ГЛАВА 1

Создание программы безопасности

> У людей аллергия на перемены. Они любят повторять: «Мы же всегда так делали». Я пытаюсь с этим бороться. Поэтому у меня на стене висят часы, которые идут против часовой стрелки.
>
> *Грейс Хоппер (Grace Hopper), «Остроумие и мудрость Грейс Хоппер» (1987)*

Создание или улучшение программы безопасности может оказаться непростой задачей. Учитывая количество подлежащих учету факторов, чем больше уделишь внимания предварительным размышлениям и планированию при формировании этой программы, тем легче будет справляться с ней в долгосрочной перспективе. В этой главе мы рассмотрим базовую структуру программы безопасности и первоначальные административные шаги.

Не заводите привычку просто выполнять задачи, следовать установленному распорядку и, завершая настройку, думать: «Мы же всегда так делали». Такое мышление со временем будет только препятствовать прогрессу и наносить ущерб положению дел в вашей системе безопасности.

Мы рекомендуем вам при формировании своей программы безопасности следовать всем описанным в этой главе шагам в указанном порядке. Хотя мы постарались соответствующим образом сгруппировать и остальные главы, но их можно изучать оптимальным для вашей организации способом.

Заложите фундамент

Не нужно изобретать велосипед, закладывая фундамент программы информационной безопасности. Есть несколько стандартов, которые могут быть очень полезны и о которых пойдет речь в главе 8. Национальный институт стандартов и технологий (NIST) разработал основанный на оценке рисков фреймворк кибербезопасности, охватывающий множество аспектов такой программы. Фреймворк кибербезопасности NIST, Cybersecurity Framework (CSF) 2.0 (https://oreil.ly/p5k3B), состоит из шести параллельно выполняющихся непрерывных функций: идентификация, защита, обнаружение, реагирование, восстановление и управление. В совокупности все эти функции обеспечивают высокоуровневое стратегическое ви́дение полного жизненного цикла системы управления рисками в области кибербезопасности в организации.

Возможным преимуществом является не только фреймворк, но и стандарты комплаенса. Хотя неудачно внедренные стандарты комплаенса могут стать помехой в обеспечении безопасности организации в целом, рассматривайте их как отправную точку новой программы. Более подробно стандарты мы обсудим в главе 8. Конечно, несмотря на то что подобные ресурсы могут быть весьма полезны, надо учитывать, что все организации разные и какие-то из описанных здесь моментов в вашем случае могут оказаться нерелевантными, — на страницах книги мы будем напоминать об этом вновь и вновь.

Сформируйте команду

Как и во множестве других отделов, в деле безопасности искусство заключается в том, чтобы собрать достойных сотрудников в достойные команды. Открытое общение между командами — это главное, ведь без этого конфигурация системы безопасности всерьез ослабнет. Хотя в небольших организациях можно объединять какие-то из описанных ниже команд — или вовсе обойтись без каких-то из них, — но это все же хороший ориентир при формировании отдела безопасности.

Руководство

Начальник информационного отдела (CIO) или отдела информационной безопасности (CISO) обеспечат команду влиянием и полномочиями, необходимыми для принятия решений и внесения изменений в масштабах всей компании. Также руководство уполномочено вырабатывать долгосрочное ви́дение, извещать о корпоративных рисках, определять задачи, обеспечивать финансирование и размечать этапы работы.

Команда управления рисками

Во многих организациях уже есть группы оценки рисков, и можно объединиться с ними. В большинстве компаний кибербезопасность — это вовсе не приоритет. Эта команда будет просчитывать риски, связанные со многими другими сферами бизнеса, от продаж до маркетинга и финансов. Возможно, кибербезопасность — это не то, в чем они хорошо разбираются. В этом случае можно либо обучать их основам кибербезопасности, разбирая каждый конкретный случай, либо добавить в команду аналитика рисков в области кибербезопасности. Тут могут оказаться полезны такие фреймворки по рискам, как фреймворк риск-менеджмента (RMF) от NIST (https://oreil.ly/wJ7W), фреймворк оценки критически опасных угроз, активов и уязвимостей (OCTAVE) или стандарты Комитета организаций-спонсоров Комиссии Тредвея (COSO).

Команда кибербезопасности

Команда кибербезопасности выполняет задачи по оценке среды и усилению защиты. Большая часть книги адресована именно ей и руководству. Ее участники отвечают за повседневную работу по обеспечению безопасности: управляют

активами, оценивают угрозы и уязвимости, проводят мониторинг среды на предмет атак и угроз, занимаются риск-менеджментом и обучают сотрудников. В достаточно крупной организации эту команду можно разбить на различные подгруппы: по сетевой безопасности, операционной безопасности (OPSEC), администрированию СЗИ (средств защиты информации), безопасности приложений, а также наступательной безопасности.

Команда аудита

Всегда полезно иметь систему проверки и балансировки. Это позволяет не только находить пробелы в мерах по обеспечению безопасности и средствах контроля над ними, но и убеждаться в том, что выполняются все необходимые задачи и достигаются контрольные показатели. Как и команду киберрисков, команду аудита также можно включить в состав более крупной команды.

И еще раз — ввиду бюджетных или кадровых ограничений малый и средний бизнес может объединять эти команды в разных конфигурациях или вообще свести все в одну. В таких случаях мы вам искренне сочувствуем. По мере роста компании и, будем надеяться, также и программы безопасности можно будет запланировать распределение ролей с наполнением их соответствующими функциями.

Определите базовый уровень безопасности

Неизвестность всегда будет вызывать опасения, но это не должно вас останавливать. Как оценить прогресс в построении системы, не зная, с чего она начиналась? По идее, приоритет всех команд при запуске новой программы безопасности — определить ее базовые характеристики, а при глубоком погружении в уже существующую — всесторонне ее исследовать. В этой книге мы не раз и под разными углами рассмотрим управление активами. Формирование базового уровня безопасности организации — это просто очередной этап процесса управления в целом. Для этого вам надо будет собрать информацию по всем этим пунктам:

- политики, процедуры и руководства по реагированию на инциденты;
- конечные точки — компьютеры и серверы, с указанием даты установки программного обеспечения и его версии;
- сроки действия лицензий на программное обеспечение, а также даты окончания сертификатов протокола SSL;
- цифровой след организации (внешний контур) — домены, почтовые серверы, устройства демилитаризованной зоны (DMZ)[1], облачная архитектура;

[1] Демилитаризованная зона (от англ. Demilitarized Zone) — это часть сети с публичной IP-адресацией, отделяющая локальную сеть организации от сетей публичного доступа (например, от сети Интернет). — *Примеч. науч. ред.*

- сетевые устройства и связанная с ними информация — маршрутизаторы, коммутаторы, точки доступа, системы обнаружения/предотвращения вторжений (IDS/IPS) и данные о сетевом трафике;
- логирование и мониторинг;
- точки входящего/исходящего трафика — контакты интернет-провайдеров (ISP), номера учетных записей и IP-адреса;
- внешние подрядчики, с удаленным доступом к системе или без, и их основные контактные данные;
- приложения — любое программное обеспечение, которое ваша компания либо поддерживает, либо использует в ключевых своих бизнес-процессах.

Оцените угрозы и риски

Как уже говорилось, создание команды или должности по управлению рисками — это ключевой элемент формирования команды информационной безопасности. Не зная угроз и рисков, с которыми сталкивается ваша организация, трудно подобрать подходящие технологии и дать рекомендации по надлежащей защите компании. Выбор способов оценки угроз и рисков зависит от специфики организации: ее инфраструктуры и среды и требует как высокоуровневого обзора рисков, так и глубокого знания активов.

Более подробную информацию можно найти, изучая тему управления, рисков и комплаенса (GRC). Поскольку в этой книге мы не можем всесторонне охватить стратегию GRC, то сделаем просто общий обзор структуры управления рисками. Есть несколько фреймворков риск-менеджмента, но в целом их можно свести к пяти этапам: *выявление, оценка, митигация, мониторинг и управление*.

Определите масштаб, активы и угрозы

Компаниям следует учитывать большое количество потенциальных угроз и рисков, которым подвержены разные отрасли. Фокусировка на отраслевых трендах и специфических угрозах поможет настроить эффективную программу безопасности и верно расставить приоритеты. Многие компании уделяют не слишком много внимания угрозам и рискам, с которыми они сами же сталкиваются практически ежедневно, — и так и будут продолжать в том же духе, пока не падут их жертвами. Хотя есть бесценный ресурс — информационно-аналитические центры (ISACs), сведенные воедино Национальным советом ISACs, NCI (https://oreil.ly/-DVqI) для обмена отраслевыми руководствами по информационной безопасности. NCI описывает их (https://oreil.ly/_xR7Q) следующим образом: «ISAC собирает, анализирует и распространяет среди своих членов практически применимую информацию о реальных угрозах и предоставляет им инструменты митигации рисков и повышения устойчивости».

Необходимо выявлять не только специфические отраслевые угрозы, но и широко распространенные, такие как вредоносное ПО, программы-вымогатели, фишинг

и удаленные эксплойты. Три важных ресурса, на которые стоит обратить внимание: OWASP Top 10[1] (https://oreil.ly/ZAuaR); Центр интернет-безопасности «Контроль над критически важными аспектами кибербезопасности» (CIS Controls, https://oreil.ly/RpT5m); стандарты, изложенные Альянсом облачной безопасности, CSA (https://oreil.ly/Z-Re1). Большинство пунктов этих списков мы еще рассмотрим подробнее, но сверяться с их ежегодными обновлениями должно стать ключевым компонентом любого стратегического плана.

Оцените риски и последствия

После выявления потенциальных рисков оцените, представляют ли они опасность для вашей компании. Сканирование внутренних и внешних систем на уязвимости, аудит правил межсетевых экранов, анализ механизмов аутентификации и прав пользователей, правил управления активами, а также их обнаружение помогут вам составить более ясное представление относительно общей подверженности рискам вашей системы.

На этапе оценки необходимо проанализировать каждый выявленный риск, чтобы определить вероятность его негативного воздействия на организацию, степень серьезности предполагаемого ущерба и вероятный способ осуществления атаки. К примеру:

Угроза: Злоумышленник использует новую уязвимость в _____.

Уязвимость: Не исправлена.

Актив: Почтовый сервер.

Последствия: Удаленное выполнение кода (RCE) для получения доступа к внутренним системам.

Митигация

Митигация рисков — это то, ради чего мы все здесь собрались, а также цель большей части этой книги. Возможные варианты: предотвращение рисков, устранение рисков, передача рисков и принятие рисков.

Предотвращение рисков

Дэйв решает, что в хранении номеров социального страхования клиентов нет необходимости, и прекращает эту практику.

Устранение рисков

Алекс отключает открытые порты, внедряет более строгие правила межсетевого экрана и латает изъяны конечных точек.

---

[1] OWASP Top 10 — список из десяти наиболее критичных уязвимостей веб-приложений по версии проекта OWASP (Open Web Application Security Project). — *Примеч. науч. ред.*

Передача рисков

Йен передает обработку кредитных карт на аутсорс третьей стороне, вместо того чтобы хранить данные в своей системе.

Принятие рисков

Кейт знает, что у определенной конечной точки нет доступа к другим конечным точкам, и запускает на ней стороннее приложение. У этого приложения есть небольшая уязвимость, необходимая для его работы. Хотя на данный момент устранить эту уязвимость невозможно, уровень риска сейчас достаточно низок и пойти на него можно.

Принимать риск следует только в крайнем случае. Если дошло уже до этого, запросите полную документацию у подрядчиков и руководства, а также документацию о мерах, в результате которых было принято это решение. Запланируйте по меньшей мере ежегодный пересмотр всех принятых рисков, чтобы гарантированно и должным образом проводить их переоценку.

Отслеживайте риски

Отслеживайте риски, проводя регулярные ежеквартальные или ежегодные встречи. В течение года изменится многое, что повлияет на количество и виды рисков, которые вам теперь следует учитывать. В рамках мониторинга изменений и контроля над ними определяйте, влияют ли каким-либо образом нынешние изменения на риски для вас.

Один из способов отслеживать текущее состояние рисков — это составить реестр рисков, чтобы документировать различные сценарии, средства контроля и планы восстановления. Это можно совместить с программой управления уязвимостями.

Управляйте рисками

Управление в контексте риск-менеджмента — это важный этап, обеспечивающий постоянное согласование методов защиты организации с ее общими целями и нормативными требованиями. Он включает в себя разработку политик, процедур и механизмов контроля, которые определяют процесс принятия решений в области управления рисками. Этот этап служит основой всего риск-менеджмента, обеспечивая согласованность, подотчетность и соответствие требованиям, принятым в организации в целом.

Эффективное управление рисками предполагает активное участие высшего руководства и всех вовлеченных в эту работу сотрудников в постановке четких целей риск-менеджмента, в распределении ролей и обязанностей, а также в установлении критериев приемлемости и допустимости рисков. Речь идет о формировании культуры осознанного подхода к рискам, когда принятие решений основывается на глубоком понимании их потенциальной угрозы для организации.

Далее рассмотрим ключевые моменты управления.

Разработка и поддержание политики

Опишите в комплексных политиках, как выявлять, оценивать, снижать, отслеживать риски и сообщать о них. Эти политики следует регулярно пересматривать и обновлять с учетом меняющегося ландшафта угроз и приоритетов организации.

Соблюдение комплаенса

Приведите риск-менеджмент организации в соответствие с действующим законом, нормативными актами и отраслевыми стандартами. Это значит быть в курсе изменений нормативов и адаптировать к ним соответствующие политики и процедуры.

Информирование о рисках и отчетность по рискам

Установите четкие каналы связи, чтобы гарантированно информировать все уровни организации о работах по риск-менеджменту, полученных результатах и сделанных выводах. Регулярная отчетность перед заинтересованными сторонами, включая руководство и совет директоров, способствует прозрачности работы, что благоприятно для принятия обоснованных решений.

Обучение и аварнес (формирование осознанного отношения)

Разработайте и проведите обучающие программы, чтобы повысить у сотрудников уровень осознанности в подходе к рискам и убедиться, что они понимают свои роли и ответственность в том, как митигировать риски, если инцидент все-таки произошел. Культивируйте восприятие безопасности и риск-менеджмента как ценность и фундаментальные составляющие успеха организации.

Непрерывное совершенствование

Внедрите систему обратной связи, чтобы учиться на прошлых инцидентах, их аудитах и выводах по ним — чтобы постоянно совершенствовать фреймворк по управлению рисками. Это означает и анализировать эффективность стратегии риск-менеджмента, и выявлять слабые, требующие усиления стороны, и корректировать сложившиеся наработки для более эффективного достижения целей организации.

Эффективно управляясь с риск-менеджментом, организация может не только защитить свои активы и минимизировать потери, но и повысить свою операционную эффективность и тем самым укрепить доверие к себе со стороны клиентов, партнеров и регуляторов. Системное руководство — краеугольный камень фреймворка риск-менеджмента, объединяющий усилия по выявлению, оценке, митигации и мониторингу рисков в последовательный стратегический подход, который обеспечивает устойчивость и успех организации.

Расставьте приоритеты

Как только вы выявили угрозы и риски, тут же приоритизируйте их: ранжируйте от наивысшего процента вероятности риска до низшего, чтобы спланировать меры по их устранению (с акцентом на постоянную защиту). Это не всегда должны быть дорогостоящие решения. Многие меры защиты могут стоить вашей организации мало или обойтись вовсе бесплатно. Это открывает множество возможностей запустить программу безопасности даже совсем без бюджета. Если тщательно подготовить запуск бесплатной программы, это должно будет выглядеть убедительно в глазах руководства.

Не всегда следуйте советам разработчиков приложений, вендоров и сторонних организаций относительно приоритизации. Каждая среда уникальна, и относиться к ней нужно соответственно. Расставляйте приоритеты, исходя из общей картины, когда собрана вся необходимая информация.

Эту книгу не следует рассматривать как последовательный список подлежащих выполнению задач. Расстановки приоритетов могут значительно отличаться друг от друга в разных средах. Просто помните, что если ваша среда уже атакована и полыхает, начинайте не с создания политик или реверс-инжиниринга вредоносного ПО. Как пожарному, вам не стоит заниматься поиском поджигателя и очага возгорания, пока вы не потушили сам пожар.

Чтобы выявить степень приоритетности тех или иных рисков, можно воспользоваться матрицей рисков (https://oreil.ly/nJdmK), в которой общий уровень риска рассчитывается по формуле «Вероятность × Последствия», как показано на рис. 1.1.

	1: Ничтожно малая	2: Низкая	3: Средняя	4: Высокая	5: Чрезвычайно высокая
5: Критические	Средний 5	Умеренно высокий 10	Высокий 15	Очень высокий 20	Очень высокий 25
4: Существенные	Низкий 4	Средний 8	Умеренно высокий 12	Высокий 16	Очень высокий 20
3: Умеренные	Низкий 3	Средний 6	Средний 9	Умеренно высокий 12	Высокий 15
2: Несущественные	Низкий 2	Низкий 4	Средний 6	Средний 8	Умеренно высокий 10
1: Незначительные	Низкий 1	Низкий 2	Низкий 3	Низкий 4	Средний 5

Рис. 1.1. Матрица рисков

Разметьте этапы продвижения

Разметка этапов работы сопроводит вас от той точки, где вы находитесь сейчас, до желаемого пункта назначения. Она отображает целиком все продвижение на пути к созданию безопасной среды. В некоторой степени это входит в обязанности руководителя проекта, но в штатах многих компаний нет такой должности. Этапы можно разбить на четыре отрезка, или уровня.

Уровень 1: Быстрые победы

Первоначальным этапом должны стать «быстрые победы» — то есть то, что можно выполнить за считаные часы и дни и что устранит серьезные уязвимости: удалить неиспользуемые конечные точки, перевести устаревшие устройства в более безопасную сеть и обновить стороннее ПО — вот что подпадает под эту категорию. Мы обозначим в книге множество бесплатных решений, поскольку процесс закупок в некоторых организациях может заметно затягиваться.

Уровень 2: Первый год

Более серьезные уязвимости, для устранения которых потребуется, возможно, запустить процесс управления изменениями, менять процедуры и оповещать значительное количество людей, могут, вероятно, не попасть на предыдущий, первый уровень. Значительные изменения в сетевой маршрутизации, внедрение обучения персонала, вывод из эксплуатации общих учетных записей, служб и устройств — все это усовершенствования, которые практически не требуют бюджета, но могут занять чуть больше времени — ведь их надо спланировать и о них нужно оповестить сотрудников.

Уровень 3: Следующий год

К этому уровню относятся исправления уязвимостей и изменения, которые надо тщательно спланировать или ради которых требуется сначала подправить что-то еще. К примеру, переход всех бизнес-функций на облачные сервисы, обновление домена, замена серверов и основных устройств инфраструктуры, внедрение мониторинга и изменение аутентификации.

Уровень 4: Долгосрочное планирование

На некоторые шаги может уйти несколько лет — в силу масштабности проекта, нехватки бюджета, продления старых контрактов или затруднений при внедрении изменений. Сюда входят и реструктуризация сети, и замена основного программного обеспечения, и создание новых дата-центров.

При этом было бы полезно увязать каждый этап с выявленными критическими рисками и точками контроля. Хотя начинать с самых высоких рисков и уязвимостей — хорошая идея, устранить их может оказаться непросто. Во многих случаях это потребует не только значительных временных затрат и усилий по разработке

решений, но также и бюджета, которого может и не быть. Все эти моменты необходимо учитывать при планировании каждого этапа.

Варианты использования, внутренние учения и тренировки

Варианты использования (use cases) важны как наглядные примеры угроз для критически важной инфраструктуры, конфиденциальных данных и других активов. Проведите мозговой штурм с обладателями данных и руководителями, чтобы заранее спланировать, как справляться с вредоносными атаками. В идеале поначалу стоит выбрать три варианта и, сфокусировавшись на них, спланировать, как выстроить по ним механизмы обеспечения безопасности и мониторинг. Варианты использования предполагают такие угрозы, как программы-вымогатели, распределенные атаки типа «отказ в обслуживании» (DDoS), недовольные сотрудники, инсайдеры и утечки данных. Выбрав несколько сценариев, можно разбить их на этапы, проанализировать и соотнести с каждым шагом любого из фреймворков безопасности, представленных в этой книге, — или любых других, что могут появиться, когда мы ее уже закончим. Например, распространенный фреймворк, который зачастую сопоставляют с вариантами использования, — это Cyber Kill Chainот Lockheed Martin: https://oreil.ly/dk8JN.

Как описано в материалах Lockheed Martin (https://oreil.ly/btd1i),Cyber Kill Chain— это «модель для actionable intelligence, когда защищающаяся сторона настраивает защитные мощности организации в соответствии с конкретными действиями противника, атакующего предприятие». Кибератака состоит из семи этапов.

1. *Разведка*

   Исследование, выявление и выбор целей — часто происходят путем просмотра интернет-сайтов, таких как материалы конференций, также используется рассылка писем для обнаружения email-адресов, отслеживания социальных связей или информации о тех или иных технологиях.

2. *Вооружение и упаковка (weaponization)*

   Объединение трояна удаленного доступа с эксплойтом в доставляемую полезную нагрузку (deliverable payload)[1] — как правило, с помощью автоматизированного инструмента (weaponizer)[2]. Все чаще для распространения вирусов используются файлы клиентских приложений, такие как Adobe Portable Document Format (PDF) или документы Microsoft Office.

---

[1] Полезная нагрузка (от *англ.* payload) — это часть вредоносного ПО, которая производит разрушительные действия с данными, копирование информации с зараженного устройства и т. д. — *Примеч. науч. ред.*

[2] Weaponizer — инструмент, который объединяет вредоносное ПО и использует его для создания полезной нагрузки. — *Примеч. науч. ред.*

3. *Доставка*

   Транспортировка оружия в среду, на которую оно нацелено. Три самых распространенных переносчика полезной нагрузки: вложения в электронной почте, веб-сайты и съемные USB-носители.

4. *Заражение*

   Когда оружие доставлено на хост жертвы, запускается код злоумышленников. Чаще всего заражение происходит через уязвимость приложения или операционной системы, но бывает и так, что проще проникнуть через самих пользователей или посредством той функции операционной системы, которая автоматически выполняет код.

5. *Установка*

   Установка трояна удаленного доступа или бэкдора на систему жертвы позволяет злоумышленнику сохранять устойчивость в среде.

6. *Управление и контроль (command and control, C&C или C2)*

   Как правило, скомпрометированные хосты должны подключиться к серверу интернет-контроллера, чтобы установить C2-канал. Вредоносным APT-программам нужно скорее ручное управление, чем автоматическое осуществление. Как только C2-канал установлен — всё, у злоумышленников есть доступ к изнанке целевой среды буквально в режиме «руки на клавиатуре».

7. *Действия по достижению целей*

   Только теперь, пройдя шесть первых фаз, злоумышленники могут предпринять какие-то шаги по достижению своих изначальных целей. Как правило, такой целью является утечка данных, под чем подразумеваются сбор, шифрование и извлечение информации из среды жертвы; потенциальные цели также — нарушение целостности и сохранности данных. Как вариант, злоумышленникам может понадобиться доступ только к первой взломанной системе жертвы, чтобы она стала точкой входа для взлома вспомогательных систем и переходов внутри сети.

В этом материале достаточно информации, который можно использовать и для создания сценариев.

Таблица 1.1 — пример пошагового сценария kill chain, реализация которого не потребует дорогостоящего программного и аппаратного обеспечения и который мы смоделировали для разработки защиты от потенциальной атаки программы-вымогателя на компанию, располагающую временем для реализации проектов с открытым исходным кодом.

Относительно каждого шага kill chain можно применить множество различных защитных нейтрализующих мер — для снижения риска в целом.