8. Лекция: Обеспечение информационной безопасности

Рассмотрены вопросы обеспечения информационной безопасности, оценки стоимости проведения мероприятий по безопасности. Уделено внимание вопросам разработки и реализации политики безопасности, а также аудита систем.

Обеспечение информационной безопасности - это процесс, опережающий управление риском, а не следующий за ним. В отличие от ответной модели, когда вначале происходит чрезвычайное происшествие, а только потом принимаются меры по защите информационных ресурсов, предупредительная модель работает до того, как что-то случится.

В ответной модели общие затраты на безопасность неизвестны.

Общие затраты на безопасность = Стоимость ущерба от происшествия + Стоимость контрмер

К сожалению, мы не узнаем стоимость ущерба от происшествия, пока оно фактически не произойдет. Поскольку организация не предпринимает никаких шагов для предотвращения инцидента, нет никакой возможности узнать величину возможного ущерба. Следовательно, нельзя оценить риск, пока не произойдет реальный инцидент.

К счастью, организация может сократить затраты на обеспечение информационной безопасности. Правильное планирование и управление риском позволят значительно снизить, если не исключить, величину ущерба от происшествия. Если принимались правильные меры, и инцидент был предотвращен, то величина затрат составляет:

Общие затраты на безопасность = Стоимость контрмер

Также обратите внимание, что

Стоимость происшествия + Стоимость контрмер >> Стоимость контрмер

Предупредительное принятие необходимых мер - это правильный подход к информационной безопасности. В этом случае организация определяет свои уязвимые места, выявляет величину риска и выбирает экономически эффективные контрмеры. Это первый шаг в процессе обеспечения информационной безопасности.

Обеспечение информационной безопасности - это непрерывный процесс, включающий в себя пять ключевых этапов (см. рис. 8.1):

- оценку;

- политику;
- реализацию;
- квалифицированную подготовку;
- аудит.

Каждый из этих этапов по отдельности повышает уровень защищенности организации; однако только взятые вместе они обеспечивают основу, которая позволит эффективно управлять риском.

Рис. 8.1. Обеспечение информационной безопасности

Оценка стоимости

Процесс обеспечения информационной безопасности начинается с оценки имущества: определения информационных активов организации, факторов, угрожающих этой информации, и ее уязвимости, значимости общего риска для организации. Это важно просто потому, что без понимания текущего состояния риска невозможно эффективно выполнить программу защиты этих активов.

Данный процесс выполняется при соблюдении метода управления риском. Сразу после выявления риска и его количественной оценки можно выбрать рентабельную контрмеру для уменьшения этого риска.

Цели оценки информационной безопасности следующие:

- определить ценность информационных активов;
- определить угрозы для конфиденциальности, целостности, доступности и/или идентифицируемости этих активов;
- определить существующие уязвимые места в практической деятельности организации;
- установить риски организации в отношении информационных активов;
- предложить изменения в существующей практике работы, которые позволят сократить величину рисков до допустимого уровня;

- обеспечить базу для создания соответствующего проекта обеспечения безопасности.

Перечисленные цели не изменят тип оценки, принятый в организации. Однако степень приближения каждой цели зависит от масштабов работы.

Перечислим пять основных видов оценки.

- Оценка уязвимых мест на системном уровне. Компьютерные системы исследованы на известные уязвимости и простейшие политики соответствия техническим требованиям.
- Оценка на сетевом уровне. Произведена оценка существующей компьютерной сети и информационной инфраструктуры и выявлены зоны риска.
- Общая оценка риска в рамках организации. Произведен анализ всей организации с целью выявления угроз для ее информационных активов. Установлены уязвимости в местах обработки информации по всей организации. Исследована информация, представленная как в электронном виде, так и на физических носителях.
- Аудит. Исследована существующая политика и соответствие организации этой политике.
- Испытание на возможность проникновения. Исследована способность организации реагировать на смоделированное проникновение. Этот тип оценки пригоден только для организаций с высокоразвитой программой безопасности.

В последующем обсуждении предположим, что во время проведения аудита будет проведено также испытание на возможность проникновения. Эти виды оценки подразумевают некоторое предварительное понимание рисков и наличие опыта в практической реализации системы безопасности и управления риском. Ни один из видов оценки не подходит, когда организация пробует понять текущее состояние безопасности.

Необходимо провести оценку собранной информации из трех главных источников:

- опрос работников;
- проверка документации;
- инвентаризация.

Нужно проводить опрос работников, которые будут обеспечивать информацией существующие системы безопасности и направления деятельности организации. Не рекомендуется смешивать служебный персонал и руководителей. Опрашивающий должен непринужденно направить разговор на задачи оценки и на то, как человек может содействовать защите информационных активов. Имейте в виду, что

сотрудник может заверить вас, что ни одно из направлений обеспечения информационной безопасности активов за ним не закреплено.

Обязательно изучите все существующие политики, связанные с безопасностью. Исследование не должно ограничиваться только готовыми документами, внимательно прочитайте и черновики.

Последний этап сбора информации - инвентаризация всех материальных ценностей организации.

При проведении оценки изучают следующие моменты:

- сетевое окружение;
- физические меры безопасности;
- существующие политики и процедуры;
- меры предосторожности, принятые на местах;
- осведомленность работников в вопросах безопасности;
- персонал;
- загруженность персонала;
- взаимоотношения работников;
- строгое соблюдение работниками установленной политики и мероприятий;
- специфику деятельности.

Сетевое окружение

Обычно в сетевом окружении находятся открытые точки доступа к информации и системам. Исследование сети начинают с построения диаграммы сети и рассматривают каждую точку возможного подключения.

Примечание

Диаграмма сети зачастую бывает неточной или устаревшей, следовательно, крайне важно, чтобы она была не единственным источником информации, используемым для определения критических сетевых компонентов.

Расположение серверов, рабочих станций, доступ в интернет, соединения наборного доступа, соединения с удаленными офисами и партнерами должны полностью представлены на диаграмме сети. На основании диаграммы и информации, полученной от системного администратора, собираются следующие данные:

- тип и количество систем в сети;
- операционные системы и их версии;
- топология сети (коммутаторы, маршрутизаторы, мосты и т. д.)
- точки доступа к интернету;

- использование интернета;
- типы, количество и версии всех межсетевых экранов;
- точки входа соединений наборного доступа;
- беспроводные точки доступа;
- тип удаленного доступа;
- топология глобальной сети;
- точки доступа в удаленных офисах;
- точки доступа других организаций;
- расположение веб-серверов, FTP-серверов и почтовых шлюзов;
- используемые протоколы;
- лица, осуществляющие управление сетью.

После определения архитектуры сети выявляются внутренние защитные механизмы сети:

- списки управления доступом маршрутизаторов, правила межсетевых экранов на всех точках доступа в интернет;
- механизмы идентификации, используемые для удаленного доступа;
- защитные механизмы во всех точках доступа других организаций;
- механизмы шифрования, используемые для передачи и хранения информации;
- механизмы шифрования, используемые для защиты переносных компьютеров;
- антивирусные системы, установленные на серверах, рабочих станциях и службах электронной почты;
- настройки безопасности сервера.

Если сетевые и системные администраторы не предоставят подробной информации о настройках безопасности сервера, то вам потребуется обследование сервера. Оно должно охватить требования к паролям, настройки аудита для каждой системы, а также используемые обновления системы и программ.

Узнайте у сетевых администраторов об использующейся системе управления сетью. Необходимо собрать информацию о типах оповещений и лицах, которые осуществляют мониторинг системы и сбор данных. Эта информация пригодится для выявления нарушителей в случае обнаружения вторжения администраторами системы.

Наконец, необходимо выполнить сканирование всех систем на предмет обнаружения уязвимых мест. Это можно сделать с помощью компьютера, размещенного внутри системы (внутреннее сканирование) или размещенного в интернете, за пределами межсетевых экранов организации. Оба результата очень важны, так как позволят выявить уязвимые места, которые могут

использоваться злоумышленниками, которые находятся в вашей организации или за ее пределами.

Совет

Имейте в виду, что сетевые администраторы могут не знать обо всех точках удаленного доступа в организации.

Физическая безопасность

Физическая безопасность помещения - важнейшая составляющая системы защиты информации. Определение мер физической безопасности включает управление физическим доступом к подразделениям, а также к секретным отделам и помещениям. Например, центр регистрации и обработки данных должен иметь собственную систему контроля физического доступа. Как минимум, этот доступ должен быть строго ограничен. При определении мер физической безопасности необходимо выявить следующее:

- тип физической защиты здания, офисных помещений, документов на бумажных носителях и центра обработки данных;
- наличие ключей у персонала;
- засекреченные помещения здания или отдела (исключая центр обработки данных).

Определите расположение линий коммуникации внутри помещений и те места, где линии коммуникации входят в здание. В этих местах могут быть размещены подслушивающие устройства, поэтому подобные точки нужно включить в список критических областей. Включите в список и помещения, где возможно аварийное отключение.

Объектами физической безопасности являются источники энергии, системы контроля состояния окружающей среды и системы противопожарной безопасности, используемые в центре обработки данных. Соберите следующую информацию об этих системах:

- какую мощность потребляет подразделение;
- какую мощность потребляет центр обработки данных;
- какие типы источников бесперебойного питания установлены;
- как долго имеющиеся источники бесперебойного питания смогут поддерживать работоспособность системы;
- какие системы соединены с источниками бесперебойного питания;
- кто будет извещен в случае отключения электроэнергии;
- какая система контроля состояния окружающей среды подключена к источнику бесперебойного питания;
- какая система контроля состояния окружающей среды связана с центром обработки данных;

- кто будет извещен в случае выхода из строя системы контроля состояния окружающей среды;
- какой вид системы противопожарной безопасности установлен в центре обработки данных;
- может ли система противопожарной безопасности центра обработки данных среагировать на пожар, не угрожающий центру.

Примечание

Многие правила противопожарной безопасности требуют установки разбрызгивателей во всех частях здания. В последнем случае необходимо использовать систему пожаротушения, которая не использует воду.

Политики и процедуры

Многие политики и процедуры организации связаны с безопасностью. При проведении оценки должны быть исследованы следующие документы:

- политика безопасности;
- информационная политика;
- план восстановления в случае чрезвычайных происшествий;
- процедуры контрмер на чрезвычайное происшествие;
- политика и процедуры резервного копирования;
- справочное руководство работника или инструкции;
- процедуры найма-увольнения работников;
- принципы конфигурирования систем;
- правила межсетевых экранов;
- фильтры маршрутизатора;
- политика сексуальных домогательств на рабочем месте;
- политика физической безопасности;
- методология разработки программного обеспечения;
- методология смены программного обеспечения;
- телекоммуникационные политики;
- диаграммы сети;
- организационная диаграмма.

После получения вышеуказанных политик и процедур каждая из них исследуется на предмет значимости, правомерности, завершенности и актуальности.

Политика или процедура должна быть значимой для практической деловой деятельности, существующей в организации в настоящее время. Общие политики не всегда работают, поскольку не учитывают особенности той или иной организации. Процедуры должны определять методики выполнения текущих задач.

Политики и процедуры должны соответствовать цели, определенной в документе. При исследовании документа на правомерность проверяйте каждое требование на соответствие установленной цели политики или процедуры. Например, если целью политики безопасности является определение требований безопасности ко всем установленным компьютерным системам, она не должна описывать особые конфигурации для майн-фреймов, рабочих станций и клиент-серверных систем.

Политики и процедуры должны охватывать все стороны деятельности организации. Нередко можно обнаружить, что отдельные аспекты деятельности не нашли свое отражение в политике либо вовсе отсутствовали на момент создания политики. Изменения в технологиях очень часто приводят к изменениям в политиках и процедурах.

Политики и процедуры могут устаревать со временем. Причиной этому является не злоупотребление, а, скорее, небрежность. Морально устаревший документ становится бесполезным и "умирает". Организации в своей деятельности не стоят на месте, меняются системы и сетевое окружение. Если политики не адаптируются к появлению новых систем или новых направлений деятельности, то она теряет свое значение. Все политики и процедуры необходимо своевременно и обоснованно обновлять.

Кроме вышеописанных документов, в процессе оценки необходимо исследовать программу в области информированности о проблемах безопасности и материалы, используемые в соответствующих тренингах. Сравните эти материалы с существующими политиками и процедурами, чтобы увидеть, насколько точно они отражают организационную политику.

И в заключение, процедура оценки должна включать исследование сведений о недавних происшествиях и проверках. Это не значит, что вы можете всецело положиться на результаты предыдущей работы, скорее, требуется установить, есть ли прогресс в существующих сферах деятельности.

Меры предосторожности

Меры предосторожности обычно используются для восстановления работоспособного состояния после каких-либо инцидентов. Основными составляющими являются системы резервного копирования и план восстановления на случай чрезвычайных происшествий.

При оценке пригодности систем резервного копирования исследование должно быть глубже, чем просто просмотр политики и процедур резервного копирования. Необходимо произвести опрос системных операторов, чтобы понять, как на самом деле используется система. Получите ответы на следующие вопросы.

- Что представляет собой система резервного копирования?
- Для каких систем проводится резервное копирование и как часто?
- Где хранятся резервные копии?
- Как часто резервные копии перемещаются в архив?
- Выполнялась ли когда-либо проверка резервных копий?
- Как часто должны использоваться резервные копии?
- Повреждались когда-либо резервные копии?
- Как часто данные нуждаются в резервном копировании?

Ответы на эти вопросы прольют свет на эффективность существующих систем резервного копирования.

Исследуйте план восстановления на случай чрезвычайных происшествий, обращая внимание на его полноту. То, как план используется на самом деле, нельзя определить, просто читая его. Опросите служащих, которые будут использовать план, чтобы определить, использовался ли план когда-либо и был ли он действительно эффективен. Задайте им следующие вопросы.

- Использовался это план когда-либо?
- Какой был результат?
- Тестировался ли план?
- Какое оборудование имеется в распоряжении для устранения последствий бедствия?
- Какое альтернативное местоположение доступно?
- Кто несет ответственность за действия по устранению последствий бедствия?

Осведомленность

Политики и процедуры работают замечательно и позволяют значительно улучшить безопасность организации, если им следуют работники вашей организации. Проводя оценку, оставьте время для беседы с постоянными сотрудниками (не имеющими обязанностей управляющих или администраторов) для определения их уровня осведомленности по вопросам политик и процедур компании, а также практических положений должной безопасности. Обойдите офисные помещения для поиска признаков несоблюдения политик. Обратите внимание на наличие бумажных листков с написанными паролями и на системы, оставленные в активированном состоянии после регистрации пользователей.

Осведомленность администратора также важна. Очевидно, что они обязаны знать политику компании по вопросам конфигурирования систем. Администраторы должны быть осведомлены об угрозах и уязвимостях, о признаках вторжений в системы. Главное, они должны знать, какие действия необходимо предпринять при обнаружении атаки.

Вопрос к эксперту

Вопрос. Имеет ли значение осведомленность сотрудников?

Ответ. Да, она имеет большое значение. Сотрудники имеют доступ и нужные сведения, следовательно, являются возможными источниками угроз. Именно поэтому злоумышленники проявляют к ним повышенный интерес. Есть много методов социального инжиниринга, позволяющих нарушителю достигнуть своей цели, когда все предыдущие попытки натолкнулись на надежную систему безопасности.

Человеческий фактор

Служащие являются одним из самых важных факторов, влияющих на общую безопасность. Отсутствие навыков или, наоборот, их избыток может стать причиной выхода из строя хорошо продуманных программ безопасности. Проверьте уровень навыков персонала, отвечающего за вопросы безопасности, и администраторов, чтобы определить, способны ли они выполнять программу обеспечения безопасности. Персонал, отвечающий за вопросы безопасности, должен понимать свою работу в плане общей политики так же хорошо, как разбираться в последних разработках в своей области. Администраторы должны иметь соответствующие навыки, чтобы на высоком уровне осуществлять управление системами и сетевым окружением внутри организации.

Все пользователи должны иметь базовые навыки в области компьютерных технологий. Тем не менее, при наличии более глубоких знаний (например, у разработчиков программного обеспечения) возможно возникновение дополнительных проблем в сфере безопасности. Если пользователи достаточно хорошо владеют компьютерными технологиями, то им не составит труда установить на свои рабочие станции дополнительное программное обеспечение, которое может повлиять на общую безопасность организации. Эти люди с большей вероятностью обладают навыками и знаниями, необходимыми для использования уязвимостей внутренних систем.

От аудиторов организации потребуется обследование систем и сетей как часть их рабочего задания. В этом случае аудиторы, разбирающиеся в существующих технологиях и системах, используемых внутри организации, быстрее смогут отыскать проблемы.

Загруженность персонала

Даже очень квалифицированные и сообразительные работники не смогут поддерживать систему безопасности, если они перегружены работой. При возрастании объема работ первым делом будут забыты именно вопросы

безопасности. Администраторы не проверяют записи журналов, пользовательские пароли на совместно используемые ресурсы, а менеджеры забывают о том, что говорилось на тренинге по защите систем. Тут даже самая серьезная организация с тщательно разработанными политиками и процедурами столкнется с уязвимостями.

Однако проблема может быть вовсе не такой страшной, как кажется. В процессе оценки необходимо определить, является ли большой объем работы временным явлением либо это постоянная практика, действующая в организации.

Отношение

Отношение управленческого персонала к вопросам безопасности - еще один ключевой аспект в общей среде безопасности. Это отношение определяется при назначении ответственных за безопасность внутри организации. Другая сторона этого отношения проявляется в том, как управляющее звено передает свои взгляды сотрудникам.

Передача взглядов на безопасность имеет две стороны: отношение управляющего звена и механизм передачи. Руководство может вполне осознавать важность процессов безопасности, но если они не доносят это до своих сотрудников, то последние не будут этого понимать.

Поэтому не забудьте исследовать состояние данного вопроса в организации, опросив руководящий состав и сотрудников.

Следование правилам

При составлении плана безопасной информационной среды необходимо определить фактическую среду безопасности. Планируемая среда устанавливается политикой, положениями и существующими механизмами. Фактическая среда определяется реальным согласием на участие в процессе обеспечения безопасности руководителей и сотрудников. Например, если политика безопасности требует еженедельного просмотра журналов аудита, а руководители не делают этого, то, значит, в организации не соблюдаются требования этой политики.

Политика использования восьмизначных паролей одинаково важна для всех сотрудников. Если руководство организации приказывает системным администраторам настроить конфигурацию их компьютеров на использование паролей с меньшим количеством знаков, это указывает на недостаточное следование правилам со стороны руководства.

Совет

Недостаточное следование правилам со стороны руководства однозначно приведет к рассогласованности действий администраторов и других сотрудников.

Специфика деятельности

В заключение исследуйте специфику деятельности организации. Опросите сотрудников и выясните издержки организации в случае нарушения конфиденциальности, целостности, доступности или идентифицируемости информации. Попробуйте выразить величину этих потерь в денежном выражении, времени простоя, утраченной репутации или в расторгнутых сделках.

При исследовании специфики деятельности определите движение информации внутри организации, между отделами и рабочими местами, внутри отделов и в другие организации. Выясните, как звенья этой цепи угрожают информации, как взаимосвязаны между собой отдельные части организации.

Частью процесса оценки является выявление систем и сетей, критичных для выполнения основной функции организации. Если организация связана с электронной коммерцией, выясните, какие системы используются для совершения сделок? Очевидно, необходим веб-сервер, но что насчет других серверных систем? Определение серверных систем позволит выявить прочие риски для организации.

Результаты оценки

После сбора всей информации группа оценки должна ее проанализировать. При оценке безопасности организации нельзя рассматривать отдельные блоки информации. Группа должна исследовать все уязвимости безопасности в контексте организации. Не все уязвимости превратятся в риски. Некоторые уязвимые места будут защищены каким-либо способом, который предотвратит их использование.

После завершения анализа группа оценки обязана представить полный набор рисков и рекомендаций для организации. Риски представляются по порядку - от наибольшего к наименьшему. Для каждого риска группа показывает возможные издержки в каком-либо выражении (денежном, временном, ресурсном, потере репутации и расторгнутых сделках). Каждый риск должен сопровождаться рекомендацией по управлению риском.

Последний шаг оценки - это разработка плана действий по безопасности. Организация должна определить, являются ли результаты оценки реальным отображением состояния безопасности, и учесть их при распределении ресурсов и составлении планов.

Примечание

Вполне вероятно, что в плане самый серьезный риск будет поставлен не на первое место. Этому могут помешать проблемы, связанные с бюджетом и ресурсами.

Разработка политики

Следующим шагом после оценки, как правило, является разработка политик и процедур. Они определяют предполагаемое состояние безопасности и перечень необходимых работ. Без политики нет плана, на основании которого организация разработает и выполнит эффективную программу информационной безопасности.

Необходимо разработать следующие политики и процедуры.

- Информационная политика. Выявляет секретную информацию и способы ее обработки, хранения, передачи и уничтожения.
- Политика безопасности. Определяет технические средства управления для различных компьютерных систем.
- Политика использования. Обеспечивает политику компании по использованию компьютерных систем.
- Политика резервного копирования. Определяет требования к резервным копиям компьютерных систем.
- Процедуры управления учетными записями. Определяют действия, выполняемые при добавлении или удалении пользователей.
- Процедура управления инцидентом. Определяет цели и действия при обработке происшествия, связанного с информационной безопасностью.
- План на случай чрезвычайных обстоятельств. Обеспечивает действия по восстановлению оборудования компании после стихийных бедствий или инцидентов, произошедших по вине человека.

Разработка политик является в большей степени политическим процессом. Во многих отделах найдутся люди, которые заинтересуются политиками и захотят сказать свое слово при их разработке.

Порядок разработки политик

Итак, какая политика должна быть разработана первой? Ответ зависит от рисков, определенных в процессе оценки. Если защита информации определена как область с высоким уровнем риска, информационная политика должна разрабатываться одной из первых. Если же вероятны потери в бизнесе из-за отсутствия плана на случай чрезвычайных действий, то этот план должен быть разработан в первую очередь.

Еще одним фактором в выборе порядка разработки политик является затрачиваемое время. Планы восстановления в случае ЧП обычно представляют очень подробные документы и требуют серьезных усилий со стороны отделов и сотрудников. Этот план потребует много времени для составления; возможно, потребуется помощь стороннего исполнителя, например, компании, поставляющей резервное оборудование для целей полного восстановления на случай стихийного бедствия.

Единственная политика, которая должна быть разработана на начальной стадии процесса, - это информационная политика. Информационная политика формирует основу понимания того, почему внутренняя информация важна и насколько она должна быть защищена. Этот документ послужит основой для программы обучения специалистов по вопросам безопасности, наряду с политикой использования и политикой паролей.

В самом лучшем случае возможна одновременная разработка нескольких политик, поскольку заинтересованные стороны будут объединены общими интересами. Например, системные администраторы интересуются политикой безопасности, но информационная политика их интересует в меньшей степени. Сотрудникам более близка политика безопасности и процедуры управления пользователями, а не политика резервного копирования, и т. д. В этом случае отдел информационной безопасности становится координатором и носителем функций, облегчающих выполнение проекта. Его представители должны присутствовать на первом собрании, посвященном разработке черновой версии плана, и их предложения станут отправным пунктом.

Совет

Для начала попробуйте составить небольшой документ с небольшим числом заинтересованных сторон. Это создаст благоприятную возможность для достижения успеха, что позволит отделу безопасности прийти к соглашениям, необходимым для разработки остальных документов.

Обновление существующих политик

Если политики и процедуры уже существуют, это хорошо. Однако вероятно, что некоторые из этих документов потребуют обновления. Если в их создании принимал участие отдел информационной безопасности, то в первую очередь необходимо собрать все заинтересованные стороны, участвовавшие в работе над предыдущей версии политики, и начать работу по обновлению. Используйте как отправную точку исходный документ и выявленные неточности.

Если в разработке документа участвовал кто-то из сотрудников организации, его также нужно привлечь к работе над обновлением. Отдел информационной безопасности не должен ослаблять контроль над

деятельностью бывшего владельца. В этом случае снова начните с исходного документа и выявленных неточностей.

Если разработчик исходного документа больше не числится в организации, то проще начать с чистого листа. Выявите заинтересованных лиц и пригласите их принять участие в процессе. Сообщите им, почему старый документ больше не является удовлетворительным

Вопросы для самопроверки

1. Общие затраты на безопасность = _____ + _____.
2. Перечислите главные элементы оценки в организации.

Реализация политики безопасности

Реализация политики заключается в реализации технических средств и средств непосредственного контроля, а также в подборе штата безопасности. Могут потребоваться изменения в конфигурации систем, находящихся вне компетенции отдела безопасности. В таких случаях в проведении программы безопасности должны участвовать системные и сетевые администраторы.

Исследуйте каждый этап для определения взаимодействий с другими системами управлениями. Например, усиление физической защиты позволит снизить требования к политике шифрования и наоборот. Установка межсетевых экранов позволит отложить немедленное устранение уязвимых мест внутренних систем.

Системы отчетности по безопасности

Системы отчетности по безопасности - это механизм, с помощью которого отдел безопасности отслеживает соблюдение политик и процедур, общее состояние уязвимых мест внутри организации. Для этого используются как ручные, так и автоматические системы. В большинстве случаев системы отчетности по безопасности включают оба типа систем.

Мониторинг использования

Механизмы мониторинга гарантируют, что работники следуют политикам использования компьютера. Они включают в себя программное обеспечение, отслеживающее использование интернета. Целью является выявление работников, постоянно нарушающих политику компании. Некоторые механизмы способны блокировать такой доступ и сохранять журнал попыток.

Мониторинг использования включает, например, удаление игр, установленных на рабочей станции. Сложные механизмы позволяют

определить, что на компьютер пользователя загружено новое программное обеспечение, но они требуют взаимодействия между администраторами и службой безопасности.

Сканирование уязвимых мест систем

Уязвимые места системы стали очень важной темой в безопасности. Установка операционной системы с параметрами по умолчанию обычно сопровождается запуском ненужных процессов и появлением уязвимых мест. Выявление таких мест не составляет труда для службы безопасности, использующей современные инструментальные средства, а вот их исправление отнимает много времени. Служба безопасности должна отслеживать системы и их уязвимые места с определенной периодичностью. Необходимо обеспечить администраторов отчетами об уязвимых местах для их удаления. Сведения о вновь установленных системах нужно доводить до сведения системного администратора.

Соблюдение политики

Соблюдение политики - это одно из заданий службы безопасности, отнимающее много времени. Для определения соблюдения политики используются ручной и автоматический режимы. Ручной механизм требует от работника службы безопасности исследования каждой системы и определения, как выполняются требования политики безопасности в конфигурации этой системы. Это отнимает чрезвычайно много времени, велика и вероятность ошибок. Намного чаще из общего количества систем выбирается одна, и проводится ее выборочное исследование. Такой способ требует меньше времени, но далек от совершенства.

Для проведения автоматической проверки соблюдения политики разрабатывается соответствующее программное обеспечение. Такой способ требует больше времени для установки и конфигурирования, но дает более точный результат в более короткие сроки. В этом случае требуется помощь системных администраторов, поскольку программное обеспечение необходимо установить в каждой проверяемой системе. Контроль соблюдения политики может выполняться на основе периодической выборки и результатов обращений к системным администраторам.

Аутентификация систем

Аутентификация систем - это механизм, предназначенный для установления личности пользователей, желающих получить доступ в систему или сеть. Она позволяет также идентифицировать лиц, пытающихся завладеть оборудованием организации. Механизмы аутентификации - это пароли, смарт-карты и биометрия. Требования к ним должны быть включены в программы профессиональной переподготовки по вопросам безопасности.

Примечание

Механизмы аутентификации можно применить к любому пользователю системы. Отсюда следует, что обучение и компетентность пользователя являются важными сторонами развертывания любого механизма аутентификации.

Если пользователи не ознакомлены с работой системы аутентификации, то отдел ИТ будет перегружен звонками в службу технической поддержки. Производительность работы будет снижена, поскольку пользователи начнут изучать, как пользоваться новой системой. Ни при каких обстоятельствах изменения в способах аутентификации не должны осуществляться без обучения пользователей. Эти способы оказывают влияние на все системы организации, и их реализация должна сопровождаться подробным планированием. Служба безопасности должна работать во взаимодействии с системными администраторами, чтобы процесс реализации проходил без сбоев.

Безопасность в интернете

Реализация безопасности в интернете включает такие механизмы, как межсетевые экраны и виртуальные частные сети (VPN), и ведет к изменениям в сетевой архитектуре. Наиболее важным аспектом ее реализации является размещение устройства управления доступом (типа межсетевого экрана) между интернетом и внутренней сетью организации. Без подобной защиты все внутренние системы открыты для неконтролируемых нарушений безопасности. Установка межсетевого экрана является достаточно сложным процессом и может повлечь за собой сбои в нормальной работе пользователей.

Примечание

Размещение межсетевого экрана или другого устройства управления доступом ведет к изменению архитектуры. Подобная операция не должна выполняться до тех пор, пока не будет определена основная сетевая архитектура: ведь нужно установить межсетевой экран соответствующей мощности и задать на нем правила в соответствии с используемыми политиками организации.

Виртуальные частные сети обеспечивают безопасность для информации, передаваемой через интернет и периметр организации. Вопросы, связанные с VPN, могут быть включены в реализацию механизмов безопасности в интернете.

Системы обнаружения вторжений

Системы обнаружения вторжений (IDS) - это системы охранной сигнализации сети. Охранная сигнализация предназначена для обнаружения попыток проникновения в защищаемое помещение, а IDS - для разграничения санкционированного входа и вторжения злоумышленника в защищаемую сеть.

Имеется несколько типов систем обнаружения вторжения, и выбор нужной зависит от совокупного риска организации и располагаемых ресурсов. Системы обнаружения вторжений требуют значительных финансовых вложений.

Самым общим механизмом обнаружения вторжений является антивирусное программное обеспечение. Это программное обеспечение должно работать на каждой рабочей станции и, разумеется, на сервере. Антивирусное программное обеспечение - наименее ресурсоемкий способ обнаружения вторжений.

Перечислим другие способы обнаружения вторжений:

- ручная проверка журнала;
- автоматическая проверка журнала;
- клиентское программное обеспечение для обнаружения вторжения;
- сетевое программное обеспечение для обнаружения вторжения.

Ручная проверка журнала весьма эффективна, но занимает много времени и склонна к ошибкам. Люди для этой цели не подходят. Наилучшим способом проверки журналов является создание программ или скриптов, которые просматривают журналы компьютера в поисках возможных отклонений.

Совет

Развертывание механизмов обнаружения вторжения не следует проводить до тех пор, пока не будут выявлены области с повышенным риском.

Шифрование

Шифрование обычно применяют для защиты конфиденциальных или частных интересов. Механизмы шифрования используются для защиты передаваемой или сохраняемой информации. Вне зависимости от типа используемого механизма возникают два вопроса, на которые нужно ответить до его реализации:

- алгоритмы;
- управление ключом защиты.

Примечание

Шифрование ведет к замедлению обработки или передачи данных. Следовательно, шифрование всей передаваемой информации не всегда является целесообразным.

Алгоритмы

При выполнении шифрования выбор алгоритма обуславливается конечной целью. Шифрование на личном ключе происходит быстрее, чем на открытом. Однако такой способ не позволяет использовать цифровую подпись или подписывание информации. Важно выбрать известные и хорошо изученные алгоритмы. Такие алгоритмы с большой долей вероятности исключают лазейки, через которые возможен доступ к защищенной информации.

Управление ключом защиты

Развертывание механизмов шифрования должно включать управление ключом защиты. При использовании шифровального блока (устройства для шифрования трафика, передаваемого от узла к узлу) система должна разрешать периодическое изменение ключа. При шифровании на открытом ключе, когда сертификаты выдаются большому количеству лиц, проблема намного серьезнее.

Если планируется введение подобной системы, удостоверьтесь в наличии времени для испытания ключа защиты. Также имейте в виду, что экспериментальная программа позволяет охватить ограниченное число пользователей, а система управления ключом защиты должна быть соразмерна всей системе.

Физическая безопасность

Физическая безопасность традиционно обособлена от информационной или компьютерной безопасности. Установка видеокамер, замков и охранников обычно не очень хорошо понималась работниками отдела компьютерной безопасности. Если в вашей организации дело обстоит именно так, вы должны найти поддержку со стороны. Имейте в виду, что устройства физической безопасности затронут работников организации, как и изменение способа аутентификации. Работники, которые видят видеокамеры в туалете или предъявляют пластиковую карту для входа в кабинет, должны приспособиться к новым обстоятельствам. Если сотрудники пользуются такими картами, то организация должна разработать процедуру действий работников, потерявших или оставивших их дома.

Такая процедура должна доказать, что данный человек действительно является сотрудником организации. Это могут быть цифровые фотографии или звонок коллеги для подтверждения подлинности. Некоторые организации полагаются только на подпись работника в соответствующем

журнале. Такой метод позволяет злоумышленнику получить доступ к ее материальным ценностям.

Применяя механизмы физической безопасности, вы не должны забывать о безопасности центра обработки данных. Доступ к центру данных должен быть ограничен, как следует защищен от огня, высокой температуры и отключения электричества. Внедрение систем пожаротушения и климат-контроля заставит вас провести всестороннюю модернизацию центра данных. Применение источника бесперебойного питания следует применять в системах, отключающихся на короткое время.

Персонал

При применении любых новых систем безопасности вы должны располагать подходящим персоналом. Некоторые системы потребуют постоянного обслуживания (механизмы идентификации пользователей и системы обнаружения вторжений). Другим системам потребуются люди для выполнения положений плана (например, для сканирования уязвимостей).

Вам потребуются обученные сотрудники при проведении учебных программ по повышению осведомленности. Сотрудник отдела информационной безопасности должен присутствовать на каждом учебном занятии, чтобы отвечать на специфические вопросы, даже если обучение проводится отделом обучения.

Последняя проблема, связанная с персоналом, - это ответственность. Ответственность за безопасность организации должна устанавливаться индивидуально. В большинстве случаев ответственным назначается руководитель отдела безопасности, который отвечает за разработку политики, исполнение плана и реализацию механизмов безопасности. Назначение этой обязанности должно быть первым шагом по пути реализации нового плана безопасности.

Проведение профессиональной переподготовки

Организация не может обеспечить защиту секретной информации, не привлекая своих сотрудников. Грамотная профессиональная переподготовка - это механизм обеспечения сотрудников необходимой информацией. Программы обучения могут иметь форму коротких занятий, информационных статей или плакатов. Наиболее эффективные программы используют все три формы.

Сотрудники

Сотрудники должны знать, почему вопросы безопасности так важны, должны быть обучены выявлению и защите секретной информации.

Компетентная профессиональная переподготовка по безопасности обеспечивает их необходимой информацией в области политики организации, выбора пароля и предупреждения атак социального инжиниринга.

Обучение сотрудников лучше всего проводить короткими занятиями - по часу или менее. Видеоматериалы способствуют более качественному уровню занятий, чем обычная лекция. Все новые сотрудники должны проходить обучение как часть инструктажа, а все работающие - раз в два года.

Администраторы

Обучение важно и для системных администраторов. Они должны быть осведомлены о последних на данный момент технических приемах хакеров, угрозах безопасности и обновления программных продуктов. Это обучение должно проходить часто (возможно, раз в месяц) и проводиться сотрудниками отдела безопасности. Информация об обновлениях может быть включена в регулярные совещания штата администраторов для экономии времени, так необходимого администраторам. В дополнение к этому отдел безопасности должен передавать обновления администраторам сразу после появления новых версий, не дожидаясь очередного совещания.

Разработчики

Обучение для разработчиков должно быть расширенной версией учебных занятий для сотрудников. Дополнительный материал включает специфические технические приемы программирования для устранения уязвимых мест и соответствующее понимание роли отдела безопасности в процессе разработки.

Для всех новых разрабатываемых проектов необходимо вовлекать на стадии проектирования отдел безопасности. Это позволит анализировать новые проекты на предмет приоритетного выделения средств на вопросы, связанные с безопасностью. Обучение разработчиков должно дать объяснение важности такого подхода.

Руководители

Презентация для руководителей организации - это отчасти и обучение, и маркетинг. Без поддержки руководства программа безопасности просто не сможет существовать. Следовательно, руководство должно быть проинформировано о состоянии безопасности и о дальнейшем развитии программы.

Периодические презентации руководству должны включать результаты недавних оценок и состояние различных проектов по безопасности. По

возможности система показателей, выражающая риски для организации, должна быть общепризнанной. Например, нужно отследить и отразить в отчете число уязвимых мест организации и нарушений системной политики.

Совет

В ходе этих презентаций можно представить информацию, используемую для обучения сотрудников, чтобы напомнить руководству об их обязанностях в плане обеспечения безопасности.

Персонал отдела безопасности

Персонал отдела безопасности должен быть осведомлен о современном состоянии дел, чтобы грамотно выполнять свою работу. Важно проводить как внешнее, так и внутреннее обучение. Например, каждому сотруднику отдела безопасности можно назначить время для проведения обучения остальных сотрудников этого отдела на любую тему по выбору. Темы должны быть связаны с безопасностью либо с текущим вопросом, интересующим персонал, либо с навыком, отсутствующим у персонала.

Проведение аудита

Аудит - это последний шаг в процессе реализации информационной безопасности. После определения состояния информационной безопасности внутри организации, создания соответствующих политик и процедур, приведения в действие технических средств контроля и обучения персонала проведение аудита позволит удостовериться, что все средства контроля сконфигурированы правильно.

Обсуждая место аудита в процессе безопасности, мы в действительности говорим о трех разных функциях:

- аудит соблюдения политики;
- периодическая оценка существующих проектов и оценка новых проектов;
- проверка возможности нарушения защиты.

Каждая из этих функций занимает свое место в процессе обеспечения безопасности.

Аудит соблюдения политики

Аудит соблюдения политики - это традиционная функция аудита. Организация имеет политику, определяющую настройки и конфигурацию систем безопасности. Аудит определяет реальное состояние дел. Любые отклонения отмечаются как нарушения. Подобные проверки могут

выполняться внутренним персоналом или внешними консультантами. И в том и в другом случае этот процесс требует участия системных администраторов.

Аудит соблюдения политики не должен ограничиваться только проверкой конфигурации систем. Он должен проявлять интерес к тому, как выполняются другие формы управления информацией. Соблюдается ли информационная политика? Как хранятся и передаются секретные документы?

Проверки должны проводиться раз в год. Они могут выполняться персоналом отдела безопасности, но, возможно, выполнение аудита больше подходит для отдела аудита организации или для сторонней фирмы. Причина в том, что в данном случае могут быть затронуты интересы самого отдела безопасности, что приведет к возникновению конфликта интересов.

Периодическая оценка проектов и оценка новых проектов

Компьютерная и сетевая среда внутри организации находятся в состоянии постоянного изменения. Эти изменения приводят к быстрому старению результатов оценки за счет сокращения некоторых рисков и введения новых. По этой причине оценка должна выполняться периодически. Полная оценка организации должна выполняться раз в два года. Как и в случае с крупными проверками, серьезные оценки выполняются персоналом отдела безопасности, если он обладает необходимыми навыками. Возможно, для этих целей больше подходит сторонняя организация.

Небольшие оценки должны выполняться в случае разработки новых проектов или изменений в организационной среде. Для каждого нового проекта отдел безопасности привлекается к работе на стадии проектирования, чтобы определить, имеет ли проект какие-либо риски, и происходит ли в результате разработки проекта появление или сокращение рисков внутри организации. Этот тип оценки должен изучать новый проект в контексте его использования по отношению к другим структурным элементам организации. Если риски определены на ранней стадии проекта, проектирование может быть скорректировано или введены другие механизмы для управления риском.

Проверка возможности нарушения защиты

Проверка возможности нарушения защиты - это спорная тема. Часто такие проверки выполняются вместо оценки. На самом деле, они имеют ограниченную ценность в программе безопасности. Причина этого проста: при проверках предпринимаются попытки воспользоваться установленной уязвимостью, чтобы получить доступ к системам и информации внутри организации. Если такая проверка имеет успех, то единственный вывод из

всего этого - обнаружена, по крайней мере, одна уязвимость. Если проверка нарушения защиты терпит неудачу, то вывод такой - проверяющий не смог обнаружить и использовать уязвимость. Это вовсе не значит, что уязвимости не существует.

Почему же тогда необходимо выполнять проверку возможности нарушения защиты? Если организация провела оценку и применила подходящие средства управления риском, она может выборочно проверить некоторых из них. Проверка защиты подходит для следующих случаев.

- Способность системы обнаружения вторжений выявить попытку нарушения защиты.
- Уместность процедуры реагирования на инцидент, связанный с безопасностью.
- Информация о сети, которую можно узнать через средства управления сетевым доступом.
- Уместность физической безопасности помещения.
- Адекватность информации, предоставляемой сотрудникам программой повышения осведомленности в плане безопасности.

Внимание!

Какой бы ни была причина проведения проверки возможности нарушения защиты, подробный план этой проверки должен быть предоставлен до ее начала. Для каждого этапа плана необходимо определить цель проверки.

Организация определяет также масштаб проверки. Проверка возможности нарушения защиты через внешнюю сеть ограничена внешними сетевыми соединениями организации (соединения через интернет или с другими внешними организациями). Они могут включать доступ через коммутируемое подключение к сети компании или доступ к беспроводным сетям. Проверка физического нарушения защиты выявляют людей, пытающихся получить несанкционированный доступ к оборудованию. Масштаб подобных тестов может быть ограничен как рабочим, так и нерабочим временем. Проверка возможности атак социального инжиниринга связана с тестированием осведомленности сотрудников, она разрешает проверяющим вступать в контакт с сотрудниками, пытаясь заставить их разгласить информацию или предоставить доступ к внутренним системам.

Многие организации начинают развертывание систем безопасности с проверки возможности нарушения защиты. Однако большой пользы это не принесет, поскольку организация не получит достаточного количества информации, позволяющего управлять ее рисками.

Разработайте программу повышения осведомленности в плане безопасности

Осведомленность в плане безопасности - это важная часть любой хорошей программы безопасности. Самым важным моментом здесь является использование наглядных и выразительных способов предоставления информации сотрудникам. Для этого у вас есть занятия, плакаты, информационные листки и электронная почта.

Шаг за шагом

1. Определите ключевую информацию, которая должна быть передана сотрудникам вашей организации. Ее можно найти в различных политиках, используемых в организации. Обратите особое внимание на требования паролей, идентификационные карточки, использование политик, в общем, на все, что напрямую влияет на работу сотрудников.
2. Определите этапы программы повышения осведомленности и то, что будет использоваться для обучения сотрудников (например, проведение занятий или вывешивание плакатов).
3. Наметьте в общих чертах, как будет представлен материал.
4. Определите ресурсы, необходимые для выполнения программы обучения (инструкторы для занятий, кабинеты и т. д.).

Выводы

В большинстве случаев лучше всего использовать сочетание ежегодных занятий с ежемесячными информационными статьями и плакатами. Занятия для сотрудников не должны длиться больше одного часа, и даже тогда они должны быть более интересными, чем просто лекция сотрудника отдела безопасности. Старайтесь повышать уровень новаторскими идеями, чтобы удерживать интерес сотрудников.

Контрольные вопросы

1. Назовите пять этапов процесса информационной безопасности.
2. Для чего используются оценки?
3. Что делает политика?
4. Включен ли план восстановления на случай чрезвычайных происшествий в разработку политики?
5. Что такое развертывание политики?
6. Назовите примерную длительность занятия по повышению осведомленности сотрудников.
7. Через какой тип учебных занятий по повышению осведомленности должны пройти руководители?
8. Являются ли учебные занятия лучшим и единственным способом для предоставления информации всем работникам?
9. Когда попытки нарушения защиты терпят неудачу?
10. Почему безопасность считается процессом, а не набора действий, совершаемых однократно?

11. Какие практические проблемы препятствуют последовательному выполнению процесса?
12. Сколько обычно длится период оценки?
13. Почему информационная политика и политика безопасности разрабатываются в первую очередь?
14. Какова основная проблема, связанная с развертыванием новых систем идентификации?
15. Почему организация должна первым делом браться за решение вопросов, связанных с меньшим уровнем риска?