Политика безопасности

Две основные схемы политики безопасности - безопасность периметра и глубокая защита. Безопасность периметра подразумевает построение крепости с высокими стенами, таким образом, что стоит поставить хороший межсетевой экран на входе в сеть, и внутри уже не нужно беспокоиться о безопасности. Однако, с появлением беспроводных сетей и соединением сетей организации и партнеров, твердая оболочка в политике безопасности периметра исчезает.

Задавайте правильные вопросы

Глубокая защита, напротив, предполагает размещение средств безопасности во всех точках сети. Например, межсетевой экран защищает от атак из Интернета, антивирусная система сканирует каждое сообщение электронной почты, а на каждом компьютере установлены программы для борьбы с вредоносными программами. Также используются шифрование и аутентификация при передаче данных между компьютерами. При проектировании системы безопасности следует учитывать простоту и минимализм. Сложность повышает риск ошибок и уязвимостей. Элементы безопасности должны быть встроены в систему, чтобы она была эффективной и гибкой. Удобство пользователей также должно приниматься во внимание при обеспечении безопасности. С технологическим развитием системы становится более безопасной и простой в использовании. Корпоративная безопасность относится к защите активов. Информация является наиболее важным активом для компании. Развитая программа безопасности определяет категории и классификацию информации. Категории включают публичную, конфиденциальную и строго конфиденциальную информацию компании. Защита информации включает защиту от изменения, утечки, кражи или уничтожения. Компании также должны обеспечивать доступность обслуживания и защиту от кражи ресурсов. Подготовка к расширенной интрасети и создание политики доступа требуют определенных шагов и понимания некоторых ключевых аспектов. Ниже приведены основные рекомендации:

1. Создание политики доступа: разработайте политику, которая будет распространяться на все уровни руководства в организации. Политика должна определить различные типы поддерживаемых соединений и общих ресурсов, а также указать офисы, которые могут устанавливать соединение с третьими сторонами.
2. Участие группы обеспечения безопасности: включите группу обеспечения безопасности вашей организации на ранней стадии разработки политики. Они смогут принести ценные знания и помочь определить наиболее важные аспекты безопасности для вашей network.
3. Политика ведения журналов: определите, что должно заноситься в журналы и на какой срок. Журналы могут быть полезны для отслеживания нарушений безопасности и ведения расследований, поэтому важно определить, какая информация должна быть записана и на какой период времени эта информация будет храниться.
4. Управление объемом журналов: учитывайте, что журналы могут занимать большие объемы дискового пространства, поэтому важно иметь временные ограничения на хранение журналов. Регулярно анализируйте и удаляйте неактуальные записи, чтобы освободить место на диске.
5. Логи в случае судебного разбирательства: проверьте, есть ли законодательные требования к хранению логов определенной даты в случае вызова в суд по уголовному делу. Если такие требования существуют, убедитесь, что ваша политика соответствует этим требованиям и предусматривает хранение логов на указанный срок.

6. Обучение персонала: обеспечьте обучение персонала организации по политике доступа и ведению журналов. Важно, чтобы все сотрудники понимали правила и процедуры, чтобы обеспечить безопасное использование интрасети.
7. Регулярное обновление политики: политика доступа и ведения журналов должна быть регулярно обновляется и предусматривать изменения в сетевом окружении, технологии и требования безопасности.

Получите поддержку высшего руководства

Правильное подготовка и проведение этих шагов помогут вашей организации создать эффективную политику доступа к расширенной интрасети и управления журналами, гарантируя безопасность и эффективность сети. Успешная программа безопасности требует поддержки высшего руководства, которое должно участвовать в создании политик и правил. Это поможет принимать правильные решения для бизнеса и обеспечит понимание руководства о принятых решениях. Чтобы получить авторитет как представитель группы обеспечения безопасности, нужно уметь ясно объяснять возможности, риски и преимущества на деловом языке. В случае несогласия с решениями руководства, нужно понять причины принятых решений и осознать, что у вас может не быть доступа к той же информации или знания бизнеса, как у руководства. Важно понять, что деловые решения учитывают технические и нетехнические потребности. Хороший представитель группы безопасности должен соглашаться с принятыми решениями руководства, которые считаются лучшими для компании. Необходимо найти баланс между построением безопасной системы и развитием бизнеса. Корпоративное решение по безопасности должно быть задокументировано, одобрено руководством и опубликовано в компании. Директор по безопасности должен иметь навыки ведения бизнеса и опыт в области защиты информации, а также возглавлять группу защиты информации с представителями из разных отделов компании. Он отвечает за разработку, одобрение и исполнение политик безопасности в компании.

Основы для технического персонала

Возникло множество вопросов и новых ситуаций. Чтобы обеспечить единую и эффективную программу безопасности, необходимо иметь одно место для их решения. Для этого нужен совет по политике безопасности или центральный орган, который будет заниматься деловыми и стратегическими решениями, а также контролировать безопасность. Если различные подразделения бизнеса имеют свою политику и контроль над созданием своих ресурсов, то они должны быть четко отделены от остальной компании. Управление несколькими автономными сетями в рамках одной компании может быть сложным и привести к нарушению неприкосновенности личной информации. Техническая эффективность безопасности зависит от ее самого слабого звена, поэтому необходим контроль над доступом к сети и возможность отслеживания нарушителей. Примером проблемы отсутствия центрального органа является компания, в которой каждое подразделение использовало свои политики безопасности без координации, что приводило к постоянным подозрениям на нарушения и затрудняло реакцию на них.

В качестве технического сотрудника группы обеспечения безопасности, вам нужно учитывать несколько принципов, включая обеспечение ежедневных рабочих потребностей пользователей, защиту от уязвимостей и атак, а также выбор правильной системы аутентификации и авторизации. Основные технологии безопасности, которые должны быть использованы во всех сетях, включают межсетевые экраны, фильтрацию электронной почты,

защиту от вредоносных программ и виртуальные частные сети. Необходимо уделять внимание этим технологиям, так как нарушители могут атаковать любой компьютер.

Для эффективной программы безопасности требуется жесткая компьютерная и сетевая инфраструктура, учет безопасности при ее построении, наличие стандартных конфигураций, возможность быстрого и недорогого создания и изменения безопасных систем, умение быстро устанавливать новые программы и патчи, а также умение отслеживать уровни патчей и версии. Постоянный процесс установки и модернизации обеспечивает противодействие атакам.

Важным элементом инфраструктуры для хорошей программы безопасности является процесс увольнения сотрудников. Он включает уведомление отдела кадров, который, в свою очередь, уведомляет другие отделы. Контрольный список для руководителя увольняемого сотрудника является полезным инструментом. Он напоминает руководителю вернуть ключи, карты доступа, удостоверение личности, средства аутентификации, оборудование и связаться с IT-подразделением для отключения доступа сотруднику.

Пример: безопасность через инфраструктуру

Небольшая группа консультантов по безопасности была привлечена на успешный сайт интернет-коммерции, который был взломан. Консультанты начали восстанавливать машины, но сайт рос так быстро, что они не успевали блокировать доступ новым злоумышленникам. Консультанты поняли, что проблема заключалась в отсутствии автоматизации загрузки, модернизации и обновления операционной системы. Для обеспечения безопасности сайта они построили инфраструктуру, позволяющую автоматически загружать операционную систему и устанавливать обновления. Таким образом, они смогли блокировать доступ злоумышленникам и обеспечить безопасные конфигурации всех машин.

Важный элемент системы безопасности - мощная система аутентификации с уникальным идентификатором для каждого человека и без учетных записей, используемых несколькими людьми одновременно. Система аутентификации работает с системой авторизации, которая определяет уровень доступа пользователя. Ролевые учетные записи предоставляют права на выполнение задач, недоступных для обычных учетных записей. Общие учетные записи следует исключить, так как они затрудняют отчетность и увеличивают риск утраты доступа. В некоторых операционных системах есть другие механизмы обеспечения доступа нескольким людям. Системы жесткой аутентификации обеспечивают большую степень уверенности в идентификации человека. Они могут быть основаны на биометрических или карманных устройствах, требующих физического устройства и секретных данных. Карманные идентификаторы могут быть удобными, если они имеют дополнительные функции и привязаны к важным личным вещам.

В выборе безопасного продукта для любой задачи следует учитывать несколько факторов. Продукт, чувствительный к безопасности, может быть использован третьей стороной с ограниченным доступом, являться частью системы аутентификации, доступен из Интернета или иметь доступ в небезопасную сеть, предоставлять доступ к важным данным или системам. При оценке его безопасности важно также учесть четыре фактора: простоту использования, текущее обслуживание и направленность поставщика, функциональность и интеграцию. Простые системы обычно более надежны и безопасны, чем сложные. При выборе продукта важно также ознакомиться с его дизайнерами и программистами, изучить их предыдущие работы и решения проблем. Открытый исходный код, хотя и может иметь уязвимости, проверяется многими людьми, что может помочь в быстром обнаружении проблем и разработке патчей. Защита закрытого исходного кода за счет его неизвестности неэффективна, так как злоумышленники в любом случае могут находить уязвимости.

Простота использования. Легко ли понять и проверить конфигурацию и случайно настроить приложение небезопасным? Как взаимодействуют компоненты и как изменение конфигурации в одной области влияет на другие? Обнаруживает ли приложение конфликты конфигурации и сколько времени занимает обучение новых сотрудников?

Функциональность. Продукт должен предоставлять только нужные функции и избыточная функциональность может быть проблемой, если ее нельзя отключить.

Связь с поставщиком. Патчи и обновления важны для безопасности, а также возможность сообщать о проблемах поставщику и ожидать их быстрого устранения. Бесплатная версия коммерческого продукта может обеспечить лучшее обслуживание. Насколько поставщик уделяет внимание безопасности и каков его механизм уведомления о проблемах?

Интеграция. Хорошая совместимость с остальной сетевой инфраструктурой и поддержка протоколов межсетевым экраном важны для продукта. Использование других протоколов и возможность отправки логов на центральный узел также важны.

Расходы на содержание. Время настройки и установки программы, возможность автоматической загрузки и стандартизации настроек, объемы ежедневного обслуживания и знакомство людей с системой важны для расходов на содержание.

Перспективы. Масштабируемость, соответствие разработки продукта направлению компании, продолжительность поддержки и регулярность выхода новых релизов важны для продукта. Распространенность на рынке также упрощает наем людей, знакомых с продуктом.

Мы определяем проверку в широком смысле, чтобы охватить все вопросы:

1. Проверка систем безопасности на соответствие политикам и структуре.
2. Проверка списков сотрудников и подрядчиков по базам данных аутентификации и авторизации.
3. Физическая проверка серверных, кабельных и телекоммуникационных шкафов на наличие инородных устройств.
4. Проверка наличия последних обновлений по безопасности на важных машинах.
5. Сканирование важных сетей для проверки предоставляемых услуг.
6. Запуск сложных, глубинных атак против конкретных областей инфраструктуры с четко определенными критериями успеха и ограничениями.

Также рекомендуется:

1. Вести и обрабатывать логи чувствительных к безопасности машин и приложений. Логи являются важным источником информации о безопасности и могут помочь отследить атаку.
2. Анализировать логи для обнаружения и определения масштабов и серьезности атаки. Логи должны быть обработаны для извлечения полезной информации и архивироваться на определенный период времени.
3. Собирать все логи, важные с точки зрения безопасности, в одной централизованной точке для обработки и сравнения информации с различных машин.
4. Не оставлять важные логи на чувствительных к безопасности машинах. Центральный узел логов должен быть хорошо защищен, чтобы обеспечить их целостность.

Также рекомендуется проверить структуру сети на наличие аномалий, например, странные маршруты или неожиданный трафик из неожиданных источников. Также рекомендуется использовать метод war-dialing для проверки модемов на неожиданных номерах.

Группе безопасности нужен доступ к различным ресурсам. Наличие большого количества связей в отрасли позволяет им быть информированными о действиях других компаний и

мнениях других людей. Это также позволяет им оценивать работу компании в сравнении с другими и узнавать о происхождении атак раньше других. Связи устанавливаются через конференции и межфирменные рабочие группы по безопасности. Помимо этого, группе безопасности нужны разные навыки и должности, такие как разработчик политик, архитектор безопасности, конструктор, операторы, аудитор, менеджер рисков и специалисты по реакции на происшествия. Разработчик политик пишет корпоративные политики и должен знать политики других компаний, чтобы определить лучшие практики. Архитектор безопасности представляет группу перед сотрудниками компании и занимается связями внутри компании. Он проектирует систему безопасности и следит за требованиями бизнеса и ключевых людей. Конструктор реализует проекты архитектора и работает над оценкой продуктов. Он также обучает операторов работе с системами.

Матрица авторизации

В этом разделе рассмотрим создание процесса урегулирования инцидентов в области безопасности путем подготовки эффективной реакции и изучения влияния политики компаний на работу группы. Для эффективного урегулирования инцидентов необходима предварительная подготовка. Группа не может быть сформирована во время кризиса. Парадоксально, но лучшее время для создания группы - это когда она вам не нужна. С ростом компании возрастает вероятность, что удар по репутации от происшествия окажется более значимым, чем потеря данных или производительности. Последствия недостаточно эффективного урегулирования - попадание на первые полосы газет, что может повлиять на курс акций и доверие клиентов. При организации группы реагирования необходимо определить, каким образом будут передаваться сообщения о возможных инцидентах. Откуда поступают сообщения и как они обрабатываются? Когда вы хотите реагировать на инциденты в области безопасности? Например, как сообщить о потенциальном инциденте в нерабочее время? Первый этап процесса должен быть интегрирован в стандартные процедуры сообщения о проблемах. Пользователи обычно не могут определить, является ли происшествие инцидентом в области безопасности. Человек, получающий сообщение, должен знать последовательность действий по обработке сообщения о потенциальном инциденте в области безопасности и определению, к кому передать это сообщение. В группе должны быть сотрудники, связанные с получением сообщений и определением серьезности инцидента. Они также должны входить в группу обеспечения безопасности. Если информация не передается соответствующим людям, это плохо. Рекомендуется привлечение сторонних консультантов по безопасности в качестве аудиторов, чтобы получить независимое мнение о работе группы безопасности и свежий взгляд на безопасность компании. Они должны быть рекомендованы и могут работать с техническим персоналом, чтобы компания могла получить максимальную выгоду от сотрудничества. Сторонние аудиторы обладают преимуществом независимости, отсутствия ожиданий и предубеждений, а также опыта в отрасли, что позволяет им предоставить высшему руководству дополнительные данные и возможные подходы к безопасности. Они также могут помочь внутренней группе безопасности получить больше ресурсов и идей. Сторонняя проверяющая группа должна проводить глубокие атаки против определенных областей и сканирование сетей и точек удаленного доступа, чтобы более реалистично проверить безопасность компании. Информация о программе по информированию в области социальной инженерии также важна.

Внутренние проверки

Группа обеспечения безопасности должна быть информирована о новых разработках бизнеса, знать особенности компании и ключевых игроков при разработке политики безопасности. Они должны иметь тесные связи с группой системных администраторов и юридическим

отделом компании. IP-менеджер может возглавить группу защиты информации, включая представителей разных отделов компании. Он также может предоставить информацию о планируемых проектах и помочь с контрактными соглашениями и обучением Продажа безопасности подобна страхованию, хотя сразу не приносит видимой выгоды, за исключением психологического комфорта. Однако в отличие от страхования, клиенты могут оценить потенциальные расходы при отсутствии безопасности и понимать ее значимость. Однако, в случае с безопасностью сложно оценить пользу, если группа безопасности не предоставляет дополнительные данные о неудавшихся атаках, глобальных тенденциях в области атак и потенциальных убытках компании.Чтобы продавать безопасность высшему руководству, людям, использующим системы, и системным администраторам, необходимо учитывать их специфические требования. Для продажи безопасности высшему руководству, необходимо показать, как она помогает компании выполнить свои обязательства перед акционерами и клиентами, а также как она может быть конкурентным преимуществом. При попытке продажи безопасности другим группам, важно показать, что ее покупка отвечает их основным интересам.Кроме того, соберите данные о вложениях в безопасность конкурентов или других компаний схожего размера в отраслях. Руководству будет полезно иметь возможность оценить, достаточно ли средств тратится на безопасность. Если возможно, создайте метрику для оценки работы группы безопасности и рассмотрите возможность привлечения сторонней группы для анализа рисков компании. Связи в отрасли безопасности - хороший источник информации о атаках, уязвимостях и мнениях о продуктах и технологиях. Посещение конференций помогает завести эти связи и опережать конкурентов. Важно быть активным участником сообщества и строить отношения с другими участниками. Также необходимо быть в курсе новых технологий и уметь отличать полезные продукты от «панацей». Метрика в безопасности помогает оценить качество работы группы безопасности и ее выгоду для компании. Следует использовать стороннюю проверку и собирать данные о предпринятых или потенциальных атаках. Хорошая метрика помогает обеспечить доверие других сотрудников и показывает выполненную работу и проблемные области.

Ресурсы

В данном разделе мы представим краткий обзор этапов разработки адекватной программы безопасности компании в зависимости от ее размера и назначения. Этот раздел является лишь руководством для создания понимания о том, насколько вы отстаете или опережаете основные тенденции и как должна развиваться ваша программа безопасности с ростом компании. Мы рассмотрим простую программу безопасности для малых, средних и крупных компаний, сайта электронной коммерции и университета. В этих примерах предполагается, что наиболее типичное количество сотрудников для малой компании – от 20 до 100, для средней – от 1000 до 3000, а для крупной – более 20 тыс. Малая компания В малой компании с одним или двумя системными администраторами обеспечение безопасности не потребует больших усилий. В компании должна быть политика допустимого использования, а также политика мониторинга и неприкосновенности личной информации. Системные администраторы, скорее всего, будут знать все, что происходит в компании, и им не понадобится участие в формальных группах. Главное для компании будет безопасность периметра, особенно в начальном этапе. Системные администраторы должны продумать механизм жесткой аутентификации, вовлечь руководство в необходимость этого и определить оптимальное время для внедрения.Если малая компания только начинает свою деятельность, особенно в компьютерной отрасли, инженерному отделу может потребоваться доступ в Интернет для получения информации о новых технологиях. Компания должна определить, справится ли с этим среда разработки, и если нет, то как защитить инженерный отдел и другие части компании от него. Средняя компания В средней компании

должна быть небольшая группа постоянно работающих системных администраторов. Один из них должен выполнять работу архитектора безопасности, а остальные – быть конструкторами и играть второстепенные роли. Ответственность за безопасность должна быть централизована, даже если системные администраторы занимаются безопасностью в удаленных офисах. Удаленные администраторы должны описывать свою работу перед группой безопасности. Архитектор безопасности будет заниматься реализацией, а конструкторы – выполнением операторской работы. Политики будут определяться архитектором и возможно, руководителем группы. Проверки могут проводиться конструкторами или архитектором, а для создания программы проверки они могут привлечь сторонних консультантов.В компании должны быть все основные политики, а также простая программа проверки. Должна быть группа защиты информации с представителями из разных отделов, а также программа информирования о безопасности, проводимая этой группой. Крупные компании сталкиваются с проблемами, связанными с их размером. В таких компаниях затрудняется реагирование на происшествия, согласованность политик и отслеживание изменений.

В крупной компании необходимы выделенные сотрудники для выполнения функций обеспечения безопасности. Компания может быть разделена на административные подразделения бизнеса, каждое из которых имеет свои политики и периметр безопасности. В каждом подразделении должны быть все необходимые политики безопасности.

Требуется широкая инфраструктура безопасности с программой проверки. В каждом подразделении должны быть группы, занимающиеся программами безопасности и информирования о безопасности.

В областях физической и электронной безопасности компании всегда повышены требования. Крупные компании обычно доверяют сотрудникам меньше, так как есть больше возможностей для раскрытия информации. Компании могут иметь соединения с третьими сторонами и системы разработки, требующие дополнительных ограничений и контрактов. Слияния и поглощения создают новые проблемы, такие как урегулирование различий в политиках безопасности, культуре и отношении, а также интеграция сетевого оборудования.У компании, занимающейся электронной коммерцией, есть особые требования. Внутри компании должно быть четкое разделение между "корпоративными" машинами и машинами "сетевого обслуживания". В компаниях электронной коммерции должен быть по крайней мере один сотрудник-профессионал в области безопасности. Компании также требуется быстро расширять свой персонал безопасности.Для управления доступом к машинам и сетевому обслуживанию такой компании требуются отдельные политики. Компания должна также обеспечивать безопасность платежной информации клиентов и предотвращать DoS-атаки на свою инфраструктуру сетевого обслуживания.