Оглавление

Предисловие

Программы правят миром. Разработчики стали новыми «делателями королей». Благодаря интернету вещей компьютер скоро появится в каждой лампочке.

Все это означает, что скоро программы настолько глубоко проникнут в нашу жизнь, что для большинства людей до ближайшего компьютера будет буквально рукой подать, и постоянное взаимодействие с предметами и окружением, управляемыми компьютерами, войдет у нас в привычку.

Но в таком мире нас подстерегают опасности. В старом добром мире безопасность всерьез рассматривалась только в банковских и правительственных системах. Однако повсеместное распространение компьютеров повышает потенциальную выгоду от их неправомерного использования, что, в свою очередь, создает стимулы для такого использования и, стало быть, повышает риски, с которыми сталкиваются системы.

В большинстве организаций стремительно принимают на вооружение гибкие (agile) методики разработки. Они позволяют своевременно реагировать на изменение условий и значительно снижать стоимость разработки, поэтому задают стандарт, который, как мы ожидаем, будет распространяться все шире, и в конечном итоге большая часть программ будет создаваться с помощью гибких методик.

Однако исторически безопасность и гибкие методики никогда не дружили между собой.

Специалисты по безопасности по горло заняты уже упомянутыми системами для государственных учреждений, банков и электронной коммерции – их архитектурой, тестированием и защитой, – и все это перед лицом непрерывно совершенствующихся угроз. То, что часто представляют самым интересным и захватывающим в области безопасности, то, о чем пишут в технических блогах и говорят в ночных новостях, делается командами профессиональных хакеров, специализирующихся на исследовании уязвимостей, разработке эксплойтов и ошеломительных взломах.

Наверняка вы сможете назвать несколько уязвимостей, бывших на слуху в последнее время: Heartbleed, Logjam или Shellshock (или еще каких-нибудь, с которыми на приведи бог столкнуться), или припомнить названия команд, которым удалось «разлочить» последние модели

устройств на основе iPhone и Android. Но когда в последний раз вы слыхали о новом средстве или методике защиты – с запоминающимся, интересным для СМИ названием? А знаете ли вы имя создателя этой методики?

Профессионалы в области безопасности отстают в понимании и опыте применения гибких методик, и этот разрыв несет серьезные риски для нашей отрасли.

С другой стороны, гибкие команды отбросили стесняющие оковы прошлого. Нет больше детальных технических требований, нет системного моделирования, не стало каскадной модели (модели «водопада») с ее традиционными этапами и контролем их выполнения. Беда в том, что гибкие команды вместе с водой выплеснули и ребенка. Старые методики, пусть даже иногда медленные и негибкие, доказали свою ценность. Они создавались не без причины, а отказавшись от них, гибкие команды рискуют забыть, в чем состояла эта ценность, и выбросить все достижения на свалку.

Поэтому гибкие команды редко относятся к безопасности, как должно. Некоторые гибкие практики позволяют получить чуть более безопасные системы, но зачастую это благоприятный побочный эффект, а не цель. И лишь очень немногие гибкие команды понимают угрозы, с которыми может столкнуться система, а большинство не понимает рисков, не отслеживает их и не делает ничего, чтобы управлять ими. Они даже слабо представляют, кто вообще атакует плоды их труда.

Кому стоит прочитать эту книгу?

Мы не знаем, кто вы: руководитель гибкой команды или разработчик, желающий больше узнать о безопасности. Быть может, вы – «безопасник», который только что узнал о существовании доселе неведомой ему группы разработчиков и хотел бы разобраться, чем она занята.

При написании этой книги мы имели в виду три потенциальные группы читателей.

Разработчики, применяющие гибкие методы

Вы жизни не мыслите без гибкой разработки. Scrum и кайдзен – для вас не пустые слова, разработка через тестирование вошла в плоть и кровь. Не важно, какую конкретную роль вы играете – Scrum-мастер, разработчик, тестировщик, тренер, владелец продукта или представитель заказчика, – вы владеете гибкими практиками и понимаете, в чем их ценность.

Эта книга поможет вам разобраться в том, что такое безопасность, какие существуют угрозы и на каком языке специалисты-безопасники описывают, что происходит. Мы научим вас моделировать угрозы, измерять степень риска, создавать ПО, помня о безопасности, безопасно устанавливать ПО и оценивать, какие проблемы (в плане безопасности) могут возникать в процессе его эксплуатации.

Специалист по безопасности

Если вы риск-менеджер, специалист по обеспечению целостности и безопасности информации (information assurance) или по анализу операционной безопасности, то что такое безопасность, вы понимаете. Наверное, вы с осторожностью подходите к использованию онлайновых служб, постоянно думаете об угрозах, рисках и формах их проявления, возможно, даже сами находили новые уязвимости и разрабатывали эксплойты для них.

Эта книга поможет вам понять, как работают гибкие команды и что, наконец, такое спринты и истории, о которых они все время толкуют. Вы научитесь видеть порядок в хаосе, и это поможет взаимодействовать с командой и влиять на нее. Эта книга покажет, где следует вмешаться или внести свой вклад, чтобы он оказался наиболее ценным для команды и дал наилучший эффект.

Специалист по гибким методикам обеспечения безопасности

Вы знаете все – от рисков до спринтов. Будь вы разработчиком инструментальных средств, который хочет помочь команде правильно подойти к безопасности, или консультантом, оказывающим команде платные услуги, эта книга и для вас тоже. Главное в ней – уяснить то, что авторы называют возрастанием доли правильной практики. Эта книга поможет вам узнать, кто работает с вами по соседству, а также составить представление об идеях, размышлениях и концепциях, которые, как мы видим, прорастают в организациях, работающих над этой проблематикой. Мы дадим широкий обзор предмета, чтобы вы смогли решить, чем заняться или что изучить дальше.

О структуре книги

Книгу можно читать от корки до корки, по одной главе за раз. Собственно, так мы и рекомендуем поступить; мы приложили немало трудов и

надеемся, что в каждой главе любой читатель найдет что-то полезное для себя, пусть даже это будут просто наши незатейливые шутки и забавные рассказы!

Но, честно говоря, мы полагаем, что некоторые главы окажутся для вас полезнее, чем другие.

Книга разбита на три большие части.

Часть 1. Основы

Гибкая разработка и безопасность – очень широкие дисциплины, и мы не знаем, что вам уже известно. А если вы специализируетесь в одной области, то вполне возможно, что знаний и опыта из другой вам недостает.

Если вы специалист по гибкой разработке, то рекомендуем сначала прочитать *главу 1 «Начала безопасности»*, из которой вы получите базовые сведения о безопасности.

Если раньше вы вообще не занимались гибкой разработкой или делаете первые шаги на этом пути, то, прежде чем переходить к введению в эту тему, рекомендуем прочитать *главу 2 «Элементы гибких методик»*.

В *главе 3 «Революция в методах разработки – присоединяйтесь!»* описывается история гибкой разработки программного обеспечения и различные подходы к ней. Эта глава будет особенно интересна специалистам по безопасности и людям, еще не имеющим практического опыта.

Часть 2. Гибкая разработка и безопасность

Затем мы рекомендуем всем без исключения прочитать *главу 4 «Работа с существующим гибким жизненным циклом»*.

В этой главе производится попытка соединить рассматриваемую нами практическую безопасность с реальным жизненным циклом гибкой разработки и объяснить, как они сочетаются.

В *главах 5–7* разбирается управление требованиями и уязвимостью, а также управление рисками. Это общие принципы, лежащие в основе управления продуктом и планирования разработки.

В *главах 8–13* рассматриваются различные аспекты жизненного цикла разработки безопасного программного обеспечения: оценка угроз, инспекция кода, тестирование и операционная безопасность.

Часть 3. Собираем все вместе

В *главе 14* рассматривается соответствие нормативным требованиям и их учет в средах гибкой разработки и DevOps.

Глава 15 посвящена культурным аспектам безопасности. Да, вы могли бы реализовать все описанные в книге практики, и в предшествующих главах описаны разнообразные средства, позволяющие затвердить новые подходы. Но гибкие методики – это в первую очередь о людях, и то же самое верно в отношении эффективных путей обеспечения безопасности: безопасность – это внутренне осознанное изменение культуры поведения, и в этой главе вы приведем примеры приемов, которые оказались эффективны на практике.

Чтобы изменить отношение компании к безопасности, необходимы взаимная поддержка и уважение безопасников и разработчиков. Чтобы создать безопасный продукт, требуется их тесное взаимодействие. Этого невозможно добиться только путем внедрения набора средств и практик, изменения должны пронизывать всю организацию.

Наконец, в *главе 16* рассматривается вопрос о том, что разные люди понимают под «гибкой безопасностью», и подводится итог опыту авторов: что у них получалось и что не получалось при попытке создать команды, сочетающие одновременно гибкость и безопасность.

Графические выделения

В книге применяются следующие графические выделения:

Курсив

Новые термины, URL-адреса, адреса электронной почты, имена и расширения имен файлов.

`Моноширинный шрифт`

Листинги программ, а также элементы кода в основном тексте: имена переменных и функций, базы данных, типы данных, переменные окружения, предложения и ключевые слова языка. Знак ↪ в конце строки кода означает, что код продолжается на следующей строке.

`Моноширинный полужирный шрифт`

Команды и другой текст, который пользователь должен вводить буквально.

`Моноширинный курсив`

Текст, вместо которого следует подставить значения, заданные пользователем или определяемые контекстом.

Так обозначается совет или рекомендация.

Так обозначается примечание общего характера.

Так обозначается предупреждение или предостережение.

Как с нами связаться

Вопросы и замечания по поводу этой книги отправляйте в издательство:

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472
800-998-9938 (в США и Канаде)
707-829-0515 (международный или местный)
707-829-0104 (факс)

Для этой книги создана веб-страница, на которой публикуются сведения о замеченных опечатках, примеры и разного рода дополнительная информация. Адрес страницы *http://bit.ly/agile-application-security*.

Замечания и вопросы технического характера следует отправлять по адресу *bookquestions@oreilly.com*.

Дополнительную информацию о наших книгах, конференциях и новостях вы можете найти на нашем сайте по адресу *http://www.oreilly.com*.

Читайте нас на Facebook: *http://facebook.com/oreilly*.

Следите за нашей лентой в Twitter: *http://twitter.com/oreillymedia*.

Смотрите нас на YouTube: *http://www.youtube.com/oreillymedia*.

Благодарности

Прежде всего мы благодарны нашим замечательным редакторам: Кортни Аллен, Вирджинии Уилсон и Нэн Барбер. Мы не смогли бы довести это дело до конца без вас и всего коллектива издательства O'Reilly.

Мы также выражаем признательность техническим рецензентам за их терпение и полезные советы: Бену Аллену (Ben Allen), Джеффу Кратцу (Geoff Kratz), Питу Макбрину (Pete McBreen), Келли Шортридж (Kelly Shortridge) и Ненаду Стояновски (Nenad Stojanovski).

И наконец, спасибо нашим друзьям и семьям, выдержавшим *еще один* безумный проект.

Глава 1

Начала безопасности

Итак, что же такое безопасность?

Обманчиво простой вопрос, на который куда как сложно ответить.

Начиная путешествие в мир безопасности, трудно не то что разобраться, но хотя бы понять, куда смотреть первым делом. В новостях об успешных *взломах* рисуют картину злоумышленника типа Нео, который располагает чуть ли не безграничным арсеналом для проведения сложнейших атак. При такой точке зрения обеспечение безопасности может показаться безнадежным делом, выходящим за рамки человеческих возможностей.

Да, действительно, безопасность – сложная, постоянно изменяющаяся дисциплина, но верно и то, что существует ряд довольно простых базовых принципов, поняв которые, будет куда легче систематизировать знания, приобретенные впоследствии. Рассматривайте обеспечение безопасности как движение вперед, а не как конечную цель – движение, начинающееся с небольшого числа фундаментальных понятий, отталкиваясь от которых, можно постепенно строить все здание.

Поэтому важно, чтобы все мы, независимо от прежнего опыта, первым делом уяснили некоторые основополагающие принципы. Мы также рассмотрим традиционные подходы к безопасности и объясним, почему они перестали быть эффективными теперь, когда гибкие методы разработки стали вездесущими.

С точки зрения команд разработчиков, под безопасностью понимается информационная безопасность (а не физическая безопасность, воплощенная в дверях и стенах, а также в организации охраны, например процедурах досмотра персонала). Информационная безопасность включает практические приемы и процедуры в начале работы над проектом, в процессе реализации системы и в ходе ее эксплуатации.

Хотя в этой книге мы будем говорить главным образом *об информационной безопасности*, для краткости будем употреблять просто слово *безопасность*. Если понадобится упомянуть о каком-то другом аспекте безопасности, например физическом, то это будет оговорено явно.

Инженеры часто обсуждают, какую технологию выбрать для систем и сред. Но вопросы безопасности вынуждают нас выходить за рамки технологий. Быть может, безопасность лучше всего представлять как область на пересечении технологии с людьми, которые эту технологию используют для повседневных надобностей (см. рис. 1.1).

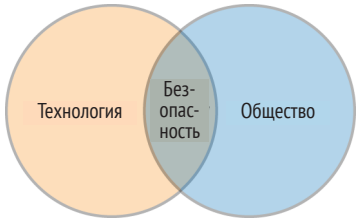

Рис. 1.1. Чем меньше общество зависит от технологии, тем меньше потребность в безопасности

Что можно сказать, глядя на эту картинку? Она показывает, что безопасность – нечто большее, чем просто технология, и, по самому своему определению, *должна* включать людей.

Людям не нужна технология, чтобы совершать дурные поступки и обманывать друг друга; этим они занимались задолго до того, как в нашу жизнь вошли компьютеры, для этого даже слово есть – *преступление*. Тысячи лет люди совершенствовались в искусстве лгать, обманывать и красть на пользу себе и своему сообществу. Но когда человек начинает взаимодействовать с технологией, это превращается в многообещающую комбинацию мотивов, целей и возможностей. В таких случаях некоторые мотивированные группы людей проводят согласованные действия в обход технологических ограничений во имя достижения конечной цели – вполне в духе человеческой природы. Именно такую деятельность и призвана предотвратить безопасность.

Следует, однако, отметить, что технический прогресс создал условия для расширения братства людей, способных на такие преступления: как благодаря доступности инструкций, так и вследствие появления всемирных сервисов, к которым может попытаться получить доступ мотивированный преступник. При наличии Интернета, мировых си-

стем связи и других достижений прогресса атаковать вас намного проще, чем раньше, притом что для преступника риск попасться гораздо ниже. Интернет и сопутствующие ему технологии сделали мир совсем маленьким, а асимметрия при этом стала даже более разительной – затраты снизились, прибыль возросла, а шансы быть пойманными резко уменьшились. В этом новом мире географическое расстояние до вожделенной богатой добычи для атакующего свелось к нулю, но действует прежняя юридическая система, основанная на межгосударственных соглашениях и процедурах межъюрисдикционных расследований и экстрадиций. И это мы еще не говорим о различиях принятых в разных странах определений существа компьютерного преступления. Технологии и Интернет также помогают взломщику избежать идентификации: вам больше не нужно явиться в банк, чтобы ограбить его, – вы можете находиться на другом конце света.

Замечание по поводу терминологии
При обсуждении небезопасности мы сознательно употребляем фразу «*в обход*», чтобы избежать неявных моральных суждений.

Чем больше в нашей жизни технологий, тем больше у нас возможностей использовать их во благо. Но у этой медали есть и оборотная сторона: чем выше зависимость общества от технологий, тем больше возможностей и стимулов использовать их во зло и тем выше доход от этого. Чем сильнее мы зависим от технологии, тем больше потребность в том, чтобы она была стабильна, защищена и всегда доступна. Если стабильность и безопасность оказываются под вопросом, страдает и бизнес, и общество. Тот же рисунок, что и выше, иллюстрирует взаимозависимость между уровнем распространения технологий в обществе и необходимостью обеспечить безопасность во имя достижения стабильности и защищенности (рис. 1.2).

Рис. 1.2. Чем сильнее зависимость от технологии, тем выше потребность в безопасности и серьезнее последствия ее отсутствия

По мере проникновения технологии в ткань общества все большую важность приобретают подходы к осмыслению ее безопасности.

Фундаментальный недостаток классических подходов к информационной безопасности – непонимание того, что люди не менее важны, чем технология. В этой книге мы хотим предложить свежий взгляд именно на эту проблему.

Не только для технарей

Было время, когда безопасность беспокоила только государство да двинутых технарей. Но теперь, когда Интернет прочно вошел в жизнь людей по всему миру, обеспечение безопасности лежащих в его основе технологий тревожит часть общества, куда большую, чем когда-либо прежде.

Если вы пользуетесь технологиями, то безопасность имеет для вас значение, потому что любой изъян в ней может нанести прямой ущерб как вам, так и вашему окружению.

Если вы создаете технологию, то должны стремиться сделать ее стабильной и безопасной, чтобы с ее помощью мы могли улучшить бизнес и общество. Безопасность уже не является вопросом, который можно оставить где-то на периферии сознания.

- Вы несете ответственность за безопасность технологии.
- Вы заботитесь о том, чтобы люди прониклись идеей безопасности в повседневной жизни.

Если вы не берете на себя такую ответственность, значит, создаваемая вами технология фундаментально ущербна и не выполняет одну из своих главных функций.

Безопасность и риск неразделимы

Безопасность, а точнее безопасность программного обеспечения, призвана минимизировать риск. Смысл ее в том, что мы пытаемся уменьшить вероятность того, что людей, системы и данные можно будет использовать таким способом, который причинит финансовый или материальный ущерб или нанесет урон репутации организации.

Уязвимость: вероятность и последствия

Большинство методов обеспечения безопасности направлено на предотвращение атак на наши системы и информацию. Но расчет риска – это не попытка предотвратить событие, а стремление понять, что и как

может случиться, с целью расположить меры по улучшению в порядке приоритетности.

Чтобы рассчитать риск, нужно знать, что может случиться с организацией и системой, насколько вероятны такие события и какова их цена.

Это позволит определиться с тем, сколько денег и усилий потратить на защиту от потенциального ущерба.

Все мы уязвимы

Уязвимость – это подверженность риску. Вне контекста безопасности мы понимаем под уязвимостью возможность понести физический или эмоциональный ущерб. Говоря о системах и безопасности, мы употребляем это слово для описания изъянов в системе, ее компонентах или процессах, которые открывают возможность нанести вред данным, системам или людям путем злонамеренного использования или раскрытия информации.

Вероятно, вам доводилось слышать фразы типа «в такой-то программе была обнаружена новая уязвимость» или «хакеры воспользовались уязвимостью в ...». Здесь под уязвимостью понимается изъян в конструкции, конфигурации или прикладной логике программы, который позволил атакующему сделать нечто такое, что не было предусмотрено или на что он не имел права. Эксплуатация уязвимости – это акт ее использования, т. е. способ, позволяющий воспользоваться ошибкой в программе на благо атакующему.

Не невозможно, просто маловероятно

Вероятность, или *шанс* – это способ измерить, насколько легко мотивированный атакующий сможет эксплуатировать уязвимость.

Вероятность – весьма субъективный критерий, при ее оценке нужно учитывать множество факторов. При простом расчете риска ее можно свести к одному числу, но для ясности перечислим некоторые вещи, которые следует принимать во внимание при оценке вероятности.

Технические знания, необходимые для эксплуатации уязвимости

Необходимо ли быть квалифицированным техническим специалистом или достаточно случайных поверхностных знаний?

Надежность

Работает ли эксплойт надежно? Подвержены ли уязвимости различные версии, платформы и архитектуры? Чем надежнее эксплойт, тем меньше шансов, что атака вызовет заметный по-

бочный эффект, а это делает эксплойт *более безопасным* с точки зрения атакующего, т. к. снижает риск обнаружения.

Автоматизация

В какой мере эксплуатация уязвимости поддается автоматизации? Это свойство дает возможность включить эксплойт в состав комплекта эксплойтов или в самораспространяющийся код (червь), что повышает вероятность оказаться мишенью неизбирательной атаки.

Доступ

Нужно ли располагать возможностью непосредственного взаимодействия с определенной системой (сетью) или иметь определенный набор прав пользователя? Необходимо ли для успешной эксплуатации уязвимости, чтобы одна или несколько частей системы уже были скомпрометированы?

Мотивация

Является ли конечный результат эксплуатации уязвимости настолько значимым, чтобы у противника был мотив потратить свое время?

Измерение затрат

Последствия – это эффект, который эксплуатация уязвимости, недопустимое использование системы или ее взлом может оказать на вас, ваших клиентов и вашу организацию.

Для большинства коммерческих предприятий последствия измеряются в сумме утраченных денежных средств. Это может быть как прямая кража денег (например, в результате кражи кредитной карты или мошенничества), так и стоимость восстановления после взлома. Стоимость восстановления часто включает не только устранение уязвимости, но и:

- реакцию на сам инцидент;
- восстановление других систем или данных, которые были повреждены или уничтожены;
- внедрение новых подходов к повышению безопасности системы, чтобы предотвратить новые попытки взлома;
- увеличение затрат на аудит, страхование и соответствие нормативным требованиям;
- затраты на маркетинг и пиар;
- увеличение операционных издержек или применение повышенных тарифов поставщиками.

Куда серьезнее последствия для тех, кто создает системы управления или приложения, оказывающие непосредственное влияние на жизни людей. В таких случаях оценка последствий уязвимости может включать учет гибели и травм отдельных лиц или групп лиц.

В мире, который быстро движется в направлении автоматизации вождения и многих физических ролей в обществе, где компьютеризованы медицинские устройства и чуть ли не все бытовые приборы в наших домах, защита от уязвимостей все чаще подразумевает защиту людей, а не только денег и репутации.

Риск можно свести к минимуму, но не устранить вовсе

Мы склонны считать, что любое несовершенство системы можно устранить. Ошибки можно исправить, а с неэффективностью справиться благодаря более изобретательной конструкции. И действительно, большинство предметов, которые мы сами создаем и контролируем, можно довести до совершенства.

Но с риском дело обстоит иначе.

Риск связан с внешними воздействиями на системы, организации и людей. Эти воздействия чаще всего нами не контролируются (экономисты говорят о внешних факторах, или *экстерналиях*). Это могут быть отдельные лица или группы лиц с собственной мотивацией и планами, производители и поставщики со своими подходами и ограничениями или факторы окружающей среды.

Поскольку мы не контролируем риск и его причины, то никогда не сможем полностью избежать его. Бессмысленно и бесплодно стремиться к этому. Вместо этого нужно сосредоточиться на понимании рисков, на минимизации рисков (и их последствий) там, где это возможно, и постоянном мониторинге нашей предметной области на предмет появления новых и видоизменения старых рисков.

В том, чтобы принять риск, тоже нет ничего страшного, при условии что это делается осознанно, с пониманием природы риска. А вот слепо мириться с риском – путь к катастрофе, нужно постоянно быть начеку, чтобы не пропустить такую опасность, а сделать это ой как легко.

Несовершенный мир – трудные решения

Хотя наша цель – минимизировать и смягчить риски, необходимо также помнить, что мы живем в мире, где есть ограничения, а ресурсы конечны. Нравится нам это или нет, но в сутках только 24 часа, и в течение этого времени нужно еще где-то поспать. У любой организа-

ции есть бюджет и ограниченное количество людей и ресурсов, которые можно выделить для решения проблем.

Поэтому лишь очень немногие организации могут позволить себе учет всех рисков, с которыми сталкиваются. А большинство способно лишь сгладить или устранить малую часть рисков. Истратив свои ресурсы, мы можем только составить список оставшихся рисков и делать все, что в наших силах, для мониторинга ситуации и уяснения того, какими последствиями грозит оставление рисков без внимания.

Чем меньше организация, тем острее эта проблема. Но напомним, что даже самая маленькая группа с крохотным бюджетом кое-что может сделать. Малая численность и нехватка ресурсов – это не оправдание ничегонеделания, а возможность сделать максимум, чтобы обезопасить системы, творчески распорядившись имеющимися технологиями и навыками.

Решить, каким рискам уделить внимание, трудно, это отнюдь не точная наука. В этой книге мы познакомим вас с инструментами и идеями, которые позволят точнее понять и измерить риски и наилучшим образом распорядиться тем временем и ресурсами, которые имеются в наличии.

Знай своего врага

Так от кого же мы защищаемся?

Конечно, всем нам хотелось бы верить, что нас и наши приложения атакует этакий мелкий суперзлодей из комиксов, но лучше бы смотреть правде в лицо.

Существует целый ряд отдельных лиц и групп, которые могли бы или захотели бы попытаться эксплуатировать уязвимости в ваших приложениях или процессах. У каждого из них своя история, мотивы и ресурсы, а мы должны знать, как все это может сойтись, и подвергнуть нашу организацию риску.

Враг найдется у каждого

Еще недавно мы употребляли слово *кибер* для описания любого противника, который приближается к нашим владениям по внутренним сетям или через Интернет. Это породило веру в то, что есть только один вид атакующего и что это, скорее всего, злоумышленник государственного масштаба, который находится «где-то далеко».

Что такое кибер?

Слово «кибер», хотя и звучит оно так, будто пришло из романов Уильяма Гибсона, – на самом деле часть терминологии, принятой в армии США. Военные считали, что существует четыре театра военных действий, на которых допустимо ведение войны между государствами: суша, море, воздух и космическое пространство. Когда Интернет начал использоваться государствами для взаимодействия и противодействия, пришло понимание, что появился новый театр военных действий – киберпространство. Отсюда и пошло название.

Коль скоро государство стало формулировать киберстратегии и говорить о киберпреступлениях, крупные производители, естественно, подхватили жаргон. Так мы и пришли к ситуации, когда отовсюду несутся слова о различных «киберах» и связанных с ними угрозах. К сожалению, слово «кибер» стало универсальным маркетинговым термином для описания угроз и патентованных решений для борьбы с ними. Коммерциализация и неумеренное использование привели к размыванию смысла термина, превратив его в посмешище в сообществе специалистов по безопасности. В частности, люди, технически подкованные или настроенные агрессивно, зачастую употребляют слово «кибер» как издевательство.

Хотя некоторые из нас (включая нескольких авторов) стараются не употреблять слова «кибер», нельзя отрицать, что оно хорошо знакомо людям, далеким от техники и проблем безопасности. Альтернативы: «информационная безопасность», «инфобезопасность», «цифровая безопасность» – для многих куда менее понятны. Так что если слово «кибер» помогает вам в общении с людьми, плохо знакомыми с тематикой безопасности или больше ориентированными на пиар и маркетинг, то так тому и быть. Ну а разговаривая на технические темы или общаясь с людьми, более близкими к хакерскому краю спектра, имейте в виду, что это слово может обесценить ваши слова или вообще лишить их смысла.

Так вот – это не так.

Есть много типов атакующих: молодые, лишенные запретов и неугомонные люди; автоматизированные скрипты и поисковые роботы, неустанно ищущие мишени; недовольные работники; организованная преступность и политические активисты. Разнообразие атакующих куда шире и сложнее, одним словом «кибер» его не опишешь.

Мотивы, ресурсы, доступ

Размышляя о том, каких противников может заинтересовать ваша организация, принимайте во внимание как работающие в организации системы, так и людей. При этом следует учитывать три аспекта противника.

1. Цели и мотивы (почему он атакует и что надеется приобрести).
2. Ресурсы (что он может сделать, чем он может воспользоваться, чтобы это сделать, и каким временем располагает).
3. Доступ (до чего он может добраться, из каких источников получить информацию).

Пытаясь понять, от какого противника защищать организацию, насколько вероятна атака со стороны противника каждого типа и каковы возможные последствия, мы должны проанализировать все эти атрибуты в контексте организации, ее ценностей, практики работы и видов деятельности.

Мы рассмотрим эту тему гораздо подробнее, когда будем изучать создание персон безопасности и интегрировать их с процессами сбора требований и тестирования.

Цели безопасности: защита данных, систем и людей

Мы имеем право ожидать, что, занимаясь повседневными делами и взаимодействуя с технологиями и системами, не попадем в беду, пока данные остаются неповрежденными и конфиденциальными.

Безопасность – это способ обеспечить такое положение вещей, а для ее достижения мы сформулируем ряд целей.

Понимание того, что мы пытаемся защитить

Прежде всего следует решить, *что именно* мы пытаемся защитить, каковы брильянты короны в нашем мире и где они хранятся. Удивительно, сколько людей совершают какие-то действия, не понимая этого, а в результате тратят уйму времени и денег, защищая совсем не то, что нужно.

Конфиденциальность, целостность и доступность

Конфиденциальность, целостность и доступность (CIA) – сокровище среди традиционных понятий безопасности. Этот акроним служит для

описания и запоминания трех краеугольных камней безопасных систем – тех аспектов, которые мы стремимся защитить.

Конфиденциальность: держи в секрете

В наши дни мало найдется систем, которые разрешали бы всем делать всё. Мы разделяем пользователей приложения на роли и обязанности. Мы хотим быть уверены, что доступ к данным и возможность манипулировать ими были разрешены только людям, которым мы доверяем, прошедшим аутентификацию и авторизацию.

Этот аспект контроля и составляет суть конфиденциальности.

Целостность: береги от повреждений

Наши системы и приложения строятся вокруг данных. В процессе работы мы сохраняем данные, обрабатываем их и обмениваемся ими десятками разных способов.

Принимая ответственность за данные, мы предполагаем, что они будут храниться в контролируемом состоянии. Что с того момента, как нам доверили данные, мы понимаем и можем контролировать способы их модификации (кто может изменять данные, когда и каким образом). Поддержание целостности данных не означает, что их надо сохранять «законсервированными», в неизменном виде; важно, чтобы они подвергались контролируемым и предсказуемым операциям, чтобы мы понимали и могли сохранить текущее состояние данных.

Доступность: держи двери открытыми, а свет включенным

Система, к которой нельзя обратиться или использовать так, как было задумано, бесполезна. Наш бизнес и сама жизнь зависят от способности получить доступ и взаимодействовать с данными и системами почти без перерывов.

Не слишком остроумные циники скажут, что для того чтобы как следует обезопасить систему, ее нужно выключить, заключить в бетонный куб и опустить на дно океана. Но это помешает удовлетворить требование доступности.

Безопасность требует защитить данные, системы и людей, не мешая взаимодействию с ними.

Это значит, что мы должны отыскать баланс между средствами (или мерами) контроля для ограничения доступами или защиты информации и функциональностью, которая предоставляется пользователям как часть приложения. Как мы увидим, именно отыскание баланса и составляет основную проблему в нашем постоянно подключенном к сети обществе, делящемся информацией.

Неотрицаемость

Неотрицаемостью называется доказательство происхождения и целостности данных, иначе говоря, уверенность в невозможности отрицать совершенное действие. Неотрицаемость – это дополнение к аудитопригодности, и вместе они дают основания утверждать, что любое действие в системе – любое изменение, любую выполненную задачу – можно проследить до конкретного лица или до авторизованной операции.

Этот механизм связывания действия с описанием факта использования или поведением физического лица дает нам возможность поведать всю историю данных. Мы можем воссоздать и проследить все изменения и операции доступа и выстроить хронологию событий. Эта хронология поможет выявить подозрительную активность, расследовать инциденты безопасности или случаи некорректного использования и даже отлаживать функциональные дефекты в системах.

Соответствие нормативным требованиям, регулирование и стандарты безопасности

Во многих организациях одна из главных движущих сил программы обеспечения безопасности – необходимость соответствовать требованиям законодательства или отраслевым нормам. Они определяют, как должно функционировать предприятие и как следует проектировать, строить и эксплуатировать системы.

Нормативные требования можно любить или ненавидеть, но они всегда были – и будут – катализатором изменений в системе безопасности и зачастую помогают получить одобрение и поддержку со стороны руководства, без которых невозможно продвигать инициативы и внедрять изменения в сфере безопасности. Непреложные нормативные требования, «надо, и все тут» – иногда единственный способ убедить людей делать неприятные вещи, необходимые для обеспечения безопасности и конфиденциальности.

С самого начала нужно ясно понимать, что соответствие требованиям и регулирование – вещи, связанные с безопасностью, но не тождественные ей. Система может соответствовать всем требованиям и быть небезопасной, или быть безопасной, но не соответствовать требованиям. В идеальном мире все системы были бы соответствующими требованиям и безопасными, но следует отметить, что одно необязательно влечет за собой другое.

Эти концепции настолько важны, что мы посвятили им целую главу 14 «Соответствие нормативным требованиям».

Типичные заблуждения и ошибки в области безопасности

При изучении любого предмета знать антипаттерны не менее полезно, чем паттерны; понимание того, чем *не является* нечто, помогает двигаться в правильном направлении к пониманию того, чем же оно является.

Ниже приведено собрание (почти наверняка неполное) типичных заблуждений, касающихся безопасности. Стоит приглядеться, как становится ясно, что они возникают с раздражающей частотой, причем не только в технологических отраслях, но и в СМИ и даже на вашем рабочем месте.

Безопасность абсолютна

Безопасность – это не черное или белое, однако представление о том, что система является либо безопасной, либо нет, бытует повсеместно и опровергается бессчетное число раз на дню. Для любой достаточно сложной системы утверждение о ее абсолютной безопасности или небезопасности невероятно трудно, а то и вовсе невозможно доказать, поскольку все зависит от контекста.

Цель *безопасной* системы – гарантировать внедрение уровня контроля, адекватного угрозам, релевантным сценарию использования данной системы. Если сценарий изменяется, то должны измениться и средства контроля, необходимые для того, чтобы система оставалась безопасной. Аналогично, если изменяются угрозы системе, то и средства контроля должны эволюционировать соответственно.

Безопасность от кого? безопасность от чего? и *как можно было бы обойти принятые меры?* – вот вопросы, которые должны вертеться на языке при рассмотрении безопасности системы.

Безопасность – достижимое состояние

Никакая организация и никакая система никогда не будут «безопасными». Никто не повесит вам медаль на грудь, и никто не скажет, что работа сделана, система безопасна и можно идти домой. Безопасность – это культура, выбор стиля жизни, если хотите, это непрерывное стремление понять мир вокруг нас и реагировать на него. Мир постоянно изменяется, изменяется его влияние на нас, поэтому должны изменяться и мы сами.

Гораздо полезнее считать безопасность вектором, указывающим направление движения, а не точкой, в которую нужно прийти. У вектора

есть длина и направление, он говорит, куда и с какой скоростью двигаться в погоне за безопасностью. Но это дорога, по которой придется идти вечно.

Классический взгляд на безопасность можно проиллюстрировать старым анекдотом о двух охотниках, неожиданно повстречавших льва. Первый останавливается, чтобы получше завязать шнурки, второй оборачивается и кричит: «Ты спятил? Тебе же никогда не обогнать льва». Второй отвечает: «А мне и не надо обгонять льва, мне надо только обогнать тебя».

Ваши системы будут безопасны, если большинство противников решит, что получит большую выгоду, атаковав кого-нибудь другого. Как правило, организация не может повлиять на мотивы и поведение противника, поэтому ваша лучшая стратегия защиты – сделать атаку настолько трудной и дорогой, чтобы овчинка не стоила выделки.

Безопасность статична

Средства обеспечения безопасности, угрозы и подходы постоянно эволюционируют. Взгляните, как изменилась разработка программного обеспечения за последние пять лет. Подумайте, сколько появилось новых языков и библиотек, сколько проведено конференций и опубликовано статей для презентации новых идей. Безопасность в этом смысле ничем не отличается. И атакующая, и обороняющаяся стороны непрерывно модифицируют подходы и разрабатывают новые методы. Стоит атакующему обнаружить новую уязвимость и превратить ее в оружие, как защитник уже наготове и разрабатывает меры смягчения последствий и заплаты. В этой области, как и в области разработки ПО, никогда не перестаешь учиться и пробовать.

Для безопасности необходимо специальное [вставьте по своему усмотрению: пункт, устройство, бюджет]

Нет никакого недостатка в производителях и специалистах, готовых обеспечить безопасность вашей организации и систем, но правда в том, что, для того чтобы начать эту работу, ничего специального не нужно. Очень немногие из лучших специалистов по безопасности имеют какой-то сертификат или особый статус, подтверждающий сдачу некоторого экзамена; они просто посвящают своему делу все время. Обеспечение безопасности – это про отношение, культуру и подход. Не ждите, пока появится подходящее время, инструмент или учебный курс. Просто начните что-то делать.

В своем путешествии в мир безопасности вы обязательно столкнетесь с производителями, которые захотят продать вам всевозможные решения, которые позаботятся о безопасности. Да, существует немало инструментов, способных внести ощутимый вклад в общую безопасность, но не попадайтесь в ловушку – не громоздите гору лишнего. Сложность – враг безопасности, а больше почти всегда означает сложнее (даже если речь идет о большем количестве средств обеспечения безопасности). Один из авторов книги следует такому эвристическому правилу: не добавлять новое решение, если оно не позволяет вывести из эксплуатации два других. Помните об этом.

Начнем, пожалуй

Если вы заинтересовались этой книгой, то, скорее всего, вы либо разработчик, который хочет побольше узнать о безопасности, либо безопасник, желающий разобраться, что это за зверь – гибкие методики, – о котором трещат все разработчики. (Если вы не попадаете ни в одну из этих категорий, то будем считать, что у вас имеются какие-то свои, чертовски веские причины прочитать книгу о гибком обеспечении безопасности, и поставим на этом точку.)

Одна из причин, побудивших нас написать эту книгу, состоит в том, что, несмотря на очевидную необходимость глубокого взаимопонимания между разработчиками и «безопасниками», за много лет наблюдений мы такого понимания (смеем даже сказать, эмоциональной близости) почти не встречали. Более того, зачастую стороны не только не понимают друг друга, но и активно стремятся свести взаимодействие к минимуму или, хуже того, подрывают все усилия другой стороны.

Мы надеемся, что некоторые воззрения и опыт, нашедший отражение на страницах этой книги, помогут хотя бы частично устранить недопонимание и, быть может, даже недоверие между разработчиками и «безопасниками» и прольют свет на то, *что и почему делает другая сторона*.