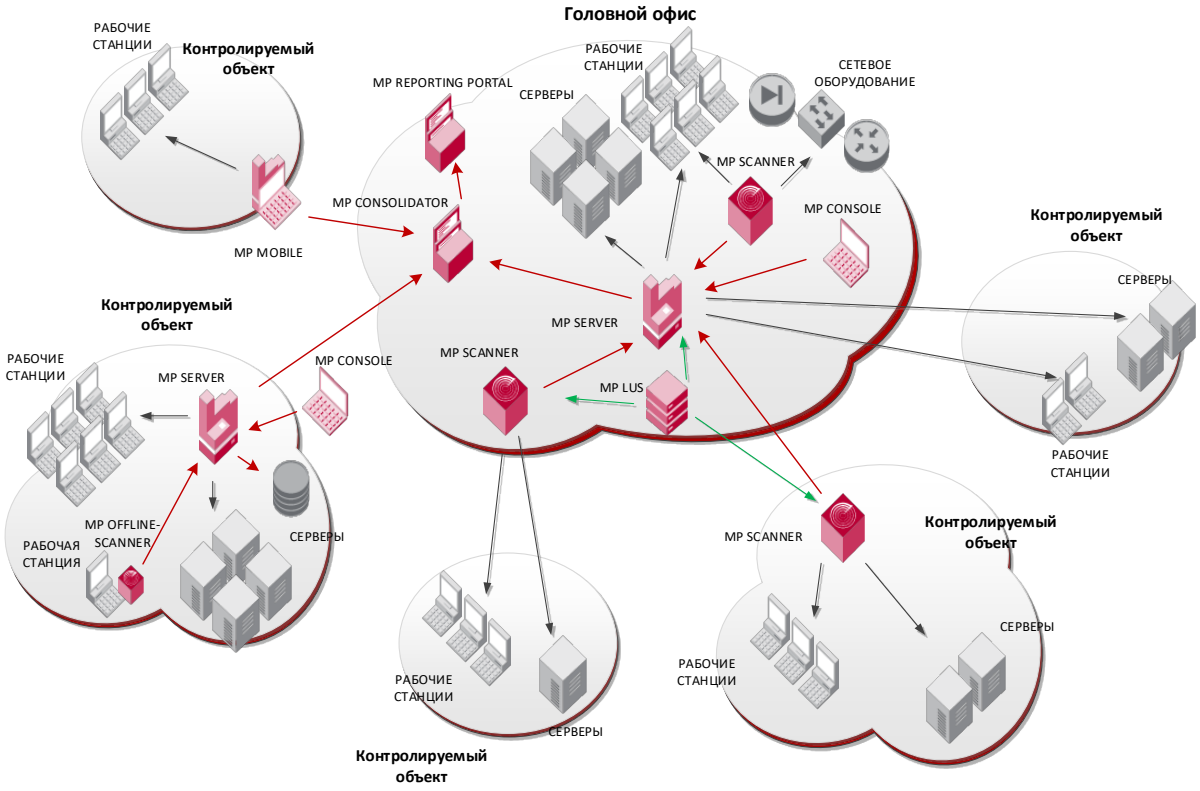

Рис. 2. Возможное размещение компонентов Системы

Компоненты MaxPatrol используют сеть для синхронизации и репликации данных, удаленного управления и выполнения других задач.

3 Интеграция со смежными системами

3.1 Интеграция с системами service desk

Процесс управления изменениями предполагает уменьшение или исключение отрицательного воздействия на ИС событий информационной безопасности — обнаруженных уязвимостей и недостатков ИС. Целью процесса управления изменениями являются регистрация и устранение известных уязвимостей в ИС компании.

Для расширения возможностей MaxPatrol в части управления изменениями рекомендуется дополнительно использовать следующие программные решения:

- MP Tracker — система учета и отслеживания заявок;
- WSUS Package Publisher — средство формирования и установки обновлений.

При помощи MP Tracker производится обработка поступившей информации, формирование заявок, работа по ним и дальнейшая передача в систему help desk (например, BPM производства TerraSoft).

3.2 Интеграция с SIEM

В компаниях с большим количеством устройств в сети администратору тяжело следить за изменениями и появлением новых угроз. В этом случае на помощь приходят системы управления событиями информационной безопасности (СУСИБ) и системы управления рисками.

Использование СУСИБ позволяет решить множество вопросов, таких как:

- применимость определенного типа атаки к конкретному узлу,
- оценка ущерба от совершенной атаки,
- отслеживание распространения атаки в режиме реального времени,
- идентификация источников распространения атаки,
- механизм реагирования на атаки через единый централизованный комплекс.

СУСИБ позволяют собрать данные от различных устройств сети и систем ИБ и представить их в консолидированном виде, с учетом ложных срабатываний. С этой целью в СУСИБ импортируются события от сканеров безопасности.

Системы управления рисками позволяют вычислять степень угрозы информационным активам компании, основываясь на ущербе, который может быть причинен активам в зависимости от расположения атакующего.

На данный момент MaxPatrol поддерживает интеграцию со следующими системами:

- Cisco Security Monitoring, Analysis, and Response System,
- Symantec Security Information Manager,
- ArcSight Enterprise Security Management,
- NetForensics SIM One,
- Skybox View.