Введение

В школе передо мной стал выбор между двумя направлениями: я хотел заняться информационной безопасностью (ИБ) или разработкой программного обеспечения (ПО). У курсов по разработке ПО были ужасно скучные названия, поэтому я остановился на ИБ. Тогда я еще не знал, на какой сложный и извилистый путь встал.

Работа в сфере ИБ может привести к самым разным результатам. За эти годы я работал с крупномасштабными вспышками вредоносных программ, собирал данные для экспертного анализа для судебных дел, ловил хакеров в компьютерных системах, взламывал системы и приложения (все в порядке, мне разрешили!), изучал огромное количество данных логов, внедрял и поддерживал всевозможные инструменты безопасности, писал тысячи строк кода, совмещал несовместимое, работал над проектами с открытым исходным кодом, выступал на конференциях по безопасности, вел курсы и писал об информационной безопасности.

В этой книге мы поговорим о сфере ИБ в целом. Она адресована тем, кому интересно, что вообще значит «информационная безопасность», а также тем, кто не знает, с чего начать. Я приведу четкие и при этом не усложненные техническими подробностями объяснения того, как работает ИБ и как применять ее принципы в своей работе. Вы узнаете основы, и вам не придется читать толстенные учебники. Сначала я расскажу об основных концепциях — аутентификации и авторизации. Это важно для понимания других понятий — принципа наименьших привилегий и различных моделей безопасности.

Мы рассмотрим несколько реальных применений этих концепций в разных системах, а именно: человеческих, физических, сетевых, операционных системах, мобильных, встроенных системах, интернета вещей (IoT) и в приложениях безопасности. А в конце поговорим о том, как оценивать безопасность.

Для кого эта книга?

Эта книга будет ценным ресурсом для начинающих специалистов в области безопасности, а также для сетевых и системных администраторов. Информация, которую вы здесь найдете, поможет лучше понять, как защитить информационные активы и спастись от атак, а также как повышать безопасность среды.

Руководители тоже наверняка сочтут эту информацию полезной, поскольку она поможет разработать более эффективные методы общей безопасности для организации. Концепции, обсуждаемые в этой книге, могут использоваться для реализации проектов и политик безопасности, а также для решения определенных проблем безопасности.

Структура

Книга знакомит читателя с основами ИБ с нуля, поэтому ее лучше читать от начала до конца. Вам будут встречаться пронумерованные ссылки на примечания в конце книги, где вы можете найти дополнительную информацию по некоторым из этих тем. Вот что вы найдете в каждой главе:

Глава 1. Что такое информационная безопасность? Здесь будут рассмотрены некоторые базовые концепции ИБ, такие как триада конфиденциальности, целостности и доступности (CIA), основные концепции риска, а также средства его снижения.

Глава 2. Идентификация и аутентификация. Охватывает принципы безопасности, связанные с идентификацией и аутентификацией.

Глава 3. Авторизация и контроль доступа. Рассмотрено использование инструментов авторизации и контроля доступа, которые позволяют разграничить, кто или что имеет доступ к тем или иным ресурсам.

Глава 4. Аудит и отчетность. В этой главе рассматривается использование аудита и отчетности, которые позволяют отслеживать деятельность других людей в вашей среде.

Глава 5. Криптография. В этой главе поговорим об использовании криптографии для защиты конфиденциальности ваших данных.

Глава 6. Соответствие, законы и нормативные положения. В этой главе описаны законы и нормативные акты, касающиеся ИБ, и то, как им соответствовать.

Глава 7. Операционная безопасность. В этой главе рассмотрена безопасность операционной деятельности — процесс, необходимый для защиты информации.

Глава 8. Человеческий фактор в безопасности. В этой главе исследуются вопросы, относящиеся к человеческому фактору ИБ, а именно

инструменты и методы, которые используют злоумышленники. Рассматриваются способы защиты от них.

Глава 9. Физическая безопасность. В этой главе рассмотрены физические аспекты ИБ.

Глава 10. Сетевая безопасность. Здесь рассмотрим, как защитить сеть на разных уровнях: правильное проектирование сети, устройства безопасности и инструменты безопасности.

Глава 11. Безопасность операционной системы. В этой главе рассмотрены стратегии, которые можно использовать для защиты ОС: усиление защиты, выпуск обновления и то, как эти стратегии реализуются.

Глава 12. Безопасность мобильных устройств, встроенных устройств и интернета вещей. Мы рассмотрим, как обеспечить безопасность мобильных устройств, встроенных устройств, устройств, подключенных к интернету вещей.

Глава 13. Безопасность приложений. Эта глава охватывает различные методы обеспечения безопасности приложений.

Глава 14. Оценка безопасности. В этой главе обсуждаются такие инструменты, как сканирование и тестирование на проникновение, которые можно использовать для поиска проблем безопасности на хосте или в приложении.

Написание книги стало для меня настоящим приключением. Надеюсь, вам понравится, что в итоге вышло, а ваше понимание сферы ИБ расширится. Мир безопасности — это захватывающая, а иногда и просто поразительная область. Добро пожаловать и удачи!

От издательства

Ваши замечания, предложения, вопросы отправляйте по адресу comp@piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На веб-сайте издательства www.piter.com вы найдете подробную информацию о наших книгах.

1

Что такое информационная безопасность?

Сегодня многие люди работают на компьютере, играют в компьютерные игры, учатся онлайн, покупают вещи в интернет-магазинах, сидят с ноутбуками в кофейнях, проверяя почту, заглядывают на свои банковские счета со смартфона или следят за калориями с помощью фитнес-браслетов. Другими словами, компьютеры повсюду.

Технологии по одному щелчку мыши дают нам доступ к огромному объему информации, но эти же технологии представляют собой серьезную угрозу безопасности. Если информация о системах безопасности, используемых работодателями или банками, попадет в руки злоумышленников, последствия могут быть катастрофическими. Например, все деньги с банковского счета могут среди ночи внезапно улететь в другой банк в другой стране. Работодатель может потерять миллионы долларов, оказаться на скамье подсудимых и лишиться репутации из-за проблемы с конфигурацией системы, которая позволила злоумышленнику получить доступ к базе данных с личными данными (ЛД) или конфиденциальной информацией. И такие случаи пугающе часто мелькают в средствах массовой информации.

Тридцать лет назад подобных ситуаций в принципе не было, в основном потому, что технологии тогда находились на относительно низком уровне и мало кто ими пользовался. Сегодня технологии стремительно меняются, а вот большая часть теории защиты информации отстает от этого развития. Но после получения хорошего представления об основах ИБ у вас будет твердый фундамент для борьбы с будущими новыми методами злоумышленников.

В этой главе мы рассмотрим некоторые базовые концепции ИБ: модели безопасности, атаки, угрозы, уязвимости и риски. Также подробнее углубимся в некоторые более сложные концепции при обсуждении риска: управление рисками, реагирование на инциденты и глубокая защита.

Определение информационной безопасности

В целом под термином *«безопасность»* следует понимать защиту ваших активов, будь то от злоумышленников, вторгающихся в ваши сети, от стихийных бедствий, вандализма, утраты или неправильного использования. Наша цель — обезопасить себя от наиболее вероятных форм атак, насколько позволяет используемая среда.

У вас может быть множество потенциальных активов, которые надо будет защитить. Например, физические предметы, ценные сами по себе (золото), или предметы, имеющие ценность для вашего бизнеса (вычислительное оборудование). У вас также могут быть нефизические ценности — программное обеспечение, исходный код или данные.

В сегодняшней вычислительной среде вы, вероятно, обнаружите, что ваши логические активы (данные или интеллектуальная собственность) столь же ценны, как физические активы (то есть вещи), а может, даже еще ценнее. И здесь возникает важность информационной безопасности.

Согласно определению законодательства США[1], *информационная безопасность* — это «защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения»*,**. Другими словами, мы хотим защитить свои данные и системы от тех, кто пытается неправомерно их использовать, намеренно или непреднамеренно, и от тех, кто вообще не должен иметь к ним доступ.

Когда можно считать себя в безопасности?

Юджин Спаффорд однажды сказал: «Единственная по-настоящему безопасная система — это та, которую отключили от питания, залили в бетон и закрыли в обшитой свинцом комнате с вооруженной охраной. Хотя даже в этом случае

---

* Согласно ГОСТ Р 50922–2006 «Защита информации», защита информации — это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. — *Примеч. ред.*

** Здесь и далее — ссылки на источники см. в разделе «Список источников». — *Примеч. ред.*

у меня есть сомнения»[2]. Система в таком состоянии, возможно, безопасна, но становится непригодной для использования. Повышая уровень безопасности, мы обычно снижаем уровень производительности.

Кроме того, при защите актива, системы или среды нужно думать о том, как уровень безопасности соотносится с ценностью охраняемого объекта. Если вы готовы приспособиться к снижению производительности, то можете применить очень высокий уровень безопасности к каждому активу, который находится в вашем ведении. Можно построить объект стоимостью в миллиард долларов, окруженный забором из колючей проволоки, патрулируемый вооруженной охраной и злобными бойцовыми собаками, в центре которого будет герметичный сейф, а в нем... рецепт шоколадного печенья вашей мамы. Согласитесь, это перебор. Стоимость системы безопасности, которую вы устанавливаете, никогда не должна превышать стоимости того, что она защищает.

Но в некоторых средах даже таких мер безопасности оказывается мало. В любой среде, где планируется обеспечить повышенный уровень безопасности, необходимо также учитывать стоимость замены ваших активов на случай их потери и убедиться, что уровень защиты соотносится с их стоимостью.

Довольно сложно определить момент, когда можно считать, что безопасность обеспечена. В безопасности ли вы, когда ваши системы правильно пропатчены? В безопасности ли вы, если используете надежные пароли? В безопасности ли вы, если полностью отключены от интернета? Думаю, что на все эти вопросы нет ответа. Панацеи не существует.

Даже если ваши системы в данный момент защищены, всегда найдутся новые атаки, к которым система окажется уязвима. Когда вы используете надежные пароли, злоумышленник воспользуется другим способом. Когда вы отключены от интернета, злоумышленник может получить физический доступ к вашим системам или украсть их. Короче говоря, сложно определить, действительно ли вы в безопасности. А вот определить обратное гораздо проще.

Ниже приведено несколько примеров небезопасных состояний:

- отсутствие исправлений безопасности или обновления приложений в ваших системах;
- использование ненадежных паролей, таких как «qwerty» или «1234»;
- скачивание программ из Сети;
- открытие вложений к электронным письмам от неизвестных отправителей;
- использование беспроводных сетей без шифрования.

Список можно дополнять долго. Важно то, что, если вы знаете, где ваша система небезопасна, вы можете предпринять меры смягчения этой проблемы. Это как бесконечно разрезать что-либо пополам — всегда останется небольшой кусочек, который снова нужно разрезать. Возможно, вы никогда не дойдете до состояния, которое окончательно можно назвать безопасным, но можете предпринимать меры в правильном направлении.

ЭТОТ ЗАКОН — ВАШ ЗАКОН...

Законы, определяющие стандарты безопасности, в разных отраслях и разных странах довольно сильно различаются. В качестве примера можно привести различие в законах о конфиденциальности данных США и Европейского союза. Организации, работающие по всему миру, вынуждены отслеживать, чтобы при ведении бизнеса не нарушать такие законы. В случае сомнений следует сначала проконсультироваться с юристом, а потом действовать.

Некоторые законы или нормативные акты прямо определяют, какие средства защиты или меры следует предпринимать, чтобы считать систему достаточно защищенной. Стандарт безопасности данных индустрии платежных карт (PCI DSS) применяется к компаниям, которые обрабатывают платежи по кредитным картам, Закон 1996 года о переносимости и подотчетности медицинского страхования (HIPAA) предназначен для организаций, которые обрабатывают медицинские карты и истории болезни пациентов, Федеральный закон об управлении информационной безопасностью (FISMA) определяет стандарты безопасности для многих федеральных агентств в США, и таких законов множество. Их эффективность — вопрос открытый, но соблюдение стандартов безопасности, определенных для отрасли, в которой вы работаете, рекомендуется, а может, даже требуется.

Модели для обсуждения вопросов безопасности

При обсуждении вопросов безопасности часто бывает полезно иметь модель, которую можно взять за основу. В этом случае у вас будет последовательный набор терминов и концепций, на которые мы как профессионалы в области безопасности можем ссылаться.

Триада конфиденциальности, целостности и доступности

Три слона информационной безопасности — это конфиденциальность, целостность и доступность, которые называются триадой CIA (Confidentiality, Integrity, Availability) (рис. 1.1).

Рис. 1.1. Триада CIA

Триада CIA — это модель, с помощью которой можно решать и обсуждать концепции безопасности. Иногда она записывается как CAI или выражается в виде противоположных понятий: раскрытие, изменение и отрицание (DAD — Disclosure, Alteration, Denial).

Конфиденциальность

Конфиденциальность — это способность защитить данные от тех, кто не имеет прав доступа к ним. Можно обеспечить конфиденциальность на разных уровнях процесса.

Например, представьте, что человек снимает деньги в банкомате. Скорее всего, он захочет сохранить в тайне ПИН-код, который позволяет ему снимать средства. Кроме того, владелец банкомата будет сохранять конфиденциальность номера счета, баланса счета и любой другой информации, которая передается банку, из которого выводятся средства. Банк также будет сохранять конфиденциальность транзакции с банкоматом и изменения баланса на счете после снятия средств.

Конфиденциальность может быть нарушена несколькими способами. Например, вы можете потерять ноутбук с данными. Когда вы вводите пароль, другой человек сможет его подсмотреть. Вы можете отправить файл по электронной почте не тому человеку, или в вашу систему может проникнуть злоумышленник.

Целостность

Целостность — это способность предотвратить несанкционированное или нежелательное изменение ваших данных другими лицами. Чтобы сохранить

целостность, нужны не только средства предотвращения несанкционированных изменений ваших данных, но и возможность откатить такие изменения.

Хороший пример механизма, позволяющего контролировать целостность, реализован в файловых системах многих современных операционных систем, таких как Windows и Linux. В целях предотвращения несанкционированных изменений в этих системах введены разрешения, ограничивающие действия, которые неавторизованный пользователь может выполнять с данным файлом. Например, владелец файла может иметь разрешение на чтение и запись в него, а другие могут иметь только разрешение на чтение или вообще не иметь доступа к файлу. Кроме того, некоторые системы и многие приложения, такие как базы данных, позволяют отменить или откатить нежелательные изменения.

Целостность особенно важна, когда речь идет о данных, которые служат основой для принятия других решений. Если злоумышленник изменит данные результатов медицинских тестов, врач может назначить неправильное лечение, которое навредит пациенту.

Доступность

Последний слон триады CIA — доступность. *Доступность* — это возможность доступа к нашим данным, когда они нам нужны. Вы можете потерять доступность из-за потери питания, проблем с ОС или приложением, сетевых атак или компрометации системы. Когда внешняя сторона, например злоумышленник, вызывает такие проблемы, мы обычно называем это *DoS-атакой* (denial-of-service, DoS — отказ обслуживания).

Как триада CIA связана с безопасностью?

Зная элементы триады CIA, мы можем начать обсуждение вопросов безопасности более подробно, чем без них. Рассмотрим поставку резервных лент, на которых вы сохранили единственную существующую и незашифрованную копию некоторых конфиденциальных данных.

Если вы потеряете груз в пути, у вас возникнут проблемы с безопасностью. Вероятно, это связано с нарушением конфиденциальности, поскольку файлы не были зашифрованы. Отсутствие шифрования также может вызвать проблемы с целостностью. Если вы восстановите ленты в будущем, вам может быть не сразу очевидно, изменил ли злоумышленник незашифрованные файлы, поскольку у вас не будет способа отличить измененные данные от неизмененных. Что касается доступности, у вас возникнет проблема, если ленты не будут восстановлены, поскольку у вас нет резервных копий файлов.