Политика сетевой безопасности: Рекомендации и Описание технологических решений

Содержание

Введение

Без политики безопасности работоспособность сети может оказаться под угрозой. Создание политики начинается с оценки угрозы для сети и формирования рабочей группы, отвечающей за безопасность. Далее требуется реализация способов управления изменением политики и отслеживание нарушений безопасности сети. В заключение процедура пересмотра усовершенствует имеющуюся политику и адаптирует новые полученные сведения.

Данный документ состоит из трех разделов: подготовка, предотвращение и реагирование. Рассмотрим каждый из этих этапов более подробно.

Подготовка

Прежде чем применять политику безопасности, необходимо выполнить следующее:

- Создание правил политики использования.
- Проведение анализа риска.
- Создание структуры рабочей группы по безопасности.

Создание правил политики использования

Рекомендуется создать правила политики использования, описывающие обязанности и роли пользователей в отношении безопасности. Можно начать с общей политики, охватывающей все сетевые системы и данные в организации. Данный документ должен предоставлять широкому сообществу пользователей сведения, необходимые для понимания политики безопасности, её цели, рекомендации для усовершенствования мер обеспечения безопасности и определения их обязанностей в плане обеспечения безопасности. Если в организации составлен перечень действий, за которые могут последовать наказание или дисциплинарные взыскания в отношении сотрудника, эти действия, а также правила их обхода, должны быть четко сформулированы в данном документе.

Следующий этап — это создание правил допустимого использования для партнеров, чтобы партнеры понимали, какая информация им доступна, где эта информация находится, а также руководство сотрудниками организации. Необходимо четко описать все особые действия, которые относятся к атакам системы безопасности, и наказание, применяемое в случае обнаружения такой атаки.

В заключение создайте правила допустимого использования для администратора, поясняющие процедуры администрирования учетных записей пользователей, применения политики и анализа привилегий. Если в организации действуют особые политики в отношении паролей пользователей или последующей обработки данных, также полно и ясно опишите эти политики. Сравните политику с правилами политики допустимого использования для пользователей и партнеров, чтобы обеспечить их согласованность. Обязательно учтите требования к администраторам, перечисленные в политике допустимого использования, в планах обучения и оценках эффективности.

Проведение анализа риска

Анализ риска должен определить угрозы для безопасности сети, сетевых ресурсов и данных. Это не означает, что нужно определить все возможные точки входа в сеть или способы атаки. Цель анализа рисков заключается в определении частей сети, назначении степени угрозы для каждой части и применении соответствующего уровня безопасности. Это помогает поддерживать рабочий баланс между безопасностью и требуемым сетевым доступом.

Назначьте каждому сетевому ресурсу один из следующих трех уровней риска:

- **Низкий риск – системы и данные, компрометация которых (несанкционированный просмотр, повреждение или утрата данных) не приведет к нарушению деятельности организации, к юридическим или финансовым последствиям.** Атакованные система или данные не дают возможности доступа к другим сетевым ресурсам, их легко восстановить.
- **Умеренный риск – системы и данные, компрометация которых (несанкционированный просмотр, повреждение или утрата данных) приведет к небольшому нарушению деятельности организации, незначительным юридическим или финансовым последствиям или предоставит доступ к другим сетевым ресурсам.** Восстановление атакованной системы или данных несложное или процесс восстановления нарушает работоспособность системы.
- **Высокий риск – системы и данные, компрометация которых (несанкционированный просмотр, повреждение или утрата данных) приведет к чрезвычайно серьезному нарушению деятельности организации, значительным юридическим или финансовым**

последствиям или создаст угрозу здоровью и безопасности человека. Восстановление атакованной системы или данных сложное или процесс восстановления нарушает деятельность организации или работоспособность других систем.

Назначьте уровень риска следующим сетевым ресурсам: основные сетевые устройства, распределительные сетевые устройства, устройства доступа к сети, устройства наблюдения за сетью (SNMP-мониторы и RMON-агенты), устройства безопасности сети (RADIUS и TACACS), электронные почтовые системы, сетевые файловые серверы, сетевые серверы печати, сетевые серверы приложений (DNS и DHCP), серверы информационных приложений (Oracle и другие автономные приложения), настольные компьютеры и другие устройства (автономные серверы печати и сетевые аппараты факсимильной связи).

Сетевое оборудование – коммутаторы, маршрутизаторы, DNS-серверы и DHCP-серверы – может предоставлять доступ к другим сетевым ресурсам, поэтому является устройствами умеренного или высокого риска. Кроме того, возможно, что в результате выхода из строя такого оборудования сеть окажется неработоспособной. Такой отказ может нанести огромный ущерб деятельности организации.

После назначения уровня риска необходимо указать типы пользователей этой системой. Пять наиболее распространенных типов пользователей:

- **Администраторы – внутренние пользователи, отвечающие за сетевые ресурсы.**
- **Привилегированные – внутренние пользователи, которым требуется расширенный доступ.**
- **Пользователи – внутренние пользователи с общим доступом.**
- **Партнеры – внешние пользователи, которым требуется доступ к некоторым ресурсам.**
- **Другие – внешние пользователи или клиенты.**

Указание уровня риска и типа доступа, необходимых каждой сетевой системе, формирует основу следующей матрицы безопасности. Матрица безопасности обеспечивает быструю ссылку для каждой системы и начальную точку для принятия дополнительных мер безопасности, например создания соответствующей стратегии ограничения доступа к сетевым ресурсам.

Система	Описание	Уровень риска	Типы пользователей
Коммутаторы ATM	Основное сетевое устройство	Высокий	Администраторы для конфигурации устройств (только технические специалисты); остальные для использования в качестве транспорта
Сетевые маршрутизаторы	Распределительное сетевое устройство	Высокий	Администраторы для конфигурации устройств (только технические специалисты); остальные для использования в

			качестве транспорта
Коммутаторы в шкафу	Устройство доступа к сети	Средний	Администраторы для конфигурации устройств (только технические специалисты); остальные для использования в качестве транспорта
ISDN-сервер или сервер удаленного доступа	Устройство доступа к сети	Средний	Администраторы для конфигурации устройств (только технические специалисты); партнеры и привилегированные пользователи для специального доступа
Межсетевой экран	Устройство доступа к сети	Высокий	Администраторы для конфигурации устройств (только технические специалисты); остальные для использования в качестве транспорта
DNS-сервер и DHCP-сервер	Сетевые приложения	Средний	Администраторы для конфигурации; обычные и привилегированные пользователи для использования
Внешний сервер электронной почты	Сетевое приложение	Низкий	Администраторы для конфигурации; остальные для обмена почтовыми сообщениями между Интернетом и внутренним почтовым сервером
Внутренний сервер электронной почты	Сетевое приложение	Средний	Администраторы для конфигурации; остальные внутренние пользователи для использования
База	Сетевое	Умере	Администраторы

данных Oracle	приложение	нный или высокий	для системного администрирования; привилегированные пользователи для обновления данных; обычные пользователи для доступа к данным; остальные для частичного доступа к данным

Создание структуры рабочей группы по безопасности

Создайте универсальную рабочую группу по безопасности, возглавляемую менеджером управления безопасностью, включив в неё специалистов из каждой области деятельности организации. Члены этой группы должны быть знакомы с политикой безопасности и техническими аспектами проектирования системы безопасности и её применения. Как правило, это требует дополнительного обучения членов рабочей группы. Рабочая группа по безопасности отвечает за три области: разработка политики, применение и реагирование.

Разработка политики сфокусирована на создании и обзоре политик безопасности для организации. Требуется по меньшей мере ежегодный обзор анализа рисков и политики безопасности.

Практика является этапом, во время которого команда безопасности проводит анализ риска, утверждение запросов изменения безопасности, рассматривает сигналы о нарушении безопасности от обоих поставщиков и списка рассылки CERT, и превращает требования политики безопасности упрощенного языка в определенные технические реализации.

Последней областью ответственности является реагирование. Когда мониторинг сети часто определяет нарушение безопасности, именно члены рабочей группы по безопасности фактически выявляют и устраняют такое нарушение. Каждый член рабочей группы по безопасности должен детально знать функции безопасности, предоставляемые оборудованием в его/её области деятельности.

Обязанности рабочей группы в целом описаны выше, необходимо также определить индивидуальные роли и обязанности членов рабочей группы по безопасности в политике безопасности.

Предотвращение

Предотвращение можно разделить на две части: утверждение изменений политики безопасности и контроль безопасности сети.

Утверждение изменений политики безопасности

Под изменениями политики безопасности понимаются изменения сетевого оборудования, которые могут повлиять на безопасность сети в целом. Политика безопасности должна

формулировать требования к конфигурации безопасности простым, не техническим языком. Другими словами, вместо формулировки требования в форме "Межсетевой экран должен блокировать FTP-соединения внешних источников" используйте такую форму: "Внешним соединениям должно быть запрещено получать файлы из внутренней сети". Необходимо сформулировать уникальный набор требований именно для конкретной организации.

Рабочая группа по безопасности должна проанализировать список требований, сформулированных простым языком, чтобы определить решения по проектированию и конфигурации сети в соответствии с этими требованиями. После выработки рабочей группой необходимых изменений конфигурации сети для реализации политики безопасности, их можно применять ко всем будущим изменениям конфигурации. Рабочая группа по безопасности может анализировать все изменения, однако этот процесс позволяет им анализировать только те изменения, которые сопряжены с достаточным риском для обоснования принятия специальных мер.

Рабочей группе по безопасности рекомендуется анализировать изменения следующих типов:

- Любое изменение конфигурации брандмауэра.
- Любое изменение списков управления доступом (ACL).
- Любое изменение конфигурации простого протокола управления сетью (SNMP).
- Любое изменение или обновление ПО, отличающееся от утвержденного списка версий ПО.

Также рекомендуется следовать указаниям:

- Регулярно меняйте пароли доступа к сетевым устройствам.
- Ограничьте доступ к сетевым устройствам утвержденным списком лиц.
- Убедитесь, что текущие версии ПО сетевого оборудования и серверных сред соответствуют требованиям конфигурации политики безопасности.

Помимо следования этим указаниям, включите одного из членов рабочей группы по безопасности в согласительный совет по контролю изменений, чтобы отслеживать все изменения, рассматриваемые советом. Представитель рабочей группы по безопасности может отклонить любое изменение, которое посчитает изменением политики безопасности с тем, чтобы решение в отношении такого изменения принимала рабочая группа по безопасности.

Контроль безопасности сети

Контроль безопасности аналогичен мониторингу сети, за исключением того, что направлен на обнаружение изменений в сети, указывающих на нарушение безопасности. Отправной точкой для контроля безопасности является определение того, что считать нарушением. В разделе Проведение анализа риска определен необходимый уровень контроля на основе угрозы для системы. В разделе Утверждение изменений политики безопасности определены особые угрозы для сети. Рассматривая оба этих параметра, сформулируем ясное представление о том, что необходимо отслеживать и как часто.

В матрице анализа риска брандмауэр считается сетевым устройством с высоким риском, что указывает на необходимость контролировать его в режиме реального времени. Из раздела Утверждение изменений политики безопасности следует, что необходимо отслеживать все изменения в брандмауэре. Это означает, что опрашивающий SNMP-агент должен отслеживать такие события, как неудачные попытки входа, нехарактерный объем

трафика, изменения брандмауэра, предоставление доступа к брандмауэру и настройку соединений через брандмауэр.

Следуя этому примеру, создайте политику контроля для каждой области, определенной во время анализа рисков. Рекомендуется осуществлять контроль оборудования с низким риском еженедельно, с умеренным риском — ежедневно и с высоким риском — ежечасно. Для более оперативного обнаружения осуществляйте мониторинг с более коротким интервалом времени.

Наконец, политика безопасности должна определять способ уведомления рабочей группы о нарушениях безопасности. Как правило, первым обнаруживает нарушение ПО для наблюдения за сетью. Оно должно инициировать уведомление центра управления, который, в свою очередь, должен уведомлять рабочую группу по безопасности, например сообщением на пейджер, если нужно.

Ответ

Реагирование можно разделить на три части: нарушения безопасности, восстановление и анализ.

Нарушения безопасности

При обнаружении нарушения способность защитить сетевое оборудование, определить глубину проникновения в сеть и восстановить нормальное функционирование зависит от оперативности принятия решений. Заблаговременная выработка действий в таких ситуациях позволяет более организованно реагировать на вторжение.

Первое действие после обнаружения вторжения — это уведомление рабочей группы по безопасности. Без заранее установленной процедуры произойдет существенная задержка уведомления соответствующих специалистов для принятия надлежащих мер. Определите процедуру в политике безопасности, действующую 24 часа в сутки 7 дней в неделю.

Далее необходимо определить уровень полномочий, предоставляемый рабочей группе по безопасности для внесения изменений, и порядок внесения таких изменений. Возможны следующие действия для исправления недостатков:

- Внесение изменений для предотвращения доступа к атакованной системе.
- Изоляция атакованных систем.
- Обращение к оператору или поставщику услуг Интернета с целью отследить источник атаки.
- Использование записывающих устройств для сбора доказательств.
- Отсоединение атакованных систем или источника атаки.
- Обращение в правоохранительные органы или другие государственные учреждения.
- Отключение атакованных систем.
- Восстановление систем согласно списку приоритетов.
- Уведомление внутреннего руководства и юристов.

Обязательно подробно описывайте все изменения, которые можно вносить в политику безопасности без утверждения руководством.

Наконец, имеется две причины для сбора и сохранения сведений об атаке на систему

безопасности: чтобы определить степень поражения систем в результате атаки системы безопасности и преследовать в судебном порядке злоумышленников. Тип сведений и способ их сбора зависит от цели.

Для определения степени нарушения выполните следующие действия:

- Запишите событие, получив трассировки анализатора сетевых пакетов для сети, скопируйте файлы журналов, учетные записи активных пользователей и сетевые подключения.
- Ограничьте дальнейшую компрометацию путем блокирования учетных записей, отсоединения сетевого оборудования от сети и отсоединения от Интернета.
- Создайте копию атакованной системы для дальнейшего подробного анализа вреда и способа атаки.
- Проверьте наличие других следов атаки. Во многих случаях атака одной системы затрагивает другие системы и учетные записи.
- Сохраните и проанализируйте файлы журналов устройств безопасности, мониторинга сети, поскольку часто они содержат подсказки, позволяющие установить способ атаки.

Для возможности подачи судебного иска необходимо, чтобы юристы из юридического отдела организации ознакомились с процедурами сбора доказательств и привлечения руководства. Поскольку такое ознакомление повысит весомость доказательства в ходе рассмотрения дела в суде. Если нарушение сугубо внутреннее и вызвано действиями сотрудника, обратитесь в отдел кадров.

Восстановление

Восстановление нормального функционирования сети является конечной целью всех мер реагирования на нарушение безопасности. Определите в политике безопасности создание, защиту и доступность рабочих резервных копий. Поскольку каждая система имеет собственные средства и процедуры для резервного копирования, политика безопасности должна действовать как метаполитика, детализируя для каждой системы параметры политики безопасности, которые необходимо восстанавливать из резервной копии. Если для восстановления требуется одобрение, также опишите процесс получения одобрения.

Анализ

Процесс анализа является заключительным действием в ходе создания и поддержания политики безопасности. Необходимо проанализировать следующее: политика, состояние и применение.

Политика безопасности должна быть "живым" документом, адаптируемым к постоянно меняющейся среде. Сравнительный анализ действующей политики с передовым практическим опытом поддерживает сеть на современном уровне. Кроме того, проверьте веб-сайт CERT о полезных советах, методах, усовершенствованиях в защите и предупреждениях, которые могут быть включены в вашу политику безопасности.

Необходимо также анализировать состояние сети в сравнении с требуемым состоянием безопасности. Сторонняя компания, специализирующаяся в области безопасности, может попробовать проникнуть в вашу сеть и протестировать не только состояние сети, но и реагирование системы безопасности организации. Для сетей с высоким уровнем доступности рекомендуется проводить такой тест ежегодно.

Наконец, применение определяется как тренировка или тест для технических специалистов, чтобы проверить, насколько ясно они понимают, что нужно делать во время нарушения безопасности. Часто такая тренировка не оглашается руководством, а проводится вместе с тестом состояния сети. Этот анализ определяет пробелы в процедурах и подготовке персонала, чтобы можно было предпринять корректирующие меры.

Дополнительные сведения

- Описание технологических решений, рекомендации
- Техническая поддержка - Cisco Systems