6. Лекция: Политика

Рассмотрены вопросы политики информационной безопасности, методика разработки политик, создания, развертывания и эффективного использования.

Наверное, самая неинтересная часть профессиональной работы в сфере информационной безопасности - это разработка политики. Развертывание политики не требует глубоких технических знаний и, таким образом, не очень привлекает профессионалов. Кроме того, не ждите благодарности, поскольку не многим сотрудникам понравятся результаты этой работы.

Политика устанавливает правила. Политика заставляет людей делать вещи, которые они не хотят делать. Но политика имеет огромное значение для организации и, вероятно, является наиболее важной работой отдела информационной безопасности.

Необходимость и важность политики

Политика устанавливает правила, которые определяют конфигурацию систем, действия служащих организации в обычных условиях и в случае непредвиденных обстоятельств. Таким образом, политика выполняет две основные функции:

- определяет безопасность внутри организации;
- определяет место каждого служащего в системе безопасности.

Какой должна быть безопасность

Политика определяет способы развертывания системы безопасности. Сюда входит правильная настройка компьютерных систем и сетей в соответствии с требованиями физической безопасности. Политика определяет надлежащие механизмы, используемые для защиты информации и систем.

Однако технические аспекты - это не единственное, что определяется политикой. Она ясно устанавливает порядок осуществления служащими своих обязанностей, связанных с вопросами безопасности, например, для администраторов. Она определяет поведение пользователей при использовании компьютерных систем, размещенных в организации.

И, наконец, устанавливает порядок реагирования в случае каких-либо непредвиденных обстоятельств. Если происходит инцидент, связанный с нарушением безопасности, или система дает сбой в работе, политики и процедуры устанавливают порядок действий и выполняемые задачи, направленные на устранение последствий этого инцидента.

Определение места каждого работника

Правила достаточно серьезны и являются необходимой частью действующей в организации программы безопасности. Таким образом, очень важно, что все службы работали во взаимодействии для построения надежной системы безопасности. Политика показывает основные направления деятельности работников компании в этой совместной работе. Политики и процедуры определяют задачи и цели программы безопасности. Когда эти задачи и цели должным образом поддерживаются служащими, это обеспечивает базу для коллективной работы в сфере безопасности.

Внимание!

В этой ситуации важную роль играет обучение, которое идет "рука об руку" с политикой. Если в организации не уделяется должного внимания программам информирования в сфере безопасности, то при развертывании политики возможно возникновение проблем.

Определение различных политик

Существует большое количество типов политик и процедур, которые определяют функционирование системы безопасности в организации. В следующих разделах мы покажем основные концепции, полезные и широко используемые на практике. Все эти концепции можно скомбинировать для лучшего использования в вашей организации. Три раздела каждой политики являются общепринятыми.

- Цель. Каждая политика и процедура имеют четко определенную цель, которая ясно описывает, почему создана та или иная политика или процедура, и какую выгоду от этого надеется получить организация.
- Область. Каждая политика и процедура имеет раздел, описывающий ее сферу приложения. Например, политика безопасности применяется ко всем компьютерным и сетевым системам. Информационная политика применяется ко всем служащим.
- Ответственность. В разделе об ответственности определяются лица, ответственные за соблюдение политик или процедур. Этот человек должен быть надлежащим образом обучен и знать все требования политики.

Информационная политика

Информационная политика определяет секретную информацию внутри организации и способы ее защиты. Политика разрабатывается таким образом, чтобы охватить всю существующую информацию. Каждый служащий отвечает за безопасность секретной информации, с которой он сталкивается в работе. Информация может быть представлена на бумажных носителях или в

виде файлов на компьютере. Политика должна предусмотреть защиту для всех форм представления информации.

Выявление секретной информации

Информация, считающаяся секретной, различается в зависимости от сферы деятельности организации. Секретные сведения включают деловые книги, проекты, патентную информацию, телефонные книги компании и т. д.

Определенная информация считается секретной для всех организаций - это сведения о выплатах, домашние адреса и номера телефонов служащих, информация о медицинском страховании и любая финансовая информация, закрытая для широкой публики.

Определение секретной информация должно быть тщательно и четко сформулировано в политике и донесено до служащих.

Внимание!

Определение секретной информации можно найти в законодательных актах и предписаниях. Поработайте с главным юрисконсультом своей организации и убедитесь, что вы четко представляете, какая информация является секретной.

Классифицирование

Двух или трех уровней классификации обычно достаточно для любой организации. Самый нижний уровень классификации - это общая информация. Над этим уровнем находится информация, недоступная для общего пользования. Она называется проприетарной, секретной или конфиденциальной. Такая информация доступна для отдельных служащих организации или для тех компаний, которые подписали соглашение о ее неразглашении. Если эта информация будет открыта для общего доступа или попадет к конкурентам, то организации будет нанесен значительный ущерб.

Существует третий уровень секретности, который называется "для служебного пользования" или "защищенная информация". Доступ к подобным сведениям открыт для ограниченного количества служащих.

Маркировка и хранение секретной информации

Для каждого уровня секретной информации, находящегося над уровнем общей, политика должна определять способ маркировки. Если информация представлена в виде бумажных документов, то каждая страница маркируется вверху и внизу. Это легко сделать в текстовом редакторе с помощью верхних и нижних колонтитулов. Обычно используют заглавные буквы, выделенные

полужирным шрифтом или курсивом, различные гарнитуры шрифта, чтобы сделать текст удобочитаемым.

Никакие секретные документы не должны оставаться на рабочих столах, здесь должна работать политика чистых столов. Закрывайте секретные бумаги в сейфах или ящиках столов. Если кабинет служащего, работающего с секретной информацией, закрывается, то можно разрешить хранение информации в этом кабинете.

Если данные записаны в компьютерных системах, политика должна определить соответствующие уровни защиты. Это может быть управление доступом к файлам или специальная парольная защита для определенных типов документов. В ответственных ситуациях используется шифрование. Имейте в виду, что системным администраторам доступны любые документы в системе. Если вы хотите скрыть защищаемую информацию от них, то единственным способом является шифрование.

Передача секретной информации

Информационная политика должна определять способы передачи секретной информации. Данные передаются различными путями (электронная почта, обычная почта, факс), и в политике должен быть оговорен каждый из них.

Если секретные данные передаются через электронную почту, то устанавливается обязательное шифрование файлов, вложенных в сообщение, либо тела сообщения. Если посылается твердая копия данных, то определяется метод с использованием письменной расписки (квитанции) - срочная доставка курьерской почтой или заказным письмом. При передаче документа по факсу необходимо, чтобы получатель находился около аппарата во время приема документа, иначе вы рискуете выставить секретные сведения на обозрение всем сотрудникам организации

Уничтожение секретной информации

Если важный документ просто выбрасывается в мусорную корзину, то он становится добычей для злоумышленников. Секретные документы нужно разрезать на мелкие части. Канцелярская бумагорезательная машина дает дополнительный уровень защиты, измельчая документ в продольном и поперечном направлении. Вряд ли такой документ можно восстановить!

Информацию в компьютерных системах можно восстановить после удаления, если она удалена неправильно. Существуют коммерческие программы, которые стирают данные с магнитных носителей без возможности их восстановления, например PGP desktop и BCWipe.

Примечание

Существуют способы восстановления данных на электронных носителях, даже если поверх что-то записано. Однако такая аппаратура дорого стоит, поэтому вряд ли применяется для получения коммерческой информации. Таким образом, дополнительное физическое уничтожение самих носителей обычно не требуются.

Политика безопасности

Политика безопасности определяет технические требования к защите компьютерных систем и сетевой аппаратуры, способы настройки систем администратором с точки зрения их безопасности. Эта конфигурация будет оказывать влияние на пользователей, и некоторые требования, установленные в политике, связаны со всем коллективом пользователей. Главная ответственность за развертывание этой политики ложится на системных и сетевых администраторов при поддержке руководства.

Политика безопасности определяет требования, выполнение которых должно быть обеспечено на каждой системе. Однако политика сама по себе не определяет конкретную конфигурацию различных операционных систем. Это устанавливается в отдельных процедурах по настройке. Такие процедуры могут быть размещены в приложении к политике.

Идентификация и аутентификация

Политика безопасности определяет порядок идентификации пользователей: либо стандарт для идентификаторов пользователей, либо раздел в процедуре системного администрирования, в котором определяется этот стандарт.

Очень важно, чтобы был установлен основной механизм для аутентификации пользователей и администраторов. Если это пароли, то в политике определяется минимальная длина пароля, максимальный и минимальный возраст пароля и требования к его содержимому.

Каждая организация во время разработки своей политики безопасности должна определить, будут ли учетные записи администраторов использовать те же самые механизмы аутентификации, что и обычные пользователи, или же более строгие. Более строгий механизм должен быть описан в соответствующем разделе политики. Он может также использоваться для удаленного доступа через виртуальные частные сети или соединения наборного доступа (dial-up).

Примечание

В большинстве случаев учетные записи администраторов должны использовать сильные механизмы аутентификации (например смарт-карты).

Управление доступом

Политика безопасности устанавливает стандартные требования к управлению доступом к электронным файлам, в которых предусматриваются формы управления доступом пользователей по умолчанию, доступные для каждого файла в системе. Этот механизм работает в паре с аутентификационным механизмом и гарантирует, что только авторизованные пользователи получают доступ к файлам. Также четко оговариваются пользователи, имеющие доступ к файлам с разрешениями на чтение, запись и исполнение.

Настройки по умолчанию для новых файлов устанавливают разрешения, принимаемые при создании нового файла. В этом разделе политики определяются разрешения на чтение, запись и исполнение, которые даются владельцам файлов и прочим пользователям системы.

Аудит

Раздел, посвященный аудиту в политике безопасности, определяет типы событий, отслеживаемых во всех системах. Стандартными событиями являются следующие:

- попытки входа в систему (успешные или неудачные);
- выход из системы;
- ошибки доступа к файлам или системным объектам;
- попытки удаленного доступа (успешные или неудачные);
- действия привилегированных пользователей (администраторов), успешные или неудачные;
- системные события (выключение и перезагрузка).

Каждое событие должно включать следующую информацию:

- ID пользователя (если имеется);
- дата и время;
- ID процесса (если имеется);
- выполненное действие;
- успешное или неудачное завершение события.

В политике безопасности устанавливается срок и способ хранения записей аудита. По возможности указывается способ и частота просмотра этих записей.

Примечание

Во многих организациях применяется политика длительного хранения информации. Перед разработкой политики безопасности внимательно

ознакомьтесь с существующими правилами, чтобы в разных политиках не было похожих требований.

Сетевые соединения

Для каждого типа соединений в сети политика безопасности описывает правила установки сетевых соединений и используемые механизмы защиты.

Соединения наборного доступа. Требования к этим соединениям устанавливают технические правила аутентификации и аутентификации для каждого типа соединения. Они излагаются в разделе аутентификации политики и могут устанавливать более сильные способы аутентификации, чем обычные. Кроме того, в политике определяются требования к аутентификации при получении доступа через соединения наборного доступа. Для организации целесообразно установить строгий контроль над разрешенными точками доступа, чтобы соблюдать требования авторизации в сети.

Выделенные линии. В организациях используются различные типы выделенных линий, и для каждого типа необходимо определить устройства защиты. Чаще всего такими устройствами являются межсетевые экраны.

Только лишь указание типа устройства само по себе не предусматривает какого-либо уровня защиты. Политика безопасности должна определять базовую политику контроля доступа, применяемую на устройстве, а также процедуру запроса и получения доступа, не являющуюся частью стандартной конфигурации.

Удаленный доступ к внутренним системам. Нередко организации позволяют своим сотрудникам осуществлять доступ к внутренним системам из внешних удаленных местоположений. Политика безопасности должна определять механизмы, используемые при осуществлении такого доступа. Необходимо указать, чтобы все соединения были защищены шифрованием, определить специфику, связанную с типом шифрования. Так как подключение осуществляется извне организации, рекомендуется использовать надежный механизм аутентификации. Кроме того, политика безопасности должна определять процедуру прохождения авторизации для такого доступа.

Беспроводные сети. Беспроводные сети становятся популярными, и установка в подразделении беспроводной связи без ведома отдела информационных технологий уже стала обычным делом. Политика безопасности должна определять условия, при которых разрешается использование беспроводных соединений, и то, каким образом будет осуществляться авторизация в такой сети.

Если предполагается разрешить использование беспроводной сети, то необходимо указать дополнительные требования, предъявляемые к аутентификации или шифрованию.

Примечание

Беспроводные сети должны рассматриваться как внешние незащищенные сети, а не как часть внутренней сети организации. Если так и есть на самом деле, данный факт должен быть отмечен в политике.

Вредоносный код

В политике безопасности должно быть определено размещение программ безопасности, отслеживающих вредоносный код (вирусы, черви, "черные ходы" и "троянские кони"). В качестве мест размещения указываются файловые серверы, рабочие станции и серверы электронной почты.

Политика безопасности должна предусматривать определение требований для таких защитных программ. В эти требования может входить проверка определенных типов файлов и проверка файлов при открытии или согласно расписанию.

В политике также указываются требования к периодическому (например, ежемесячному) обновлению признаков вредоносного кода для защитных программ.

Шифрование

Политика безопасности должна определять приемлемые алгоритмы шифрования для применения внутри организации и ссылаться на информационную политику для указания соответствующих алгоритмов для защиты секретной информации. В такой политике совершенно не обязательно указывать какой-либо один конкретный алгоритм. Политика безопасности также определяет процедуры управления ключами.

Отказ от защиты

Несмотря на всевозможные усилия сотрудников отдела безопасности, менеджеров и системных администраторов, обязательно возникнут ситуации, когда будут запущены системы, не отвечающим требованиям политики безопасности. В этих системах, скорее всего, будут выполняться задачи, связанные с бизнес-процессами организации, причем эти задачи будут ставиться выше политик безопасности. На этот случай в политике безопасности предусматривается механизм, оценивающий степень риска, которому подвергается организация; кроме того, данная политика должна

обеспечивать разработку плана действий, предпринимаемых при возникновении непредвиденных обстоятельств.

Процесс отказа от защиты предназначен для использования именно в этой ситуации. В каждом конкретном случае конструктор системы или менеджер проекта должен заполнять форму отказа следующей информацией.

- Система с отказом от защиты.
- Раздел политики безопасности, соответствие которому будет нарушено.
- Ответвления организации (обуславливают повышенную степень риска).
- Шаги, предпринимаемые для снижения или контроля степени опасности.
- План восстановления соответствия системы требованиям политики безопасности.

Отдел информационной безопасности должен просмотреть запрос об отказе от защиты и предоставить свою оценку риска, рекомендации по его снижению и управлению потенциально опасными ситуациями. На практике должна осуществляться совместная работа менеджера проекта и специалистов по безопасности для обработки всех возможных ситуаций, чтобы по завершении заполнения отказа от защиты обе стороны достигли договоренности по всем пунктам.

Наконец, отказ от защиты подписывается должностным лицом организации, ответственным за проект. Он таким образом заверяет свое понимание потенциальной опасности, связанной с отказом от защиты, и соглашается с необходимостью отказа организации от соответствия требованиям защиты. Кроме этого, подпись должностного лица означает согласие с тем, что шаги по контролю над степенью риска соответствуют требованиям и будут выполняться (при необходимости).

Приложения

В приложениях или в отдельных описаниях процедур должны размещаться подробные сведения о конфигурации для различных операционных систем, сетевых устройств и другого телекоммуникационного оборудования. Это позволяет модифицировать документы по мере необходимости без изменения политики безопасности организации.

Политика использования компьютеров

Политика использования компьютеров в случае судебного разбирательства определяет, кто может использовать компьютерные системы, и каким образом они могут использоваться. На первый взгляд, значительная часть

информации в этой политике имеет лишь общий смысл, но если организация не определит явным образом политику принадлежности и использования компьютера, то будет велика вероятность судебных исков от ее сотрудников.

Принадлежность компьютеров

Политика должна четко определять, что все компьютеры принадлежат организации, и что они предоставляются сотрудникам для работы в соответствии с их должностными обязанностями. Политика также может запрещать использование компьютеров, не принадлежащих организации, для выполнения работы, связанной с деловой деятельностью этой организации. Например, если сотрудник предполагает выполнять работу дома, организация предоставит ему компьютер. Также в политике может указываться, что только компьютеры, принадлежащие организации, могут использоваться для подключения к внутренним системам компании через систему удаленного доступа.

Принадлежность информации

Политика должна определять, что вся информация, хранимая или используемая на компьютерах организации, принадлежит организации. Некоторые сотрудники могут использовать компьютеры организации для хранения личных данных. Если в политике не оговорить данный вопрос в отдельном порядке (или если сотрудники просто не поймут это), то личные данные, при условии хранения в частных папках, действительно могут считаться личными данными. Это обстоятельство может привести к судебным искам в случае разглашения данной информации.

Приемлемое использование компьютеров

Обычно предполагается, что сотрудники используют для выполнения работы только те компьютеры, которые предоставляются организацией. Это предположение не всегда верно. Следовательно, оно должно быть оговорено в политике. Достаточно просто указать, что "компьютеры организации предназначены только для выполнения сотрудниками их должностных обязанностей". В других организациях могут детально определяться обязанности сотрудников.

Иногда сотрудникам разрешается использовать компьютеры фирмы для других целей, например, запускать вечером сетевые игры. Если это не запрещено, то данное обстоятельство должно быть четко оговорено в политике.

При использовании компьютеров, предоставляемых организацией, возникает вопрос о программном обеспечении, загружаемом в эти системы. Иногда требуется установить правило, согласно которому на компьютерных

системах запрещена загрузка неавторизованного программного обеспечения. В этом случае политика должна определять, кто может загружать авторизованные программы, и каким образом программы становятся авторизованными.

Приватность отсутствует

Возможно, самой важной частью политики использования компьютеров является заключение о том, что сотрудник не должен подразумевать частный статус любой информации, хранимой, отправляемой или получаемой на любых компьютерах организации. Очень важно, чтобы сотрудник понимал, что любая информация, включая электронную почту, может просматриваться администраторами. Кроме того, сотрудник должен знать, что администраторы или сотрудники отдела безопасности могут отслеживать все действия, связанные с компьютерами, включая посещение веб-сайтов.

Политика использования интернета

Политика использования интернета, как правило, включается в главную политику использования компьютеров. Однако в некоторых случаях эта политика представляется в виде отдельной политики в силу своих особенностей. Организации предоставляют своим сотрудникам доступ в интернет, чтобы они выполняли свои обязанности более эффективно и, следовательно, приносили большую прибыль. К сожалению, веб-сайты, посещаемые сотрудниками в интернете, далеко не всегда связаны с их работой.

Политика использования интернета определяет соответствующее назначение интернета (например, связанные с работой статистические исследования, покупка товаров или связь по электронной почте). Она определяет нецелевое использование интернета (например, посещение веб-сайтов, не связанных с деятельностью компании, загрузка защищенного авторскими правами содержимого, продажа музыкальных файлов или отправка писем по цепочке).

Если политика отделена от политики использования компьютеров, в ней указывается, что организация может отслеживать работу в интернете, и что сотрудники не должны рассматривать обмен данными через интернет как операцию, проводимую в частном порядке.

Политика работы с электронной почтой

В некоторых организациях разрабатывается специальная политика, определяющая методы работы с электронной почтой (она может быть включена в политику использования компьютеров). Электронная почта используется огромным числом организаций при управлении бизнесом.

Электронная почта представляет угрозу утечки важных данных. Если принято решение определить специальную политику электронной почты, то данная политика должна оговаривать как внутренние проблемы, так и внешние.

Внутренние проблемы, связанные с почтой

Политика работы с электронной почтой не должна конфликтовать с другими политиками, связанными с персоналом организации. Например, она должна указывать на все политики организации, в которых говорится о сексуальном притеснении. Если в организации запрещено передавать с помощью электронной почты неприличные шутки, то имеющиеся определения непристойных и неприличных комментариев нужно указать внутри данной политики.

Если в организации планируется отслеживание электронной почты на предмет наличия определенных ключевых слов или файловых вложений, в политике оговаривается данный типа мониторинга, однако не должны указываться конкретные слова, которые вызовут пометку сообщений. Политика также определяет, что сотрудник не должен считать электронную почту частной.

Внешние проблемы, связанные с почтой

Исходящая электронная почта может содержать секретную информацию. Политика почты должна определять, при каких условиях это обстоятельство допустимо, и в ней должны присутствовать ссылки на информационную политику, определяющую методы защиты секретных данных. Кроме того, может потребоваться определить отказ от прав или заключение внизу исходящих сообщений, в котором говорится о том, что информация, являющаяся собственностью организации, должна защищаться.

В политике почты оговариваются вопросы, связанные с входящей электронной почтой. Например, во многих организациях осуществляется тестирование входящих файлов на наличие вирусов. Политика должна ссылаться на политику безопасности организации, в которой говорится о соответствующих мерах, направленных на борьбу с вирусами.

Процедуры управления пользователями

Процедуры управления пользователями - это процедуры, выполняемые в рамках обеспечения безопасности, которым зачастую не уделяется должного внимания, что представляет собой огромный риск. Механизмы защиты систем от несанкционированного доступа посторонних лиц - отличные средства безопасности, однако они бесполезны при отсутствии должного управления пользователями компьютерных систем.

Процедура нового сотрудника

Для предоставления новым сотрудникам санкционированного доступа к компьютерным ресурсам необходимо разработать соответствующую процедуру. Над разработкой этой процедуры должны работать сотрудники отдела безопасности совместно с отделом кадров при участии системных администраторов. В идеальном случае запрос на компьютерные ресурсы будет генерироваться супервизором нового сотрудника. В зависимости от того, в какой отдел зачислен новый сотрудник, и от запроса доступа, сделанного супервизором, системные администраторы предоставят сотруднику соответствующий доступ к файлам и системам. Эта процедура должна использоваться при приеме на работу консультантов и совместителей, с присвоением срока действия их учетным записям для определения последнего рабочего дня в данной организации.

Процедура перемещенного сотрудника

В каждой организации должна быть разработана процедура пересмотра прав доступа сотрудников при их перемещении внутри организации. Эта процедура разрабатывается при поддержке отдела кадров и системных администраторов. В идеальном случае новый и старый руководитель сотрудника определяют тот факт, что сотрудник переходит на новое место, а также доступ, который ему больше не требуется, и доступ, необходимый для работы на новом месте. Соответствующий системный администратор затем внесет все необходимые изменения.

Процедура удаления сотрудника

Возможно, наиболее важной процедурой, связанной с управлением пользователями, является удаление уволившихся пользователей. Эта процедура разрабатывается при содействии отдела кадров и системных администраторов. Когда отдел кадров идентифицирует сотрудника, увольняющегося из компании, следует заблаговременно предупредить системного администратора, чтобы учетные записи данного сотрудника были удалены в последний день его работы.

В некоторых случаях необходимо отключать учетные записи сотрудника перед уведомлением сотрудника о его удалении. Данная ситуация также должна рассматриваться в процедуре удаления.

Совет

Процедуры удаления сотрудника должны предусматривать механизм очень быстрого удаления сотрудника (например, на тот случай, когда требуется немедленно выпроводить сотрудника из здания).

Процедура удаления сотрудника должна распространяться на совместителей и консультантов, имеющих учетные записи в системе. О таких пользователях отдел кадров может и не знать. Следует определить, кому будет известно о таких сотрудниках, и также включить этих лиц в процедуру.

Удаление системных или сетевых администраторов должно производиться под управлением отдельной задокументированной процедуры. Эти сотрудники, как правило, имеют множество учетных записей, и им известны основные административные пароли. Если такой сотрудник увольняется из организации, все эти пароли нужно сменить.

Внимание!

Очень легко упустить уволившегося сотрудника из виду. Чтобы организовать повторную проверку уволившихся сотрудников, рекомендуется разработать процедуру, осуществляющую периодическое подтверждение существующих учетных записей. Эта процедура содержит отключение учетных записей, не используемых в течение определенного промежутка времени, а также уведомление администраторов о наличии таких учетных записей.

Процедура системного администрирования

Процедура системного администрирования определяет, каким образом осуществляется совместная работа отдела безопасности и системных администраторов с целью обеспечения безопасности систем. Данный документ состоит из нескольких специальных процедур, определяющих, каким образом и как часто должны выполняться задачи системного администрирования, связанные с безопасностью. Эта процедура отмечается в политике использования компьютера (когда речь идет о возможности системных администраторов осуществлять мониторинг сети) и, следовательно, является отражением того, каким образом предполагается осуществлять управление системами.

Обновление программного обеспечения

Данная процедура определяет, как часто администратор проверяет наличие обновлений, выпускаемых производителем программного обеспечения. Предполагается, что новые надстройки не будут устанавливаться, следует предусмотреть выполнение предварительного тестирования.

Наконец, процедура должна документировать соответствующие сведения при проведении обновлений, а также процедуру отката в случае ошибки при установке обновления.

Сканирование уязвимостей

В каждой организации должна быть разработана процедура определения уязвимостей в системах. Как правило, сканирование осуществляется под руководством отдела безопасности, и соответствующие изменения вносятся системными администраторами. Существует ряд коммерческих средств сканирования и бесплатных программ, которые также могут использоваться для этой цели.

В процедуре определяется, насколько часто необходимо проводить сканирование. Результаты сканирования должны передаваться системным администраторам для корректировки или объяснения (может получиться так, что некоторые уязвимости не смогут быть устранены из-за программного обеспечения, установленного в системе). В этом случае администратору придется устранить уязвимости до следующего сканирования.

Проверка политики

Политика безопасности организации определяет требования безопасности для каждой системы. Для проверки соответствия информационной системы установленной политике используется периодическое проведение внешних или внутренних аудитов. В промежутке между основными аудитами отдел безопасности должен работать вместе с системными администраторами для проверки систем на соответствие политике безопасности. Это действие может осуществляться в автоматическом режиме или вручную.

Процедура проверки политики должна определять, насколько часто должна проводиться эта проверка. Кроме того, в ней описывается, кто получает результаты проверки, и каким образом разрешаются вопросы, возникающие при обнаружении несоответствий.

Примечание

Если проверку политики предполагается выполнять автоматически, то ее частота должна быть снижена, чтобы обеспечить запас времени на проверку конфигурации системы вручную.

Проверка журналов

Следует регулярно изучать журналы, полученные от различных систем. В идеальном случае сотрудники отдела безопасности просматривают записи журналов, помеченные программой, вместо просмотра всего журнала целиком.

Если предполагается использовать автоматическое средство, данная процедура должна определять конфигурацию этого средства, а также обработку исключений. Если процесс проводится вручную, в процедуре

определяется частота проверки файлов журналов, а также типы событий, которые должны отмечаться для проведения более основательной оценки.

Регулярный мониторинг

В организации должна быть определена процедура, указывающая, когда следует осуществлять отслеживание сетевого трафика. В некоторых организациях данный тип мониторинга осуществляется непрерывно, в других - случайным образом.

Политика резервного копирования

Политика резервного копирования определяет, каким образом осуществляется резервное копирование данных. Зачастую эти требования включаются в политику безопасности организации.

Частота резервного копирования

Политика резервного копирования должна определять частоту резервного копирования данных. Как правило, конфигурация предусматривает проведение полного резервного копирования данных один раз в неделю с дополнительным резервным копированием, проводимым в остальные дни. Дополнительное резервное копирование сохраняет только файлы, изменившиеся с момента последнего резервирования, что сокращает время процедуры и обеспечивает меньший объем пространства на резервном носителе.

Хранение резервных копий

Необходимо хранить носители с резервными копиями в защищенных местах, которые, тем не менее, должны быть доступны в случае, если потребуется восстановить утерянные данные. Например, в большинстве организаций предусмотрена ротация резервных носителей, согласно которой последние резервные ленты отключаются и помещаются в место хранения, а более ранние копии изымаются из хранилища для повторного использования. В данном случае ключевым параметром является скорость отключения и перемещения в место хранения. Это время зависит от степени опасности, представляемой для организации, если сбой произойдет в то время, когда резервный носитель будет отключен, от убытков вследствие хранения резервного носителя и времени, затрачиваемого на доставку носителей из места хранения. В организации должно быть установлено, насколько часто требуется применение резервных носителей для восстановления файлов. Если носители требуются каждый день, то, вероятно, имеет смысл хранить их несколько дней, пока не будет создана лента с более новой информацией.

Политика резервного копирования должна ссылаться на архивную или информационную политику организации для определения времени хранения файлов до повторного использования носителя.

Резервируемая информация

Не каждый файл на компьютере требует ежедневного резервного копирования. Например, исполняемые системные файлы и файлы конфигурации практически не меняются, поэтому для них не обязательно ежедневное резервирование. Имеет смысл создать резервную копию системных файлов заранее и загружать их с надежного носителя, если требуется переустановить систему.

Файлы данных, в особенности часто изменяющиеся, должны резервироваться регулярно. В большинстве случаев необходимо осуществлять их ежедневное резервное копирование.

Совет

Структура каталогов, используемая на файловых серверах, облегчает определение данных, подлежащих резервированию. Если все файлы содержатся в одном каталоге высокого уровня (содержащем подкаталоги), то осуществляется резервное копирование только одного каталога. Администратору не придется отыскивать отдельные файлы, разбросанные по всей файловой системе.

В политике резервного копирования предусматривается периодическое тестирование восстановления. Если даже резервное копирование осуществляется без ошибок, при восстановлении вероятно возникновение проблемы считывания файлов. Периодическое тестирование резервного носителя увеличивает вероятность обнаружения подобных проблем.

Процедура обработки инцидентов

Процедура обработки инцидентов (IRP) определяет способы реагирования на возникновение инцидентов, связанных с безопасностью. IRP определяет, кто имеет право доступа и что необходимо сделать, однако не всегда содержит описание конкретных действий.

Примечание

Если речь идет о банковской организации, название этой процедуры следует изменить (например, на "процедура обработки событий"). Термин "инцидент" имеет определенное значение в банковской сфере и необходимо избегать его использования, если событие не связано напрямую с финансовыми потерями.

Цели обработки инцидентов

Процедура IRP должна определять цели организации, достигаемые при обработке инцидента. Среди целей IRP можно выделить следующие:

- защита систем организации;
- защита данных организации;
- восстановление операций;
- пресечение деятельности злоумышленника;
- снижения уровня антирекламы или ущерба, наносимого торговой марке.

Эти цели не являются взаимоисключающими, и в организации вполне могут быть определены несколько целей. Ключевым моментом является определение целей организации до того, как возникнет инцидент.

Идентификация событий

Идентификация инцидента является, вероятно, наиболее важной и сложной частью процедуры обработки инцидента. Некоторые события очевидны (например, несанкционированное изменение содержимого веб-сайта), другие же события могут означать либо вторжение, либо просто ошибку пользователя (например, удаление файлов).

Перед объявлением конкретного инцидента сотрудники отдела безопасности и системные администраторы должно провести небольшое исследование, чтобы определить, действительно ли инцидент имел место. В этой части процедуры могут быть выявлены события, представляющие собой очевидные инциденты, а также определены действия, которые необходимо предпринять, если событие не является очевидным инцидентом.

Совет

Оказать помощь в идентификации инцидентов может служба технической поддержки. Если ее сотрудники обучены задавать конкретные вопросы обращающимся к ним пользователям, то их можно использовать для формирования первичного представления о вероятном инциденте.

Эскалация

В IRP должна быть определена процедура эскалации данных по мере поступления информации о произошедшем событии. В большинстве организаций процедура эскалации предназначена для активизации действий группы сотрудников, которым поручена обработка инцидентов. В банковских структурах предусматривается два уровня эскалации, в зависимости от того, связано ли событие с финансовыми потерями.

В каждой организации должны быть определены сотрудники, являющиеся членами группы, ответственной за обработку инцидентов. Их следует выбирать из следующих подразделений организации:

- отдел безопасности;
- системные администраторы;
- юридический отдел;
- отдел кадров;
- рекламный отдел.

По мере необходимости в группу могут быть добавлены и другие сотрудники.

Контроль информации

При обнаружении инцидента необходимо обеспечить контроль информации об инциденте. Количество получаемой информации зависит от того, какое влияние окажет инцидент на организацию и ее клиентскую базу. Кроме того, информацию следует оглашать таким образом, чтобы она положительно сказалась на делах организации.

Примечание

Только сотрудники отдела рекламы и юридического отдела могут обсуждать информацию об инциденте с представителями прессы, и никто более.

Обработка

Обработка инцидента напрямую вытекает из целей, определенных в IRP. Например, если целью данной процедуры является защита систем и информации, имеет смысл отключить системы от сети и провести необходимые восстановительные работы. В других случаях важнее сохранить систему в рабочем режиме и подключенном состоянии для продолжения обслуживания клиентов либо позволить злоумышленнику вернуться, чтобы собрать о нем больше данных и, возможно, идентифицировать.

В любом случае метод обработки, используемый организацией, должен обсуждаться и отрабатываться заблаговременно.

Примечание

Месть злоумышленнику никогда к добру не приводит. Такие ответные действия бывают незаконными - не делайте их никогда!

Полномочия

Важной частью IRP является определение того, кто в организации и в группе обработки инцидентов имеет полномочия на выполнение определенных действий. В этой части процедуры определяется, кто имеет полномочия на отключение системы и чьей обязанностью является контакт с клиентами, прессой и органами правопорядка. Назначается официальное лицо, которое будет заниматься именно этими вопросами. Обычно это сотрудник, входящий в группу обработки инцидентов либо внештатный консультант. В любом случае этот человек определяется в процессе разработки процедуры IRP, а не после проведенной атаки и не во время обработки инцидента.

Документирование

Процедура IRP должна определять, каким образом группа обработки инцидентов будет фиксировать свои действия, включая описание данных, подлежащих сбору и сохранению. Этот момент важен по двум причинам: он помогает разобраться в последствиях инцидента и, возможно, предотвращает дальнейшие неприятности посредством привлечения органов правопорядка. Как правило, группе обработки инцидента полезно иметь набор переносных компьютеров для работы.

Тестирование процедуры

Обработка инцидентов требует тестирования. Не следует надеяться на то, что при первом запуске процедуры IRP все пройдет гладко. Сразу после разработки процедуры IRP группе обработки следует провести некоторые тесты. Необходимо проговорить ситуацию и попросить каждого члена группы обработки рассказать о действиях, которые необходимо предпринять в описанных обстоятельствах. Каждый член группы должен следовать предписаниям процедуры. С помощью этого подхода определяются очевидные недостатки процедуры с последующим их устранением.

Процедура IRP должна пройти тестирование в реальных условиях. Попросите сотрудника отдела безопасности смоделировать атаку на организацию, обработку которой произведет группа обработки инцидентов. Эти тесты могут быть как плановыми, так и внезапными.

Процедура управления конфигурацией

Процедура управления конфигурацией определяет шаги, предпринимаемые для изменения состояния компьютерных систем, сетевых устройств и программных компонентов. Целью данной процедуры является идентификация соответствующих изменений во избежание их ошибочного расценивания как инцидентов, связанных с нарушением безопасности, и для проверки новой конфигурации с точки зрения безопасности.

Вопрос эксперту

Вопрос. Действительно ли необходимо тестировать процедуру IRP?

Ответ. Да, это так. Процедура обработки инцидентов, как правило, выполняется не ежедневно и даже не еженедельно. Только имея опыт, можно безошибочно определять ту или иную ситуацию при исследовании инцидента. Ничто не может заменить регулярные упражнения.

Начальное состояние системы

Когда новая система начинает работу, это состояние следует задокументировать. Как минимум, в этой документации необходимо указывать следующие параметры:

- операционную систему и ее версию;
- уровень обновления;
- работающие приложения и их версии;
- начальные конфигурации устройств, программные компоненты и приложения.

Кроме того, может понадобиться создать криптографические проверочные суммы для всех системных файлов и любых других файлов, которые не должны изменяться в процессе функционирования системы.

Процедура контроля над изменениями

Когда в систему необходимо внести изменения, следует выполнять процедуру контроля над конфигурацией. Эта процедура призвана обеспечить резервирование старых данных конфигурации и тестирование предлагаемых изменений перед их реализацией. В дополнение к этому в запросе об изменении следует отобразить процедуры изменения и отката изменений. После внесения изменения конфигурацию системы нужно обновить для отражения нового состояния системы.

Методология разработки

В организациях, разрабатывающих новые системы, должна присутствовать методология разработки. Она включает множество шагов, которые не связаны с обеспечением безопасности и поэтому не будут здесь обсуждаться. Тем не менее, чем раньше в новом проекте будут рассмотрены вопросы безопасности, тем вероятнее, что конечная система будет должным образом защищена. Для каждой из фаз разработки, описанных в следующих разделах, мы обсудим вопросы безопасности, на которые следует обратить особое внимание.

Определение требований

Методология предусматривает учет требований безопасности в процессе сбора требований в любом проекте. Для некоторых требований методология должна ссылаться на политики информации и безопасности организации. Кроме того, в документе с требованиями необходимо определять секретную информацию и все ключевые требования безопасности для системы и проекта.

Разработка

В процессе разработки проекта методология предусматривает представление безопасности для обеспечения надежной защиты проекта. Сотрудники отдела безопасности могут участвовать в процессе в качестве членов группы разработки или рецензентов. Любые требования безопасности, которые не могут быть выполнены в процессе разработки, должны быть идентифицированы, при необходимости следует отказаться от защиты.

При программировании системы разработчики ПО должны быть осведомлены о проблемах программирования, таких как переполнение буфера. Перед тем как приступить к программированию, следует обучить персонал нужным аспектам компьютерной безопасности.

Тестирование

По достижении фазы тестирования необходимо осуществить проверку требований безопасности. Сотрудники отдела безопасности могут оказать помощь в написании плана тестирования. Имейте в виду, что тестирование требований безопасности зачастую оказывается сложным процессом (трудно доказать, например, что злоумышленник не сможет просматривать секретную информацию).

Примечание

Тестирование безопасности включает тесты, направленные на определение уровня защиты системы. Этот аспект можно выразить следующим вопросом: насколько вы уверены в том, что злоумышленник не сможет преодолеть средства контроля над безопасностью? Такое тестирование является очень дорогостоящим и отнимает много времени.

Реализация

Фаза реализации проекта также предусматривает требования безопасности. Группа реализации должна использовать нужные процедуры управления конфигурацией, а сотрудники отдела безопасности должны проверить систему на наличие уязвимостей и соответствие политике безопасности.

Примечание

Методология разработки предназначена не только для внутренних разработок. Аналогичные шаги следует предпринимать и при работе с коммерческими проектами.

Планы восстановления после сбоев

В каждой организации должен быть предусмотрен план восстановления после сбоев (DRP) для выхода из таких экстремальных ситуаций, как пожары, атаки на переполнение буфера и другие события, выводящие систему из строя. Часто этот план отсутствует, так как считается слишком дорогостоящим, либо организация не может держать альтернативную базу для выполнения операций с оборудованием, находящимся в состоянии готовности. DRP не обязательно требует наличия запасного помещения, это план, которому будет следовать организация, в случае если произойдет наихудшее. Это может быть либо простой документ, предписывающий сбор ключевых сотрудников в соседнем ресторане в случае пожара в здании, либо достаточно сложный, определяющий порядок функционирования организации, в случае если все (или отдельные) компьютеры выйдут из строя.

Правильный план DRP должен учитывать различные уровни неполадок: отдельные системы, хранилища данных и помещения в целом. В следующих параграфах этот материал рассматривается более подробно.

Сбои отдельной системы или устройства

Наиболее часто происходит сбой отдельной системы или устройства. Такие сбои происходят в сетевых устройствах, жестких дисках, материнских платах, сетевых картах или программных компонентах. В рамках разработки данной части DRP необходимо проверить среду организации на предмет ее уязвимости в случае такого сбоя. Для каждого сбоя должен быть разработан план, позволяющий возобновить функционирование системы за приемлемый промежуток времени. Каким по длительности является этот "приемлемый" промежуток, зависит от важности рассматриваемой системы. Например, компьютерный узел, задействованный в производственном процессе и предназначенный для разработки графиков производства и оформления заказов на поставку сырья потребует восстановления в течение четырех часов, в противном случае производство остановится. Для предотвращения подобного сбоя требуется запасная система, которую можно оперативно подключить, либо кластеризация. Выбор метода зависит от стоимости решения. Независимо от того, какому решению отдается предпочтение, DRP указывает, что необходимо предпринять для продолжения работы системы без потерявших работоспособность компонентов.

Совет

План DRP должен разрабатываться совместно с функциональными подразделениями организации, чтобы их сотрудники имели понятие о том, какие шаги они должны предпринимать для продолжения нормальной работы.

События, связанные с хранением данных

План DRP должен предусматривать процедуры на случай серьезной неполадки центра хранения данных. Например, что делать в случае, если центр сгорел, как восстановить его работу? Одним из обязательных вопросов для рассмотрения является поломка оборудования. В плане должны быть предусмотрены способы подключения дополнительного оборудования.

На тот случай, если центр данных вышел из строя, а остальная часть системы функционирует нормально, план DRP должен предусматривать размещение нового оборудования, а также способы быстрого восстановления всех сетевых соединений. В данном случае можно использовать запасное помещение, однако этот способ является довольно дорогостоящим. Если наличие запасных помещений не входит в план, следует предусмотреть другие варианты восстановления компьютерных систем.

Как в случае с отдельными событиями, план DRP определяет порядок работы организация в процессе восстановления систем.

События, связанные с организацией в целом

Когда речь идет о плане DRP, обычно подразумеваются события, наносящие ущерб организации в целом. Такие события происходят не часто, но представляют наибольшую опасность. Чтобы предусмотреть в плане DRP подобные события, необходимо, чтобы каждое подразделение организации участвовало в создании этого плана. Первым шагом является выявление первоочередных систем, которые нужно восстановить для обеспечения жизнедеятельности организации. Если компания поддерживает сайт электронной коммерции, наиболее важными системами являются компьютеры и сеть. Если фирма выпускает продукцию, в первую очередь нужно восстанавливать производственное оборудование.

Тестирование DRP

План DRP - это сложный документ, и, скорее всего, вы не напишете его с первого раза. Следовательно, необходимо проводить тестирование DRP. Тестирование необходимо не только для обеспечения правильности DRP на данный момент времени, но и на будущее.

Проверка DRP может быть очень дорогостоящей операцией и привести к значительным финансовым затратам. Имея это в виду, целесообразно

определить ответственных сотрудников и периодически выполнять проверку плана, а также ежегодное полномасштабное тестирование.

Вопросы для самопроверки

- Почему политика является важным документом?
- Политика, определяющая технические требования безопасности, называется.

Создание политики

Теперь, после обсуждения всех политик, действующих в организации, давайте поговорим о создании политики, соответствующей вашей компании. Каждая компания работает по собственным правилам, следовательно, должна иметь собственную уникальную политику. Для обучения персонала разработке политики полезно использовать шаблоны политик. Однако повторение слово в слово политики другой организации не является хорошим способом создания политик.

Определение наиболее важных аспектов

Первым шагом при создании политики организации является определение наиболее важных политик. Например, компания, занимающаяся распространением информации через интернет, будет придавать большее значение плану восстановления в сравнении с политикой использования компьютеров. Сотрудники отдела безопасности организации должны выявить и описать все важнейшие политики, в противном случае необходимую информацию в этой области можно будет получить посредством оценки угроз.

Совет

Сотрудники отдела безопасности должны прибегать к помощи системных администраторов, отдела кадров и руководителей организации для определения наиболее важных политик.

Определение допустимого поведения

То, что называется допустимым поведением сотрудников, зависит от порядков, установленных в организации (культуры организации). Например, в некоторых компаниях сотрудникам разрешается неограниченно работать в интернете. Культура организации призвана обеспечить эффективность исполнения обязанностей сотрудниками и их начальниками. В других компаниях налагаются ограничения на выход сотрудников в интернет, кроме того, работают программы, ограничивающие доступ к определенным веб-сайтам.

Политики этих компаний значительно отличаются друг от друга. Действительно, сотрудники первой компании вовсе не применяют политику использования интернета. Специалисты в области информационной безопасности должны помнить, что не все политики подходят для использования. Перед началом создания политики необходимо внимательно изучить культуру организации и требования, предъявляемые к ее сотрудникам.

Определение руководителей

Политика, созданная в вакууме, редко является успешной. Имея это в виду, разработку политики должны проводить работники отдела безопасности при помощи других сотрудников организации. Отдел безопасности при разработке любых политик должен руководствоваться рекомендациями генерального директора организации и сотрудников отдела кадров. В процессе создания политик, как правило, участвуют системные администраторы, пользователи компьютеров и отдел охраны.

Другими словами, в разработке политики должны быть задействованы те лица, на которые данная политика будет распространяться, чтобы сотрудники понимали, чего ожидать в той или иной ситуации.

Определение схем политик

Разработка политики начинается с формирования схемы (одна схема уже была представлен в этой лекции). Существует множество источников качественных схем политик. Некоторые из них приведены в книгах, а некоторые доступны в интернете. Например, RFC 2196 "The Site Security Handbook" содержит перечень схем для различных политик.

Разработка

При разработке политик безопасности необходимо, в первую очередь, руководствоваться вопросами безопасности. Это не означает, что отдел безопасности должен разрабатывать политики без участия других подразделений, но он должен взять на себя ответственность за проект и проконтролировать его завершение.

Процесс разработки политики следует начать со схемы и черновых набросков каждого раздела политики. В то же время следует проконсультироваться с руководителями организации и сообщить им о выполняемом проекте. Пригласите руководителей для участия в проекте. Тем из них, кто примет предложение, необходимо выслать черновой вариант политики и пригласить на собрание, на котором он будет обсуждаться и корректироваться. В зависимости от размеров организации и того, какая

именно политика разрабатывается, могут рассматриваться несколько аспектов.

Руководить собранием должны сотрудники отдела безопасности. Следует проработать каждый раздел политики, выслушать все комментарии и все обсудить. Однако имейте в виду, что некоторые предложения бывают ошибочными. В этом случае сотрудники отдела безопасности должны объяснить причины того, что предлагаемые решения увеличат риск или не смогут быть правильно реализованы. Следите за тем, чтобы остальные слушатели понимали, о чем идет речь, и осознали причины выбора тех или иных решений.

Данный процесс имеет смысл повторить при работе с окончательным черновым вариантом. По завершении обсуждения проекта его следует отдать менеджерам для утверждения и реализации.

Развертывание политики

Чтобы создать политику, требуется несколько человек. Чтобы эффективно применить политику, необходимо работать со всей организацией в целом.

Понимание политики

Сотрудники каждого подразделения компании, на которое распространяется политика, должны вникнуть в ее суть. Это достигается довольно легко, так как в процессе создания политики участвуют все руководители отделов. Менеджерам отделов можно сообщить, кто из подразделений организации участвовал в процессе, голосуя за нужды своего отдела.

Также требуется согласие менеджеров с важностью политики и необходимостью ее применения. Вышестоящий менеджер зафиксирует тот факт, что политика важна для успешной и безопасной работы организации, и этим заявлением будут руководствоваться подчиненные ему менеджеры.

Обучение

Сотрудники, на которых распространяется новая политика, должны пройти обучение согласно доли своей ответственности. В обучении могут участвовать отдел кадров или учебный отдел, однако это задача отдела безопасности, в особенности когда речь идет об изменениях, которые распространяются на всех пользователей. Возьмем, к примеру, изменение политики использования паролей. По состоянию на утро понедельника все пароли пользователей должны быть длиной в восемь символов и содержать некоторый набор из букв и цифр, срок действия паролей равен 30 дням. При внесении подобного изменения в домене Windows все пароли немедленно становятся недействительными. Это вынудит каждого пользователя изменить

свой пароль в понедельник утром. Без соответствующего инструктажа пользователи не смогут выбрать сильные пароли и, вероятно, начнут обращаться в службу технической поддержки. Если пользователи выберут пароли и не запомнят их, то на следующий день они опять будут звонить в службу поддержки или начнут записывать пароли на листочках. И то и другое ведет к снижению безопасности системы.

Лучше всего провести учебу по вопросам, связанным с безопасностью, и рассказать сотрудникам о вносимых изменениях и их причинах. Их можно научить, как выбирать надежные пароли, простые для запоминания. Службу поддержки следует проинформировать о возможных проблемах с паролями. Сотрудники отдела безопасности совместно с системными администраторами выяснят, возможно ли в данной ситуации провести смену паролей в несколько этапов.

Примечание

Изменения, вносимые в систему аутентификации, оказывают влияние на максимально возможное число сотрудников (на всех!) и, следовательно, должны проводиться с осторожностью.

Реализация

Как показано в предыдущем разделе, радикальные изменения в среде безопасности могут плохо повлиять на безопасность организации. Постепенный и тщательно спланированный переход всегда более предпочтителен. Имея это в виду, отдел безопасности должен совместно с системными администраторами или другими подразделениями, на которые распространяется изменение, максимально упростить это изменение. Помните, что безопасность уже рассматривалась как препятствие для работы, доказывать эту мысль сотрудникам уже не требуется.

Эффективное использование политики

Политика может работать как полицейская дубинка, но она более эффективна, когда используется в качестве средства обучения. Имейте в виду, что большинство сотрудников работают, в первую очередь, в интересах организации и стараются выполнять свои обязанности по возможности лучше.

Новые системы и проекты

При запуске новых систем и проектов должны соблюдаться имеющиеся политики безопасности и процедуры разработки. Это позволяет отделу безопасности быть участником разработки проекта и на ранней стадии процесса определить требования безопасности.

Если новая система не сможет отвечать требованиям безопасности, то у компании будет время, чтобы понять суть представляемой опасности и обеспечить другой механизм защиты.

Имеющиеся системы и проекты

По мере утверждения новых политик каждая система должна проверяться на соответствие утверждаемым политикам. Отдел безопасности совместно с системными администраторами и подразделением, использующим систему, должен внести в системы соответствующие коррективы. Иногда эти коррективы требуют перепрограммирования каких-либо модулей, которое не может быть выполнено мгновенно. Отдел безопасности в этом случае должен осознать, что функционирование организации может быть прервано на некоторое время, и совместно с администраторами и другими подразделениями приложить все усилия для обеспечения скорейшего внесения изменений в рамках бюджета и структурных ограничений системы.

Аудит

Во многих организациях имеются внутренние отделы аудита, которые периодически осуществляют аудит систем на соответствие политике. Отдел безопасности должен ознакомить сотрудников этого отдела с новыми политиками и поработать некоторое время вместе, чтобы аудиторы вникли в суть политики, прежде чем будут проверять системы на соответствие.

Обмен информацией должен быть двусторонним. Отдел безопасности должен объяснить аудиторам, как была разработана политика и что ожидается от политики с точки зрения безопасности. Аудиторы должны объяснить специалистам по безопасности, каким образом будет проводиться аудит и на поиск чего он будет нацелен. Необходимо разработать соглашение о том, какие типы систем являются адекватными для различных разделов политики.

Проверка политики

Даже качественно разработанная политика не вечна. Каждая политика должна регулярно проверяться на соответствие требованиям организации. В большинстве случаев достаточно проводить такую проверку раз в год. Некоторые процедуры, например процесс обработки инцидентов или план восстановления после сбоев, требуют более частых проверок.

В процессе проверки необходимо связаться со всеми руководителями и подразделениями, которые не участвовали в разработке политики. Попросите каждого сотрудника прокомментировать имеющуюся политику. Возможно, имеет смысл устроить общее собрание, если имеются какие-либо важные комментарии (например, комментарии сотрудников из отдела безопасности).

Внесите корректировки в политику, получите подтверждение и возобновите процесс обучения.

Разработка политики использования интернета

Этот проект продемонстрирует, как разработать политику, а также какие вопросы могут возникнуть при использовании этой политики.

Шаг за шагом

1. Если вы работаете в группе, разделите группу на пары. Каждая пара будет разрабатывать свою собственную политику и представлять собой отдельную группу.
2. Разработайте схему политики. Не забудьте включить раздел для входящих и исходящих соединений.
3. Определите приемлемые типы входящих соединений.
4. Определите приемлемые типы исходящих соединений. Если вам кажется, что все указано правильно, перейдите к определению типов сайтов, которые могу посещать сотрудники.
5. Представьте политику другим членам группы. Некоторые из них должны выступать в роли сотрудников организации, а другие - в роли менеджеров.
6. Как вариант, различные пары могут работать над разными политиками организации.

Выводы

Разработка политики, как правило, осуществляется очень просто. Тем не менее, сотрудники и руководители встают перед выбором тех или иных подходов при разработке политики. Рядовым сотрудникам не нравится все, что может сказаться на их рабочей нагрузке или секретности их действий. Руководителям же не нравятся политики, предоставляющие слишком много свободы.

Контрольные вопросы

1. Назовите три раздела, которые должны присутствовать в каждой политике или процедуре.
2. Что определяет политика безопасности?
3. Должна ли политика безопасности определять конкретные требования реализации для каждого типа систем внутри самой политики?
4. Почему в политику безопасности включают отказы от защиты?
5. Что должна определять политика использования компьютеров?
6. Рекомендуется ли разрешать неограниченное использование компьютеров?

7. Для каких лиц должны указываться требования, содержащиеся в процедурах управления пользователями?
8. Когда сотрудник переходит с одной должности на другую внутри организации, кто должен нести ответственность за уведомление системных администраторов о необходимости изменения профиля доступа данного сотрудника?
9. Какова цель процедуры системного администрирования?
10. Почему необходимо соблюдать внимательность при определении целей IRP?
11. Назовите пять подразделений, сотрудники которых всегда должны входить в группу обработки инцидентов.
12. Назовите четыре ключевых раздела методологии разработки.
13. Назовите три типа событий, которые должны быть указаны в DRP.
14. Какие действия должен выполнять отдел безопасности в процессе создания политики?
15. Почему отдел безопасности должен работать совместно с отделом аудита?