9. Лекция: Рекомендации по обеспечению сетевой безопасности

Вводится понятие административной безопасности. Даются рекомендации по организации работы службы безопасности на предприятии. Анализируются средства технической безопасности. Рассматриваются плюсы и минусы использования стандарта ISO 17799.

Концепция "авторитетных рекомендаций" представляет собой набор указаний, которые обеспечивают должный уровень безопасности. Авторитетные рекомендации (далее - рекомендации) - это комбинация указаний, эффективность которых доказана при применении в самых различных организациях. Не все указания пригодны для использования в конкретной организации. В некоторых компаниях необходимы дополнительные политики и процедуры, обучение персонала или контроль за технической безопасностью для достижения приемлемого уровня управления безопасностью.

Административная безопасность

Рекомендации по административной безопасности - это те решения, которые соответствуют политикам и процедурам, ресурсам, степени ответственности, потребностям в обучении персонала и планам по выходу из критических ситуаций. Эти меры призваны определить важность информации и информационных систем для компании и объяснить персоналу, в чем именно заключается эта важность. Рекомендации по обеспечению административной безопасности определяют ресурсы, необходимые для осуществления должного управления рисками и определения лиц, несущих ответственность за управление безопасностью организации.

Политики и процедуры

Политики безопасности определяют метод, согласно которому обеспечивается безопасность внутри организации. После определения политики предполагается, что большинство сотрудников компании будут ее соблюдать. Следует понимать, что полного и безоговорочного выполнения политики не будет. В некоторых случаях политика будет нарушаться из-за требований, связанных с деловой деятельностью организации. В других случаях игнорирование политики обусловлено сложностью ее выполнения.

Даже принимая во внимание тот факт, что политика будет выполняться не постоянно, она формирует ключевой компонент программы по обеспечению безопасности и должна быть включена в перечень рекомендаций по защите. При отсутствии политики сотрудники не будут знать, что делать для защиты информации и компьютерных систем.

В качестве рекомендаций по безопасности необходимо рассматривать следующие политики.

- Информационная политика. Определяет степень секретности информации внутри организации и необходимые требования к хранению, передаче, пометке и управлению этой информацией.
- Политика безопасности. Определяет технические средства управления и настройки безопасности, применяемые пользователями и администраторами на всех компьютерных системах.
- Политика использования. Определяет допустимый уровень использования компьютерных систем организации и штрафные санкции, предусмотренные за их нецелевое использование. Данная политика также определяет принятый в организации метод установки программного обеспечения и известна как политика приемлемого использования.
- Политика резервного копирования. Определяет периодичность резервного копирования данных и требования к перемещению резервных данных в отдельное хранилище. Кроме того, политики резервного копирования определяют время, в течение которого данные должны быть зарезервированы перед повторным использованием.

Политики сами по себе не формируют исчерпывающих инструкций по выполнению программы безопасности организации. Следует определить процедуры, согласно которым сотрудники будут выполнять определенные задачи, и которые будут определять дальнейшие шаги по обработке различных ситуаций с точки зрения безопасности. Внутри организации должны быть определены следующие процедуры.

- Процедура управления пользователями. Определяет, кто может осуществлять авторизованный доступ к тем или иным компьютерам организации, и какую информацию администраторы должны предоставлять пользователям, запрашивающим поддержку. Процедуры управления пользователями также определяют, кто несет ответственность за информирование администраторов о том, что сотруднику больше не требуется учетная запись. Аннулирование учетных записей важно с той точки зрения, чтобы доступ к системам и сетям организации имели только лица с соответствующими деловыми потребностями.
- Процедуры системного администрирования. Описывают, каким образом в данный момент времени применяется политика безопасности на различных системах, имеющихся в организации. Эта процедура подробно определяет, каким образом должна осуществляться работа с обновлениями и их установка на системы.
- Процедуры управления конфигурацией. Определяют шаги по внесению изменений в функционирующие системы. Изменения могут включать в

себя обновление программного и аппаратного обеспечения, подключение новых систем и удаление ненужных систем.

Примечание

Во многих организациях управление обновлениями представляет собой большую проблему. Отслеживание обновлений для снижения уровня уязвимости систем, а также тестирование этих обновлений перед установкой на функционирующие системы (чтобы не отключать работающие приложения) занимает очень много времени, но эти задачи очень важны для любой организации.

Наряду с процедурами по управлению конфигурацией устанавливаются методологии разработки новых систем. Они очень важны для управления уязвимостями новых систем и для защиты функционирующих систем от несанкционированного изменения. Методология разработки определяет, как и когда должны разрабатываться и применяться меры защиты. Необходимо делать акцент на этих сведениях при проведении любых инструктажей разработчиков и менеджеров проектов.

Ресурсы

Для применения корректных рекомендаций по безопасности необходимо осуществить присвоение ресурсов. К сожалению, не существует формулы, которую можно использовать для определения того, сколько ресурсов (денег или сотрудников) должно быть выделено в соответствии с программой безопасности, руководствуясь лишь размерами организации. В этом уравнении слишком много переменных. Необходимые ресурсы обуславливаются размером организации, деловыми процессами организации и опасностями, угрожающими ей.

Количество ресурсов должно определяться на базе корректной и полной оценки рисков, в соответствии с алгоритмом обработки рисков. В этом случае используется управление проектом. На рисунке 9.1 показано, каким образом относятся друг к другу ресурсы, время и область проекта. Если программа безопасности воспринимается как проект, то организация должна выделить достаточно ресурсов для уравновешивания треугольника либо расширить время или уменьшить область.

Персонал

Независимо от того, насколько велика или мала организация, некоторым сотрудникам должно быть поручено выполнение задач, связанных с обработкой уязвимостей и обеспечением информационной безопасности. В небольших организациях это может быть возложено на сотрудника отдела информационных технологий. В более крупных организациях могут

существовать целые отделы безопасности. В рекомендациях не предписывается какое-либо определенное число сотрудников, однако настоятельно рекомендуется, чтобы, по крайней мере, на одного сотрудника были возложены обязанности по обеспечению безопасности.

Сотрудники отдела безопасности должны иметь следующие навыки.

- Администрирование безопасности. Понимание ежедневного процесса администрирования устройств обеспечения безопасности.
- Разработка политик. Опыт в разработке и поддержке политик безопасности, процедур и планов.
- Архитектура. Понимание сетевой и системной архитектур и применение новых систем.
- Исследование. Проверка новых технологий безопасности на предмет того, насколько они могут противостоять риску, представляемому для организации.
- Оценка. Наличие опыта сбора сведений о потенциальных рисках в организациях или подразделениях. Оценка может включать в себя навыки проникновения и тестирования безопасности.
- Аудит. Наличие опыта ведения аудита систем или процедур.

Рис. 9.1. Треугольная диаграмма управления проектом

Все эти навыки полезны для организации, однако мелкие компании могут не иметь возможности привлечь сотрудников, обладающих всеми этими навыками. В данном случае наиболее рациональным выходом из положения является привлечение администратора безопасности или разработчика политик в качестве сотрудника, а для выполнения других функций следует воспользоваться услугами сторонних организаций.

Существуют люди, у которых есть практически все перечисленные навыки. Эти специалисты, как правило, обладают большим опытом и, следовательно, требуют очень высокой зарплаты. Если в рассматриваемой организации бюджет ограничен, и зарплата соответствующего уровня не может быть обеспечена, не стоит надеяться на то, что удастся привлечь такого специалиста. Вместо этого следует заняться поиском лиц, у которых есть

общее представление обо всех перечисленных моментах и конкретные навыки, которые необходимы в наибольшей степени.

Бюджет

Размер бюджета безопасности организации зависит от области действия и временных рамок проекта безопасности, а не от размеров организации. Организации с мощными программами безопасности могут иметь меньший бюджет, чем мелкие организации, которые только начинают создавать свою программу безопасности.

Распределение средств играет важную роль в вопросах, связанных с бюджетом безопасности. Бюджет безопасности должен быть разделен между капитальными затратами, текущими операциями и обучением персонала. Во многих организациях допускается ошибка, заключающаяся в том, что компаниями приобретаются дорогие средства безопасности без резервирования достаточного количества средств на обучение персонала работе с этими средствами. В других случаях организации приобретают эти средства, предполагая, что число сотрудников может быть сокращено, или руководство сотрудниками может осуществляться на разных уровнях. В большинстве случаев новые средства безопасности не позволяют сократить штат сотрудников. Несомненно, данному вопросу следует уделить дополнительное внимание.

Во многих организациях сотрудники и руководящий состав полагают, что повышенный уровень автоматизации средств безопасности позволит сократить число сотрудников, задействованных в обеспечении безопасности. К сожалению, это предположение оправдывается очень редко. Причина в том, что новые средства безопасности не автоматизируют процесс, выполняемый вручную. В большинстве случаев получается так, что процесс в данный момент времени не выполняется вовсе. Следовательно, новое средство безопасности "предоставляет новую возможность", а не повышает эффективность системы безопасности. Таким образом, покупка нового средства, как правило, увеличивает нагрузку на сотрудников и требует привлечения дополнительного персонала.

Распределение бюджета, согласно рекомендациям, должно основываться на планах проекта безопасности (которые, в свою очередь, базируются на риске, существующем для организации). Для успешного выполнения планов проекта безопасности должны быть выделены все необходимые средства.

Ответственность

Некоторое должностное лицо в организации должно нести ответственность за управление рисками, связанными с безопасностью информации. С недавнего времени эти обязанности в крупных компаниях принято возлагать

на специального сотрудника исполнительного уровня - главного специалиста по безопасности информации (Chief Information Security Officer, CISO).

Вопрос эксперту

Вопрос. Старший руководящий сотрудник попросил обосновать бюджет безопасности. Каким образом это лучше сделать?

Ответ. Бюджет безопасности должен быть связан с уменьшением уровня опасности, представляемой для информации организации. Иными словами, бюджет должен четко соответствовать потенциальным результатам оценки рисков. Выделите следующие моменты.

- Во-первых, покажите, что существует опасность, которую необходимо взять под контроль или снизить. Это подтвердит актуальность и необходимость проекта.
- Во-вторых, оценка риска должна включать в себя определение потенциального ущерба, наносимого организации в случае успешного проведения атаки. Здесь речь идет о том, во сколько организации обойдется устранение последствий инцидента.

Независимо от размеров организации, должностное лицо исполнительного уровня должно нести эту ответственность. В некоторых компаниях главный специалист по финансам предоставляет соответствующие отчеты безопасности. В других компаниях эти обязанности выполняют главный специалист по безопасности информации или главный специалист по технологии.

Независимо от того, какое должностное лицо предоставляет отчеты, этот сотрудник должен понимать, что безопасность - очень важная часть его работы. Сотрудник исполнительного уровня должен иметь право на определение политики организации и проверять все политики, связанные с безопасностью организации. Этот сотрудник также должен иметь право на принуждение к использованию политики системных администраторов и сотрудников, задействованных в обеспечении физической безопасности организации.

Не предполагается, что рассматриваемый сотрудник будет выполнять ежедневные операции по администрированию и обеспечению безопасности. Эти функции могут и должны быть поручены сотрудникам отдела безопасности.

Главный специалист по безопасности организации должен разработать систему измерения, фиксирующую степень достижения целей по обеспечению безопасности. Среди измеряемых параметров могут быть число уязвимостей в системах, степень выполнения проекта безопасности или

реализации соответствия рекомендациям. Измеренные параметры должны регулярно сообщаться старшему руководящему составу (как правило, ежемесячно). Данные отчеты также должны представляться совету директоров компании. Так как безопасность стала важной частью процесса управления рисками в организациях, необходимо обеспечить широкую огласку и понимание данного вопроса всеми сотрудниками компании.

Примечание

Инструкции по выполнению финансовых операций и страхованию должны требовать предоставление совету директоров регулярных отчетов о состоянии безопасности организации.

Обучение

Обучение сотрудников является одной из наиболее важных составляющих процесса управления угрозами, представляемыми для безопасности информации. Если сотрудники не будут обладать достаточным уровнем знаний и не будут работать сообща, любые попытки управления рисками безуспешны. Рекомендуется осуществлять три формы обучения.

- Превентивные меры.
- Принудительные меры.
- Поощрительные меры.

Превентивные меры

Обучение превентивным мерам обеспечивает сотрудников детальными знаниями о защите информационных ресурсов организации. Сотрудникам следует рассказать, почему требуется защищать информационные ресурсы организации; понимание причин применения превентивных мер сделает их более совместимыми с политиками и процедурами. Если сотрудники не будут знать, каковы цели обеспечения безопасности, то попытаются нарушить установленные политики и процедуры.

Кроме информирования сотрудников о важности обеспечения безопасности, необходимо предоставить подробные сведения и подходы к обеспечению соответствия политике организации. Такие мифы, как, например, "надежные пароли трудно запоминать, поэтому их следует записывать на бумаге", следует рассмотреть и скорректировать.

Строгие превентивные меры могут принимать различные формы. В осведомительные программы следует включить как рекламные кампании, так и обучение сотрудников. Рекламные кампании должны включать в себя статьи новостей и плакаты. Для напоминания сотрудникам об их

обязанностях используйте электронные сообщения и всплывающие окна. Ключевыми темами рекламных кампаний должны являться следующие.

- Распространенные ошибки сотрудников, например, запись на бумаге или разглашение паролей.
- Распространенные случаи несоблюдения безопасности, например, предоставление слишком большого объема информации клиенту.
- Важная информация, связанная с вопросами безопасности, например, с кем необходимо связываться в случае подозрения на угрозу безопасности.
- Текущие вопросы информационной безопасности, такие как антивирусная защита и безопасность удаленного доступа.
- Темы, помогающие сотрудникам в работе, например, защита переносных компьютеров в поездке или защита детей от злоумышленников в интернете.

Занятия по обучению безопасности должны быть нацелены на различные группы сотрудников организации. Все новые сотрудники должны проходить краткий инструктаж (длительностью до часа). Других сотрудников следует обучать примерно каждые два года. В процессе этого обучения предоставляется следующая информация.

- Почему в организации необходимо обеспечивать безопасность.
- Ответственность сотрудника относительно вопросов безопасности.
- Детальные сведения о политиках информационной безопасности организации.
- Детальные сведения о политиках использования, установленных в организации.
- Предлагаемые методы выбора надежных паролей.
- Предлагаемые методы предотвращения атак социального инжиниринга, включая вопросы, заданные и не заданные сотрудниками справочной службы.

Совет

Вместо того чтобы тратить час на устную лекцию, попробуйте включить в занятия практические примеры и видеоматериал. На сайте Commonwealth Films (http://www.commonwealthfilms.com//) есть хороший выбор обучающих видеоматериалов по теме безопасности.

Администраторы должны получить базовые инструкции по вопросам безопасности и пройти дополнительное обучение согласно их конкретной ответственности. Длительность дополнительных уроков не должна превышать полчаса, и на этих занятиях необходимо рассмотреть следующие вопросы.

- Самые последние методы работы хакеров.
- Текущие угрозы безопасности.
- Текущие уязвимости и обновления безопасности.

Разработчики должны получить базовые инструкции по вопросам безопасности. Для них следует проводить дополнительные занятия в зависимости от вопросов, за которые они ответственны, в частности, за обеспечение безопасности процесса разработки. Во время этих занятий необходимо сконцентрироваться на методологии разработки и процедурах управления конфигурацией.

Для менеджеров компании следует периодически устраивать презентации о текущем состоянии дел с предоставлением актуальных и детальных оценок угроз и планов по снижению риска. В презентации включается обсуждение системы измерения и методов определения эффективности программы безопасности при помощи этой системы.

Не следует считать, что сотрудникам отдела безопасности не нужно проходить инструктаж по обеспечению безопасности. Можно предположить, что как добросовестные сотрудники они и так прекрасно знают о своих обязанностях, однако им следует периодически предоставлять инструкции по самым последним средствам безопасности и методам работы хакеров.

Принудительные меры

Большинство сотрудников будут выполнять превентивные меры и следовать политике организации. Тем не менее, некоторые сотрудники могут уклоняться от этого (непреднамеренно или даже умышленно), что может нанести организации вред. В организациях следует принимать меры для защиты от таких сотрудников.

Важной составляющей процесса "избавления" от таких сотрудников является обеспечение осведомленности сотрудников об основах политики организации. Обеспечить эту осведомленность можно при помощи соглашений о безопасности. По завершении прохождения сотрудником обучения безопасности ему нужно предоставить копии соответствующих политик и предложить подписать соглашение о том, что он ознакомился и согласился с политиками организации. Эти подписанные документы отдаются на хранение в отдел кадров и могут использоваться в случае судебного процесса.

Поощрительные меры

Вследствие природы вопросов, связанных с безопасностью, сотрудники могут не утруждать себя информированием отделов безопасности о наличии нарушений безопасности. Однако, так как сотрудники отдела безопасности

не могут одновременно находиться в нескольких местах и уследить абсолютно за всем, сотрудники являются важной частью системы оповещения об опасностях.

Одним из методов, используемым здесь для увеличения уровня отчетности сотрудников об аспектах безопасности, является программа поощрений сотрудников организации. Поощрения не должны быть большими. На самом деле, лучше, если поощрения будут выдаваться в виде небольших денежных сумм. Сотрудников также следует убедить в том, что такие отчеты очень нужны организации, и что сотрудники не будут наказываться за ложные оповещения.

Поощряться могут сотрудники, вносящие предложения о повышении уровня безопасности и решении других проблем, связанных с безопасностью. Успешные поощрительные программы реализуются посредством запросов у сотрудников ответов на вопросы через службу новостей организации. В такой программе организация может публиковать полученные рекомендации с указанием сотрудников, внесших соответствующие предложения.

Планы выхода из критических ситуаций

Даже в наиболее благоприятных обстоятельствах никогда не получится полностью устранить опасности, представляемые для информационных ресурсов организации. Чтобы обеспечить быстрое восстановление и снижение ущерба, нанесенного организации в результате инцидента, необходимо сформулировать планы выхода из критических ситуаций.

Обработка инцидентов

В каждой организации должна присутствовать процедура обработки инцидентов. Она определяет шаги, которые необходимо предпринимать в случае взлома защиты или проникновения в систему злоумышленника. Без этой процедуры вы можете потратить много времени на устранение его последствий. Это время является для потенциальных клиентов компании антирекламой и означать потерю средств и утечку информации.

В процедуре обработки инцидента следует детально определить, кто несет ответственность за обработку инцидентов в организации. Без предоставления четких инструкций по этому поводу может быть потрачено лишнее время на поиск виновного в происшествии и ответственного за перевод систем в автономный режим и обращение в органы правопорядка.

В рекомендациях указывается, что периодически нужно тестировать процедуры обработки инцидентов. Изначальные тесты могут анонсироваться заранее и заключаться в совместном диалоге сотрудников в форуме и высказывании ими своего мнения по поводу того, каким

образом можно обработать тот или иной инцидент. Дополнительное тестирование в "реальном" мире должно проводиться таким образом, чтобы неожиданные события симулировали реальные вторжения злоумышленников.

Резервное копирование и архивация данных

Процедуры резервного копирования должны исходить из политики резервного копирования. Процедуры определяют время выполнения резервного копирования и указывают шаги, которые следует выполнять при резервировании данных и их безопасном сохранении. В процедурах архивации данных указывается периодичность повторного использования резервных носителей и места, где должны располагаться носители.

Когда резервный носитель требуется извлечь из места отдельного хранения, необходимо руководствоваться инструкциями, включенными в процедуру и указывающими, каким образом осуществляется запрос и идентификация носителей, метод восстановления данных и способ возвращения носителя в место хранения.

Если в организациях такие процедуры отсутствуют, то существует опасность неправильной интерпретации сотрудниками политики резервного копирования. В этом случае возможны ситуации, когда резервные носители не будут вовремя отсоединяться от сайта или восстановление данных будет происходить некорректно.

Внимание!

Убедитесь, что процедуры разработаны в соответствии с политикой хранения данных организации.

Восстановление после сбоев

В каждой организации должны присутствовать планы восстановления после сбоев для определения требований и целей, достигаемых при возникновении каких-либо неполадок. Планы детально описывают, какие вычислительные ресурсы являются наиболее критичными для организации, и с помощью этих планов формируются конкретные требования по возврату этих ресурсов в работоспособное состояние.

В организациях необходимо иметь планы, предусматривающие выход из различных неблагоприятных ситуаций, начиная от потери одного компьютера и заканчивая выходом из строя всей сети. Кроме того, в сценарии восстановления следует включить ключевые компоненты инфраструктуры, такие как каналы связи и оборудование.

Планы восстановления после сбоев могут не предусматривать наличие резервных "горячих сайтов" с полными копиями всего имеющегося оборудования. Тем не менее, эти планы должны быть хорошо продуманными, а стоимость применения плана - взвешена относительно потенциального ущерба, который может быть нанесен организации.

Любой план восстановления после сбоев необходимо периодически тестировать. По крайней мере, один раз в год должно проводиться полное тестирование. При выполнении этого теста возможно перемещение сотрудников в альтернативные помещения, если это предусматривается в плане.

Планы проектов безопасности

Так как обеспечение безопасности является непрерывным процессом, безопасность информации следует рассматривать как постоянно выполняемый проект. Разделим общий проект на несколько мелких, которые должны быть завершены. Согласно рекомендациям, отдел безопасности организации должен утверждать следующие планы.

- Планы усовершенствования.
- Планы проведения оценок.
- Планы оценки уязвимостей.
- Планы аудита.
- Планы обучения.
- Планы оценки политики.

Усовершенствование

Планы усовершенствования вытекают из процедур оценки. Если в результате оценки определены некоторые опасные области, следует создать планы по усовершенствованию для разрешения возможных проблем и внесения соответствующих изменений в среду. Планы усовершенствования могут включать в себя планирование установки политики, применения средств или внесения изменений в систему, либо создания обучающих программ. Каждая оценка, проводимая в рамках организации, должна быть отправной точкой плана усовершенствования.

Оценка

Отдел безопасности организации должен разрабатывать ежегодные планы оценки риска для организации. В средних организациях это может быть план полной оценки, проводимой один раз в год. В крупных организациях план может предусматривать оценки по подразделениям, а полные оценки могут проводиться реже одного раза в год.

Большим организациям рекомендуется отклоняться от концепции ежегодных оценок. На практике оценки занимают много времени при их организации, выполнении и анализе. В очень больших компаниях может быть затрачено несколько месяцев на планирование, несколько месяцев на выполнение и несколько месяцев - на анализ, в результате чего останется совсем немного времени на непосредственное применение изменений, перед тем как наступит время следующей оценки. В подобных случаях эффективнее выполнять менее масштабные оценки с большей частотой, а полные оценки осуществлять периодически, согласно имеющимся условиям.

Оценка уязвимостей

Отделы безопасности организаций должны регулярно проводить оценку уязвимостей (сканирование) систем организации. Отдел безопасности должен планировать ежемесячную оценку всех систем внутри организации. Если в организации очень много компьютеров, то их нужно сгруппировать и по частям сканировать каждую неделю. Необходимо наличие планов к исполнению, с помощью которых администраторы смогут внести соответствующие коррективы в системы.

Внимание!

При сообщении системным администраторам результатов сканирования уязвимостей необходимо соблюдать внимательность. Помните, что администраторы выполняют свою работу на благо организации, и это их "хлеб". Здесь не должна идти речь о каком-либо соперничестве; наоборот, системные администраторы и администраторы безопасности должны работать совместно для выявления уязвимостей и контроля рисков в организации.

Аудит

Отдел безопасности должен разработать планы проведения аудита на соответствие политике организации. Такие аудиты могут быть сфокусированы на конфигурации систем, соответствии политике резервного копирования или на защите информации в физической форме. Так как аудиты требуют больших усилий со стороны персонала, каждый аудит нацелен на небольшую часть организации. При проведении аудитов системных конфигураций из всех систем можно выбрать образец. При обнаружении значительных расхождений и несоответствий в соответствующем подразделении проводится более масштабный аудит.

Внутренний отдел аудита организации должен иметь свои собственные расписания и планы аудитов. Аудиты, проводимые отделом безопасности, не заменяют аудиты, осуществляемые внутренним отделом аудита. Эти аудиты направлены на определение того, насколько хорошо понимаются и

выполняются политики и процедуры безопасности, с дальнейшим устранением несоответствий и недостатков.

Обучение

Планы обучения должны создаваться совместно с отделом кадров. Эти планы включают в себя расписание учебных занятий и планы проведения рекламных кампаний. В расписании необходимо учитывать, что каждый сотрудник должен проходить обучение один раз в два года.

Оценка политики

Каждая политика организации должна предусматривать даты пересмотра политики. Отдел безопасности должен разрабатывать планы для начала пересмотра и оценки политики по мере приближения даты пересмотра. Как правило, каждый год требуется пересмотр двух политик.

Вопросы для самопроверки

1. Бюджет безопасности должен быть обоснован результатами _____.
2. Когда сотрудники организации должны в первый раз проходить обучение безопасности?

Техническая безопасность

Меры по обеспечению технической безопасности связаны с применением элементов управления безопасностью на компьютерах и в компьютерных сетях. Эти элементы управления являются отражением политик и процедур организации.

Сетевые соединения

Результатом перемещения информации между организациями явились возросшие коммуникационные возможности между сетями различных организаций. Соединение с интернетом сегодня доступно практически в любой организации, и большая часть компаний использует интернет в определенных деловых целях. Чтобы защитить организацию от нежелательных вторжений, необходимо соблюдать следующие рекомендации.

Постоянные соединения

Сетевые соединения с другими организациями или с интернетом должны защищаться межсетевым экраном. Межсетевой экран играет роль огнеупорной стены между двумя комнатами, которая разделяет пространство на два различных участка, и при возникновении пожара в одной из комнат

огонь не перекинется на вторую. Аналогичным образом межсетевые экраны отделяют сети организаций от интернета или сетей других организаций для предотвращения распространения ущерба. Межсетевые экраны являются фильтрующими маршрутизаторами, фильтрами пакетов или межсетевыми экранами прикладного уровня, в зависимости от требований организации.

Примечание

Беспроводные сети следует также отделять от внутренней сети организации (для этого рекомендуется использовать межсетевой экран), так как беспроводное соединение, по сути, представляет собой постоянное соединение с некоторыми неизвестными объектами (это может быть любой пользователь, находящийся поблизости и имеющий карту беспроводного сетевого интерфейса!).

Соединения удаленного доступа

Соединения удаленного доступа могут использоваться для получения несанкционированного доступа к организациям и, следовательно, эти соединения необходимо защищать. Такие соединения могут устанавливаться посредством коммутируемого телефонного подключения либо через интернет. Поскольку они обеспечивают доступ во внутреннюю сеть организации как обычное постоянное соединение, необходимо использовать некоторую форму двухфакторной аутентификации. Речь идет о следующих механизмах аутентификации.

- Модемы обратного вызова. Используются совместно с механизмом аутентификации и являются достаточным средством аутентификации для телефонных соединений. Модемы обратного вызова настраиваются на определенный номер, который они набирают перед установкой телефонного соединения. Пользователь, пытающийся подключиться, не может изменить этот номер. Модемы обратного вызова не подходят для мобильных пользователей (т. е. пользователей, постоянно переезжающих с места на место).
- Динамические пароли. Используются в качестве механизма аутентификации и являются таковыми, если комбинируются с какими-либо данными, известными пользователю.
- Устройства шифрования. Портативные устройства шифрования используются в качестве механизмов аутентификации при их комбинировании с какими-либо данными, известными пользователю. Устройство шифрования должно быть предварительно снабжено соответствующими ключами шифрования и соответствовать тому, что имеет пользователь.

Любой из этих механизмов подходит для аутентификации пользователей через соединения удаленного доступа.

Примечание

Некоторые типы механизмов аутентификации не подходят для виртуальных частных сетей (VPN). Например, если бы для аутентификации использовался биометрический сканер отпечатков пальцев, потенциальная опасность обмана системы была бы намного выше, так как компьютер находится за пределами защищаемого физического местоположения.

Защита от вредоносного кода

Вредоносный код (компьютерные вирусы, троянские программы и черви) является одной из наиболее серьезных угроз для информации. Число и степень сложности этих программ продолжает с каждым днем увеличиваться, и также возрастает степень подверженности современных приложений нецелевому использованию этими программами. Вредоносный код проникает в организации четырьмя основными способами.

- Файлы с общим доступом с домашних и рабочих компьютеров.
- Файлы, загружаемые с сайтов интернета.
- Файлы, поступающие в организацию в виде вложений электронной почты.
- Файлы, внедряемые в системы посредством использования уязвимостей.

Для контроля этой опасности в организации нужно разработать эффективную антивирусную программу. Хорошая антивирусная программа осуществляет контроль за вредоносным кодом в трех точках.

- Серверы. Антивирусное ПО устанавливается на всех файловых серверах и настраивается на периодическое выполнение полной проверки наличия вирусов во всех файлах.
- Рабочие станции. Антивирусное ПО устанавливается на всех рабочих станциях и настраивается на периодическое выполнение полной проверки наличия вирусов во всех файлах. Кроме того, антивирусное ПО настраивается на проверку каждого открываемого файла.
- Системы электронной почты. Антивирусное ПО устанавливается либо на главный почтовый сервер, либо на пути следования электронной почты внутри организации. Настраивается на проверку каждого файлового вложения перед непосредственной доставкой пользователю.

Примечание

Системные уязвимости устраняются посредством регулярного сканирования уязвимостей и установкой соответствующих обновлений.

Установка и настройка антивирусного программного обеспечения лишь наполовину решает проблему вредоносного кода. Для полноты антивирусной программы необходимо обеспечить частые обновления признаков вредоносного ПО и доставку этих обновлений на серверы, рабочие станции и системы электронной почты. Обновления необходимо получать согласно рекомендациям производителя программного обеспечения. Это действие должно выполняться не реже одного раза в месяц.

Многие производители антивирусного ПО предоставляют автоматизированные механизмы загрузки самых последних признаков вирусов и распространения их по организации. Это позволяет осуществлять ежедневную загрузку признаков вредоносного ПО.

Аутентификация

Аутентификация авторизованных пользователей предотвращает получение неавторизованными пользователями доступа к корпоративным информационным системам. Использование механизмов аутентификации предотвращает доступ авторизованных пользователей к той информации, просмотр которой им запрещен. В настоящее время главным механизмом аутентификации при внутрисистемном доступе являются пароли. При использовании паролей следует руководствоваться приводимыми ниже рекомендациями.

- Длина пароля. Минимальная длина пароля должна составлять не менее 8 символов.
- Частота смены пароля. Возраст паролей не должен превышать 60 дней. Кроме того, пароли не должны изменяться в течение дня после плановой смены пароля.
- История пароля. Не должны использоваться последние десять прежних паролей.
- Содержимое паролей. Пароли не должны состоять только из букв; они должны представлять комбинацию букв, цифр и специальных символов пунктуации. При изменении паролей система должна в принудительном порядке налагать эти ограничения.

Примечание

Точные характеристики паролей корректируются в зависимости от используемой системы. Например, пароли Windows 2000 обладают самой высокой надежностью, если имеют длину в семь или четырнадцать символов. Пароли из восьми символов лишь немного надежнее, чем пароли из семи символов.

Пароли всегда хранятся в зашифрованном виде и недоступны обычным пользователям. Для систем или информации особой секретности пароли

могут не обеспечивать должной защиты. В этих случаях следует использовать динамические пароли или двухфакторную аутентификацию. Имейте в виду, что аутентификация представляет собой комбинацию следующих компонентов.

- То, что известно пользователю, например пароль.
- То, что есть у пользователя, например карта доступа.
- То, что представляет личность пользователя, например отпечаток пальца.

Двухфакторная аутентификация используется для снижения уязвимости каждого типа аутентификационных данных. Например, пароли записываются на бумаге и, следовательно, могут быть раскрыты. Карты доступа можно украсть, а биометрические средства аутентификации дороги и требуют контролируемого или доверенного доступа между пользователем и компьютером.

Все системы организации следует настроить на запуск экранной заставки для удаления информации с экрана и требование повторной аутентификации, если пользователя нет за компьютером больше 10 минут. Если сотрудник оставит компьютер без присмотра, не выходя из сети, то при отсутствии повторной аутентификации злоумышленник сможет использовать этот компьютер под видом работника организации.

Отслеживание

Отслеживание (мониторинг) сетей на предмет наличия подозрительной активности стал необходимым и обязательным действием. Это действие включает как аудит, так и мониторинг сети и системы в реальном времени. Как правило, оно разделяется на аудит и обнаружение вторжений.

Аудит

Аудит - это механизм, записывающий действия, происходящие на компьютере. Журнал содержит информацию о произошедших событиях (вход в систему, выход из системы, доступ к файлам и т. д.), о том, кто выполнил то или иное действие, когда выполнено действие, было ли это действие успешным. Журнал аудита - это материал для исследовательских действий, выполняемых после какого-либо происшествия. Журнал содержит информацию о том, каким образом осуществлено проникновение в компьютерную систему, какая информация считана или изменена. Должна вестись запись следующих событий.

- Вход/выход пользователей.
- Неудачные попытки входа.
- Попытки сетевого подключения.

- Попытки удаленного подключения по телефонной линии.
- Вход супервизора/администратора/основателя.
- Функции, привилегии на выполнение которых имеются у супервизора/администратора/основателя.
- Доступ к секретным файлам.

В идеальном случае эти события записываются в файл, расположенный на защищенной системе - злоумышленник не сможет удалить следы своих действий.

Журналы аудита полезны в том случае, если они регулярно просматриваются. К сожалению, журналы аудита - это одни из наиболее сложных файлов для просмотра вручную. Человеку очень трудно искать в огромном файле журнала несколько записей, которые могут означать некоторое интересуемое событие. Следовательно, в организациях следует использовать автоматизированные средства просмотра журналов аудита. Эти средства представляют собой сценарии, просматривающие файлы журналов на предмет поиска определенных строк текста. Рекомендуется осуществлять еженедельный просмотр журналов аудита.

Совет

Процесс воссоздания часто затрудняется тем, что временные метки в различных журналах не соответствуют друг другу. Чтобы упростить процесс просмотра журнала, рекомендуется синхронизировать часы на всех системах при помощи централизованной системы синхронизации времени, такой как NTP.

Обнаружение вторжений

Системы обнаружения вторжений (IDS) используются для мониторинга сетей или систем и оповещения в реальном времени о событии, представляющем интерес для лиц, обеспечивающих безопасност. Использование узловой системы обнаружения вторжений помогает при проверке журналов аудита, т. к. дает возможность просмотра файлов журналов. Сетевая IDS используется для мониторинга сети на предмет атак или трафика, который отличается от нормального потока данных, обычно наблюдаемого в сети. Системы IDS обоих типов обеспечивают безопасность посредством выдачи предупреждений и оповещений при наличии необычной активности в системе, тем самым снижая время, затрачиваемое на обработку инцидента.

Внимание!

Не следует ограничиваться только лишь применением IDS. Развертываемая IDS должна быть тесно связана с политикой использования компьютеров и

политикой безопасности, а также с процедурами обработки инцидентов, имеющимися в организации.

Шифрование

Секретная информация подвергается опасности при передаче незащищенным способом, например через электронную почту или телефонные линии. Секретная информация подвергается опасности при хранении на незащищенном переносном компьютере. Защиту информации обеспечивает шифрование.

Если уровень секретности информации того требует, информация должна шифроваться при передаче по незащищенным каналам связи или через электронную почту. Используемый алгоритм шифрования должен обеспечивать уровень защищенности, соответствующий степени секретности защищаемой информации. На линиях связи между компьютерами организации должно применяться шифрование канала связи. Если между компьютерами используются VPN-соединения, то VPN должны использовать очень мощное шифрование для всей информации, передаваемой между двумя расположениями.

Если электронная почта используется для передачи секретной информации внутри организации, шифрование сообщений не обязательно. Однако если секретные данные передаются за пределы внутренней сети организации, необходимо шифровать сообщения. Если сообщение передается в другую организацию, следует заранее разработать процедуры, обеспечивающие шифрование сообщения. Некоторые правила (такие как HIPAA) требуют шифрования секретной информации при ее прохождении через открытые сети.

При хранении на переносных компьютерах секретная информация должна находиться в зашифрованном виде. Используемый алгоритм шифрования должен обеспечивать уровень надежности, соответствующий степени секретности защищаемой информации. Система на портативном компьютере должна требовать аутентификацию пользователя перед тем, как он сможет осуществить доступ к информации. В идеальном случае система должна запрещать доступ к информации, если пользователь компьютера недоступен.

При шифровании любых данных следует использовать хорошо известные и проверенные алгоритмы шифрования.

Обновление систем

Поставщики программного обеспечения выпускают обновления для устранения уязвимостей и ошибок в своих программах. Эти обновления очень важны с точки зрения безопасности, так как без них системы будут

находиться в состоянии, уязвимом для атаки и проникновения. Тем не менее, обновления не следует устанавливать без их тестирования.

В каждой организации должна быть тестовая лаборатория, в которой будет проводиться проверка новых обновлений различными приложениями перед установкой на функционирующие системы. Администраторы должны регулярно проверять наличие новых обновлений. Все обновления должны устанавливаться в соответствии с процедурами контроля за изменениями, установленными в организации.

Резервное копирование и восстановление

Как говорилось в разделе "Административная безопасность", резервное копирование и восстановление являются неотъемлемыми процедурами для обеспечения восстановления после сбоя. Чем более "свежими" являются резервные копии, тем легче восстановить все текущие операции. Информация на серверах должна резервироваться ежедневно. Один раз в неделю необходимо осуществлять полное резервное копирование. Резервирование данных в течение последующих шести дней должно дополнять полное резервирование.

Все резервные копии должны периодически проверяться для определения того, успешно ли созданы резервные копии важных файлов. Должны быть установлены регулярные расписания тестирования, чтобы осуществлялось периодическое тестирование всех носителей.

Резервное копирование рабочих станций и портативных компьютеров может вызвать проблемы в любой организации. Одной из них является большой объем данных. Вторая проблема заключается в надобности выполнения резервного копирования между различными сетями. Как правило, резервное копирование рабочей станции и портативных компьютеров производится только в том случае, если информация является слишком секретной, чтобы находиться на файловом сервере. В данном случае резервная система должна находиться в одном местоположении с рассматриваемым компьютером.

Внимание!

Если информация слишком секретна для размещения на файловых серверах, резервные носители требуют особой защиты.

Не менее важно обеспечить правильное хранение резервных копий после их создания. Резервное копирование осуществляется таким образом, чтобы организация смогла восстановить информацию в случае сбоя. Под сбоями подразумеваются такие события, как случайное удаление важного файла пользователем или выход из строя всего сайта. Для восстановления из первой и второй ситуации предъявляются конфликтующие требования к хранению

резервных копий. Для восстановления важных пользовательских файлов резервные копии должны находиться под рукой, чтобы восстановление можно было произвести быстро. Для защиты от сбоев и других непредвиденных обстоятельств резервные копии должны храниться в отключенном от сети состоянии.

Согласно рекомендациям, резервные копии нужно отключать от сети для максимизации уровня защиты информации. Резервные копии следует систематизировать, чтобы их можно было быстро найти и использовать для восстановления определенных файлов. Резервные копии необходимо отключить от сети в течение 24 часов после создания.

Физическая безопасность

Для обеспечения полной защиты необходимо выполнять требования физической безопасности, наряду с обеспечением технической и административной безопасности. Все меры по обеспечению технической безопасности не смогут защитить секретную информацию, если не контролировать физический доступ к серверам. Кроме того, на доступность информационных систем могут повлиять такие факторы, как электроэнергия и климатические условия. Согласно рекомендациям, физическая безопасность обеспечивает защиту информационных систем в следующих областях.

- Физический доступ.
- Климатические условия.
- Защита от пожара.
- Электроэнергия.

Физический доступ

Все секретные компьютерные системы должны быть защищены от несанкционированного доступа. Как правило, это реализуется посредством содержания систем в едином информационном центре. Доступ к информационному центру контролируется различными способами. Доступ с помощью магнитной карты или кодового замка призван ограничить число сотрудников, которые могут входить в информационный центр. Стены информационного центра должны быть капитальными, чтобы исключить доступ через пространство над фальш-потолком.

Климатические условия

Компьютерные системы чувствительны к высоким температурам. Кроме того, компьютеры сами по себе генерируют большое количество тепла. Модули контроля за климатом в информационном центре должны обеспечивать постоянную температуру и влажность, а также обладать

мощностью, соответствующей размерам помещения и количеству теплоты, выделяемому компьютерными системами. Эти модули настраиваются на уведомление администраторов о сбоях либо о выходе температуры за пределы допустимого интервала. Если вокруг кондиционеров в информационном центре конденсируется влага, то из помещения центра необходимо убрать все емкости с водой.

Защита от пожара

В информационных центрах нельзя использовать водяные системы пожаротушения, так как в этом случае компьютерные системы выйдут из строя. Следует использовать системы пожаротушения, активное вещество которых основано не на воде. Система пожаротушения должна быть размещена и настроена таким образом, чтобы огонь в прилегающем пространстве не смог изолировать какую-либо систему информационного центра.

Если применение неводяной системы пожаротушения требует слишком больших затрат, можно использовать "сухую" систему, отключающую электроэнергию в информационном центре перед последующей подачей воды. Посоветуйтесь с пожарным инспектором, чтобы выяснить, можно ли использовать этот вариант.

Во многих инструкциях по борьбе с огнем говорится о том, что во всех помещениях здания должны быть установлены распылительные системы пожаротушения, независимо от наличия других систем. В этом случае неводяные системы подавления огня должны быть настроены на работу перед распылительными системами.

Электроэнергия

Для функционирования компьютерных систем необходима электроэнергия. Часто происходят скачки напряжения и кратковременное отключение электроэнергии. Такие прерывания в электроснабжении могут вывести компьютеры из строя и, следовательно, привести к потере данных. Все важные компьютерные системы должны быть защищены от кратковременных отключений электроэнергии.

Лучше всего с этой задачей справляются резервные источники питания. Эти источники должны обеспечивать электропитание в течение времени, достаточного для выполнения корректного отключения компьютеров. Чтобы защитить системы от более длительных отключений электричества, следует использовать резервные генераторы. В любом случае должны быть настроены оповещения, сообщающие администраторам об отключении электроэнергии.

Совет

Если резервный электрогенератор недоступен, следует приобрести аккумуляторные системы, позволяющие осуществить корректное отключение систем в случае продолжительного отсутствия электропитания. Это предотвратит выход компьютеров из строя при внезапном отключении из-за "севших" аккумуляторов.

Использование стандарта ISO 17799

Существует много различных инструкций, в которых приводятся разного рода рекомендации по той или иной тематике (в данном случае их количество слишком велико для отражения в материале этой книги). Подобные документы опубликованы многими ассоциациями и правительственными агентствами. В 2000 г. Международная организация по стандартизации (ISO) издала международный стандарт для методов безопасности информации. Документ называется "Информационные технологии - методы обеспечения информационной безопасности" - ISO/IEC 17799 (доступен на сайте американского Национального института стандартов http://www.ansi.org/; его стоимость - 112 долларов). Документ напрямую базируется на BS (British Standards Institution) 7799.

Данный документ предназначен для использования в качестве стартовой точки. Несмотря на то, что это очень качественный и полезный документ, каждая организация уникальна и, как правило, требует дополнительных мер контроля или же, наоборот, применения меньшего их количества, нежели указано в стандарте.

Ключевые концепции стандарта

ISO 17799 охватывает десять основных областей.

- Политика безопасности. В данном разделе рассказывается о необходимости политики безопасности и регулярного пересмотра и оценки этого документа.
- Организационная безопасность. В данном разделе описывается, как следует обеспечивать безопасность информации. Содержится информация о работе со сторонними организациями и управлении безопасностью при этих взаимоотношениях.
- Классификация и контроль имущества. В данном разделе обсуждается необходимость правильной защиты как физических, так и информационных ресурсов.
- Безопасность персонала. В данном разделе обсуждается необходимость контроля рисков, связанных с наймом на работу сотрудников, а также обсуждается обучение сотрудников организации. Кроме того, здесь впервые затрагивается тема обработки инцидентов.

- Физическая безопасность и безопасность среды. Все физическое имущество должно быть надежно защищено от хищения, пожара и других воздействий. Данный раздел посвящен именно этой теме.
- Управление коммуникациями и операциями. Рассматривается необходимость в документируемых процедурах управления компьютерами и сетями, а также обсуждается вопрос безопасности информации при ее передаче. Здесь также упоминается необходимость защиты компьютеров от вредоносных программ.
- Контроль доступа. В данном разделе обсуждается контроль доступа к информации, системам, сетям и приложениям, а также говорится об управлении пользователями и о необходимости мониторинга.
- Разработка и поддержка систем. В данном разделе рассматриваются вопросы безопасности, связанные с разработкой проектов. Кроме того, здесь обсуждаются необходимость в шифровании и управлении ключами, а также контроль конфигурации системных файлов.
- Поддержка непрерывности деловых процессов. Здесь рассказывается об опасности прерывания деловых процессов и о различных альтернативных способах поддержки их непрерывности.
- Соответствие политике. В данном разделе говорится о том, каким образом в организации следует соблюдать установленную политику и как должна проводиться проверка на соответствие установленной политике.

Для каждого раздела четко определены цели тех или иных контролирующих действий. Кроме того, во введении приводится полезная информация о том, как достичь защищенного состояния информации внутри организации.

Каким образом использовать этот стандарт

Стандарт ISO 17799 используется как стартовая точка для разработки программ безопасности. При построении программы безопасности необходимо ознакомиться с этим документом и использовать его в качестве руководства при работе в той или иной области. Если уже имеется разработанная программа безопасности, то с помощью стандарта ISO 17799 можно проверить, не упущены ли какие-либо важные вопросы.

Во введении в документ говорится о том, что некоторые меры контроля могут не понадобиться, и что могут потребоваться некоторые дополнительные меры, не включенные в материал стандарта. Точный набор средств, мер и действий по управлению, включаемый в каждую программу безопасности, определяется в процессе оценки угроз.

Внимание!

Не используйте стандарт ISO 17799 или какой-либо другой рекомендательный документ в качестве требований, соответствие которым

должно быть полным и безусловным. Всегда проводите оценку угроз и определяйте действительные требования безопасности для вашей конкретной организации.

Проведение анализа уязвимостей

Этот проект покажет, насколько рассматриваемая организация соответствует авторитетным рекомендациям. Имейте в виду, что это несколько иная задача, нежели оценка угроз. Вы не будете пытаться выявить угрозы, а будете искать вещи, о которых раньше могли и не знать.

Шаг за шагом

1. Начните прорабатывать рекомендации, приводимые в данной лекции или в стандарте ISO 17799, если у вас имеется этот документ.
2. При работе с каждым разделом определите, соответствует ли ваша организация (или последняя проведенная оценка угроз) приводимым рекомендациям.
3. Если рассматриваемая организация не соответствует какой-либо рекомендации, попробуйте понять причину. Возможно, имеются другие меры и средства контроля, или степень угрозы для организации очень мала, вследствие чего неэффективно применять рекомендуемое средство или метод контроля. Кроме того, какая-либо рекомендация могла попросту ранее нигде не приводиться.
4. Для тех рекомендаций, явная причина применения которых в организации отсутствует, разработайте рекомендацию, обеспечивающую соответствующий уровень контроля.

Выводы

Как уже упоминалось выше, этот проект не является повторным проведением оценки угроз, а представляет собой наименее дорогостоящий способ рассмотреть под другим ракурсом имеющуюся программу безопасности. Даже самые опытные сотрудники отдела безопасности могут слишком "зацикливаться" на имеющейся программе, и день ото дня бороться с проблемами, возникающими при поддержке этой программы. Внешний наблюдатель, как правило, может внести "свежую струю" в виде рекомендаций, которые позволят усовершенствовать программу безопасности лишь потому, что не будут скованы ежедневным функционированием этой программы. Точно таким же образом может использоваться и документ с авторитетными рекомендациями.

Контрольные вопросы

1. Что такое "авторитетные рекомендации"?
2. Назовите четыре необходимых политики безопасности.

3. Назовите шесть навыков, которыми должны обладать сотрудники отделов безопасности.
4. Является ли закономерностью, что приобретение средств обеспечения безопасности снизит затраты на работу персонала отдела безопасности?
5. Кто должен нести ответственность за безопасность внутри организации?
6. Какова длительность занятия по изучению вопросов безопасности?
7. Должны ли планы восстановления после сбоев включать резервные "горячие сайты"?
8. Каким образом необходимо обеспечивать защиту постоянных соединений с внешними организациями?
9. На каких системах должны устанавливаться антивирусные программы?
10. Какой длины должны быть пароли?
11. Если информация очень секретна, какой метод аутентификации следует использовать?
12. Где должны храниться записи аудита в идеальном случае?
13. Должны ли программные обновления немедленно устанавливаться на все системы после их выпуска производителем?
14. Перечислите четыре аспекта защиты компьютерных систем, размещенных в информационном центре.
15. Что представляет собой стандарт ISO, в котором говорится об информационной безопасности?