Содержание

Об авторах

Юрий Диогенес – профессор Университета EC-Council. Получил степень магистра по кибербезопасности в колледже UTICA и степень магистра делового администрирования в FGV, Бразилия. В настоящее время имеет сертификаты CISSP, CyberSec First Responder, CompTIA CSA+, E|CEH, E|CSA, E|CHFI, E|CND, CyberSec First Responder, CompTIA, Security+, CompTIA Cloud Essentials, Network+, Mobility+, CASP, CSA+, MCSE, MCTS и Microsoft Specialist – Azure.

Прежде всего я хотел бы поблагодарить Бога за предоставленную мне возможность написать еще одну книгу. Я также хотел бы поблагодарить свою жену Александру и дочерей Янн и Айсис за их безоговорочную поддержку. Выражаю благодарность своему соавтору и другу Эрдалю Озкайе за прекрасное партнерство и Амрите Норонье за ее удивительную поддержку на протяжении всего этого проекта.

Эрдаль Озкайя – доктор философии в области кибербезопасности, магистр безопасности информационных систем и компьютерных исследований. Имеет сертификаты CEI, MCT, MCSE, E|CEH, E|CSA, E|CISO, CFR и CISSP. Он работает в компании Microsoft архитектором по кибербезопасности и консультантом по вопросам ИБ, а по совместительству преподает в Университете Чарльза Стерта в Австралии. Является соавтором множества учебных материалов по сертификации безопасности для различных поставщиков и выступает на международных конференциях, имеет множество наград в своей области. Он много работает над тем, чтобы сделать кибермир безопасным.

Я бы хотел поблагодарить свою жену Арзу и моих детей Джемре и Азру за их поддержку и любовь и выразить особую благодарность моим родителям и братьям, которые помогли мне стать тем, кто я есть. Я также хотел бы поблагодарить своего руководителя, доктора Рафикула Ислама, за его помощь всякий раз, когда она была мне нужна.

О рецензентах

Виджай Кумар Велу – специалист по информационной безопасности, автор, докладчик и блогер. В настоящее время он живет в Малайзии. Имеет более чем 11-летний опыт работы в IT-индустрии. Является лицензированным специалистом по тестированиям на проникновения и специализируется на предоставлении технических решений различных киберпроблем. Автор книг *Mastering Kali Linux for Advanced Penetration Testing* (второе издание) и *Mobile Application Penetration Testing*.

Паскаль Акерман – опытный профессионал в области промышленной безопасности. Имеет степень по электротехнике и более чем 15-летний опыт в проектировании, поиске, устранении неисправностей и защите крупных промышленных систем управления и различных типов сетевых технологий. После более чем десятилетнего практического опыта работы в полевых условиях в 2015 г. он стал работать в компании Rockwell Automation. В настоящее время является старшим консультантом по промышленной кибербезопасности в Network and Security Services Group, а недавно стал цифровым кочевником и теперь путешествует по миру со своей семьей, сражаясь с киберпротивниками.

Предисловие

Когда ландшафт угроз постоянно расширяется, возникает необходимость иметь надежную стратегию в области безопасности, что в действительности означает усиление защиты, обнаружения и реагирования. На протяжении этой книги вы будете изучать методы атак и шаблоны, позволяющие распознавать аномальное поведение в вашей организации, с помощью тактических приемов Синей команды. Вы также научитесь методам сбора данных об эксплуатации, выявления рисков и продемонстрируете влияние на стратегии Красной и Синей команд.

Для кого эта книга

Эта книга предназначена для специалистов по информационной безопасности и IT-специалистов, которые хотят узнать больше о кибербезопасности.

О чем идет речь в этой книге

Глава 1 «Стратегия безопасности» определяет, что представляет собой данная стратегия и насколько важно наличие хорошей стратегии защиты и атаки.

Глава 2 «Процесс реагирования на компьютерные инциденты» знакомит с процессом реагирования на компьютерные инциденты и его значением. В ней рассматриваются различные отраслевые стандарты и передовые методы реагирования.

Глава 3 «Жизненный цикл атаки» готовит читателя к пониманию того, как мыслит злоумышленник, знакомит с различными этапами атаки и тем, что обычно происходит на каждом из этих этапов.

Глава 4 «Разведка и сбор данных» рассказывает о различных стратегиях проведения разведки и о том, как собирать данные для получения информации о цели, чтобы спланировать атаку.

Глава 5 «Компрометация системы» демонстрирует текущие тенденции в стратегии по взлому системы и объясняет, как скомпрометировать ее.

Глава 6 «Охота на пользовательские реквизиты» объясняет важность защиты реквизитов доступа пользователя во избежание кражи учетных данных, а также рассматривает процесс взлома данных реквизитов.

В *главе 7 «Дальнейшее распространение по сети»* описывается, как злоумышленники выполняют дальнейшее распространение по сети, после того как заразили систему.

Глава 8 «Повышение привилегий» показывает, как злоумышленники могут повысить привилегии, чтобы получить доступ к сетевой системе с правами администратора.

Глава 9 «Политика безопасности» фокусируется на различных аспектах начальной стратегии защиты, которая начинается с важности хорошо продуманной политики безопасности и охватывает передовые методы безопасности, стандарты, тренинги по безопасности и базовые средства контроля безопасности.

В *главе 10 «Сегментация сети»* подробно рассматриваются различные аспекты защиты, включая физическую сегментацию сети, а также виртуальное и гибридное облака.

Глава 11 «Активные сенсоры» подробно описывает различные типы сетевых сенсоров, которые помогают организациям обнаруживать атаки.

В *главе 12 «Кибербразведка»* рассказывается о различных аспектах кибербразведки, включая сообщество и основных поставщиков.

В *главе 13 «Расследование инцидента»* рассматриваются два тематических исследования для локальной скомпрометированной системы и облачной скомпрометированной системы, а также показываются все этапы, связанные с расследованием безопасности.

Глава 14 «Процесс восстановления» фокусируется на процессе восстановления взломанной системы и объясняет, насколько важно знать, какие параметры доступны, поскольку моментальное восстановление системы невозможно при определенных обстоятельствах.

В *главе 15 «Управление уязвимостями»* описывается важность управления уязвимостями для нейтрализации процесса эксплуатации уязвимостей. В ней показываются текущая картина угроз и растущее число программ-вымогателей, эксплуатирующих известные уязвимости.

В *главе 16 «Анализ журналов»* рассматриваются различные методы ручного анализа журналов, поскольку читателю важно получить знания о том, как подробно анализировать различные типы журналов для обнаружения подозрительных действий.

Чтобы получить максимальную отдачу от этой книги

1. Мы предполагаем, что читатели этой книги знакомы с основными понятиями информационной безопасности и операционными системами Windows и Linux.
2. Некоторые демонстрации из этой книги также могут быть проведены в лабораторной среде, поэтому мы рекомендуем вам создать виртуальную лабораторию, используя виртуальные машины Windows Server 2012, Windows 10 и Kali Linux.

Скачать цветные изображения

Мы также предоставляем PDF-файл с цветными изображениями скриншотов/диаграмм, используемых в этой книге. Вы можете скачать его здесь: **http://www.packtpub.com/sites/default/files/downloads/CybersecurityAttackandDefenseStrategies_ColorImages.pdf**.

Используемые условные обозначения

В этой книге используется ряд текстовых обозначений.

`КодВТексте`: указывает кодовые слова в тексте, имена таблиц базы данных, папок и файлов, расширения файлов, пути, фиктивные URL-адреса, ввод данных пользователем и имена пользователей в Twitter. Например: «Смонтируйте загруженный файл образа диска `WebStorm-10 * .dmg` в качестве еще одного диска в вашей системе».

Жирный шрифт: обозначает новый термин, важное слово или слова, которые вы видите на экране. Например, слова в меню или диалоговых окнах выглядят в тексте следующим образом: «Выберите раздел **Системная информация** на панели **Администрирование**».


Так будут оформляться советы и подсказки.


Так будут оформляться предупреждения и важные примечания.

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте **www.dmkpress.com**, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу **dmkpress@gmail.com**; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу **http://dmkpress.com/authors/publish_book/** или напишите в издательство по адресу **dmkpress@gmail.com**.

Скачивание исходного кода примеров

Скачать файлы с дополнительной информацией для книг издательства «ДМК Пресс» можно на сайте **www.dmkpress.com** или **www.дмк.рф** на странице с описанием соответствующей книги.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг – возможно, ошибку в основном тексте или программном коде, – мы будем очень благодарны, если вы сообщите нам о ней. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Если вы найдете какие-либо ошибки в коде, пожалуйста, сообщите о них главному редактору по адресу **dmkpress@gmail.com**, и мы исправим это в следующих тиражах.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и MITP очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты **dmkpress@gmail.com**.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Глава 1

Стратегия безопасности

За прошедшие годы инвестиции в сферу обеспечения безопасности перешли из разряда «nice to have» в разряд «must have», и теперь организации по всему миру понимают, насколько важно постоянно инвестировать в безопасность. Эти инвестиции обеспечат конкурентоспособность компании на рынке. Неспособность надлежащим образом защитить свои ресурсы может привести к невосполнимому ущербу, а в некоторых случаях – к банкротству. Из-за нынешнего ландшафта киберугроз недостаточно инвестировать только в защиту. Компании должны улучшать общую стратегию безопасности, а это означает, что инвестиции в защиту, обнаружение и реагирование должны быть согласованы.

В этой главе мы рассмотрим следующие темы:

- текущий ландшафт киберугроз;
- проблемы в пространстве кибербезопасности;
- как улучшить свою стратегию безопасности;
- роли Синей и Красной команд в вашей компании.

Текущий ландшафт киберугроз

С преобладанием постоянных подключений и достижений в технологиях, которые доступны на сегодняшний день, киберугрозы быстро развиваются, чтобы эксплуатировать различные аспекты этих технологий. Любое устройство уязвимо для атаки, а с появлением концепции «интернета вещей» (IoT) это стало реальностью. В октябре 2016 г. на DNS-серверы была проведена серия DDos-атак, в результате чего перестали работать некоторые основные веб-сервисы, такие как GitHub, Paypal, Spotify, Twitter и др. (1).

Это стало возможным из-за большого количества небезопасных IoT-устройств по всему миру. В то время как использование IoT для запуска масштабной кибератаки является чем-то новым, наличие уязвимости в этих устройствах таковым не является. На самом деле они были там довольно давно. В 2014 г. компания «ESET» сообщила о 73 000 незащищенных камерах безопасности с паролями по умолчанию (2). В апреле 2017 г. компания «IOActive» обнаружила

7000 уязвимых маршрутизаторов Linksys, хотя, по ее словам, число дополнительных маршрутизаторов могло доходить до 100 000 (3).

Главный исполнительный директор (CEO) может даже спросить: какое отношение уязвимости в домашнем устройстве имеют к нашей компании? Именно в этот момент **главный специалист по информационной безопасности** (CISO) должен быть готов дать ответ. Ведь у него должно быть лучшее понимание ландшафта киберугроз и того, как домашние устройства пользователей могут влиять на общую безопасность. Ответ приходит в виде двух простых сценариев, таких как удаленный доступ и **Bring your Own Device (BYOD).**

Хотя удаленный доступ не является чем-то новым, число удаленных работников растет в геометрической прогрессии. По данным Gallup (4), 43 % занятых американцев уже работают удаленно, а это означает, что они используют свою собственную инфраструктуру для доступа к ресурсам компаний. Усугубляет эту проблему рост числа компаний, разрешающих концепцию BYOD на рабочем месте. Имейте в виду, что существуют способы безопасного внедрения BYOD, но большинство сбоев в сценарии BYOD обычно происходит из-за плохого планирования и сетевой архитектуры, которые приводят к небезопасной реализации (5).

Что общего между всеми вышеупомянутыми технологиями? Чтобы управлять ими, нужен пользователь, и он по-прежнему является главной целью для атаки. Люди – самое слабое звено в цепи безопасности. По этой причине старые угрозы, такие как фишинговые электронные письма, продолжают расти в объеме, поскольку они затрагивают психологические аспекты пользователя, побуждая его кликнуть что-либо, например вложение файла или вредоносную ссылку. Обычно, когда пользователь выполняет одно из этих действий, его устройство заражается вредоносным ПО или к нему удаленно получает доступ хакер.

Таргетированная фишинговая кампания (spear phish) может начаться с электронного письма, которое, по сути, станет отправной точкой для злоумышленника, после чего будут использованы другие угрозы для эксплуатации уязвимостей в системе.

Одними из примеров растущей угрозы, которая использует фишинговые письма в качестве отправной точки для атаки, являются программы-вымогатели (ransomware). По сообщениям ФБР, только в течение первых трех месяцев 2016 г. вымогателям было выплачено 209 млн долл. (6). По данным компании «Trend Micro», рост числа атак с использованием программ-вымогателей стабилизировался в 2017 г. Тем не менее методы атаки и цели варьируются (7).

На рис. 1.1 показана взаимосвязь между этими атаками и конечным пользователем.

Эта диаграмма показывает четыре точки входа для конечного пользователя. Все они должны иметь свои риски, идентифицированные и обработанные с надлежащим контролем. Сценарии перечислены следующим образом:

- связь между локальными и облачными ресурсами (1);
- связь между BYOD-устройствами и облачными ресурсами (2);
- связь между корпоративными устройствами и локальными ресурсами (3);
- связь между персональными устройствами и облачными (4).

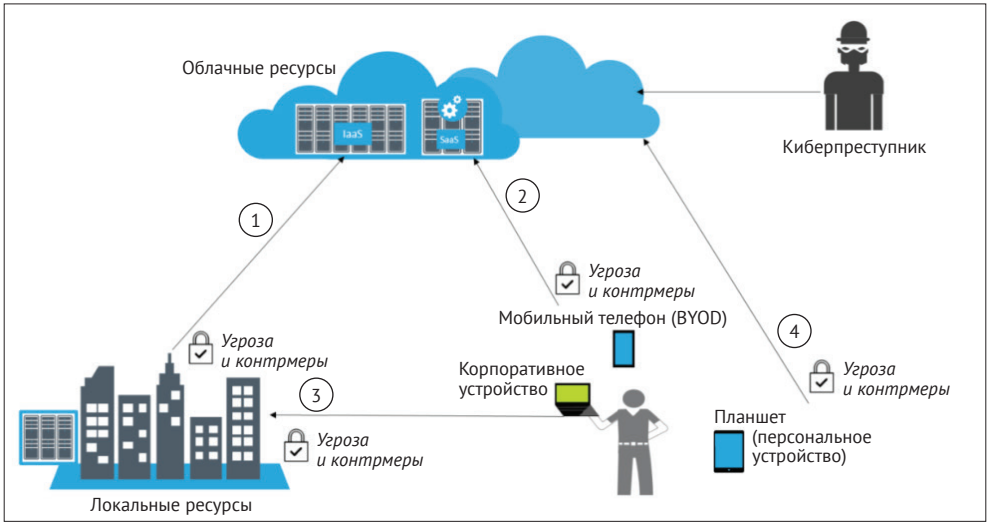

Рис. 1.1

Обратите внимание, что это разные сценарии, но все они связаны между собой одним объектом – конечным пользователем. Общий элемент во всех сценариях обычно является предпочтительной целью для киберпреступников, что показано на предыдущей диаграмме получения доступа к облачным ресурсам.

Во всех сценариях постоянно появляется еще один важный элемент – ресурсы облачных вычислений. Реальность такова, что в настоящее время нельзя игнорировать тот факт, что многие компании внедряют облачные вычисления. Подавляющее большинство начнется в гибридном сценарии, где модель **«Инфраструктура как услуга»** (**IaaS**) является их основным облачным сервисом. Ряд других компаний может использовать модель «**Программное обеспечение как услуга**» (**SaaS**) для некоторых решений, например для **управления мобильными устройствами** (**MDM**), как показано в сценарии (2). Можно утверждать, что в организациях с высокой степенью безопасности, таких как военные, может не быть облачной связи. Это, конечно, возможно, но, с коммерческой точки зрения, внедрение облачных вычислений растет и будет постепенно доминировать в большинстве сценариев развертывания.

Локальная безопасность имеет решающее значение, потому что это ядро компании, именно там большинство пользователей будет получать доступ к ресурсам. Когда организация решает расширить свою локальную инфраструктуру с помощью облачного провайдера, чтобы использовать модель IaaS (1), компании необходимо оценить угрозы для этого соединения и контрмеры для борьбы с этими угрозами с помощью оценки рисков.

Последний сценарий (4) может быть интригующим для некоторых скептически настроенных аналитиков. В основном это происходит потому, что они не сразу могут увидеть, что этот сценарий имеет корреляцию с ресурсами компа-

нии. Да, это персональное устройство без прямой связи с локальными ресурсами. Однако если это устройство скомпрометировано, то пользователь может потенциально скомпрометировать данные компании в следующих ситуациях:

- открытие корпоративной электронной почты с этого устройства;
- доступ к корпоративным SaaS-приложениям с этого устройства;
- если пользователь использует один и тот же пароль (8) для своей личной электронной почты и корпоративной учетной записи, это может привести к компрометации учетной записи посредством метода полного перебора или подбора пароля.

Наличие технических средств контроля безопасности может помочь нейтрализовать некоторые из этих угроз, направленных на конечного пользователя. Тем не менее основной защитой является постоянное обучение с проведением тренингов по безопасности.

Пользователь будет использовать свои **учетные данные** для взаимодействия с **приложениями**, чтобы либо использовать **данные**, либо записывать их на серверы, расположенные в облаке или локально. Все, что выделено жирным шрифтом, имеет уникальный ландшафт угроз, который должен быть идентифицирован и обработан. Мы рассмотрим эти области в следующих разделах.

Учетные данные – аутентификация и авторизация

Согласно отчету по расследованиям инцидентов в области информационной безопасности за 2017 г. от компании «Verizon» (9), связь между субъектом угрозы (или просто субъектом), его мотивами и способом действия варьируется в зависимости от отрасли. Тем не менее в докладе говорится, что украденные учетные данные являются предпочтительным вектором атаки для финансовой мотивации или организованной преступности. Эти данные очень важны, т. к. они показывают, что субъекты угроз следуют за учетными данными пользователя. Это позволяет сделать вывод, что компании должны уделять особое внимание аутентификации и авторизации пользователей и их прав доступа.

Отрасль согласилась с тем, что личность пользователя – это новый периметр. Он требует мер безопасности, специально разработанных для аутентификации и авторизации лиц на основании их работы и потребности в конкретных данных в сети. Кража учетных данных может быть только первым шагом, чтобы разрешить киберпреступникам доступ к вашей системе. Наличие действующей учетной записи пользователя в сети позволит им распространяться дальше и в какой-то момент найдет правильную возможность повысить привилегию до учетной записи администратора домена. По этой причине применение старой концепции глубокой защиты все еще является хорошей стратегией для защиты личности пользователя, как показано на рис. 1.2.

Здесь можно увидеть несколько уровней защиты, начиная с регулярного применения политики безопасности для учетных записей, которые следуют передовым отраслевым методам, таким как строгие требования к паролям, политика, требующая частой смены паролей и их надежности.

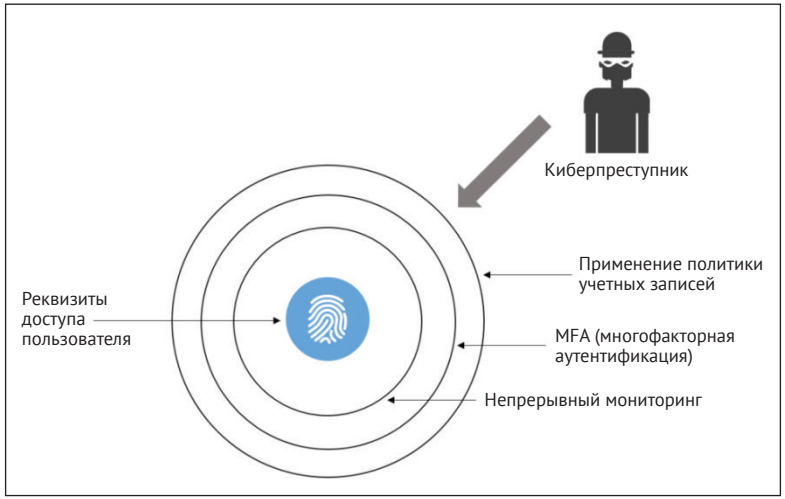

Рис. 1.2

Еще одной растущей тенденцией для защиты личных данных пользователей является применение многофакторной аутентификации. Один из методов, который получил более широкое распространение, – это функция обратного вызова, когда пользователь первоначально аутентифицируется, используя свои учетные данные (имя пользователя и пароль), и получает вызов для ввода своего пин-кода. Если оба фактора аутентификации успешны, им разрешен доступ к системе или сети. Мы рассмотрим эту тему более подробно в главе 6 «Охота на пользовательские реквизиты».

Приложения

Приложения являются точкой входа для пользователя, который использует данные и передает, обрабатывает или хранит информацию в системе. Приложения стремительно развиваются, и внедрение приложений на основе модели SaaS находится на подъеме. Тем не менее у этого объединения приложений есть унаследованные проблемы. Вот два ключевых примера:

- **безопасность** (насколько безопасны приложения, которые разрабатываются внутри компании, и приложения, за которые вы платите как за сервис);
- **приложения, принадлежащие компании, и персональные приложения** (у пользователей будет собственный набор приложений на своих устройствах – сценарий BYOD). Как эти приложения угрожают безопасности компании, и могут ли они привести к потенциальной утечке данных?).

Если у вас есть команда разработчиков, которые создают собственные приложения, следует принять меры, гарантирующие, что они используют безопас-

ную среду на протяжении всего жизненного цикла разработки программного обеспечения, например **Microsoft Security Security Lifecycle (SDL)** (10). При использовании SaaS-приложения, такого как Office 365, необходимо убедиться, что вы ознакомились с политикой безопасности и соответствия поставщика (11). В данном случае цель состоит в том, чтобы увидеть, могут ли поставщик и SaaS-приложение соответствовать требованиям безопасности и соответствия вашей компании.

Еще одна проблема безопасности, с которой сталкиваются приложения, заключается в том, как данные компании обрабатываются в разных приложениях, т. е. в тех, которые используются и одобрены компанией, и в тех, которые используются конечным пользователем (личные приложения). Эта проблема становится еще более острой в случае с SaaS, когда пользователи используют множество приложений, которые могут быть небезопасными. Традиционный подход к сетевой безопасности для поддержки приложений не предназначен для защиты данных в SaaS-приложениях. Дело обстоит еще хуже. Они не дают IT-специалистам наглядного представления о том, как их используют сотрудники. Этот сценарий также носит название Shadow IT, и, согласно опросу, проведенному **Cloud Security Alliance** (**CSA**) (12), только 8 % компаний знают о масштабах Shadow IT в своих организациях. Вы не можете защитить то, чего не знаете, а это уязвимый момент.

Согласно отчету о глобальных рисках в сфере IT лаборатории Касперского за 2016 г. (13), 54 % предприятий считают, что основные угрозы информационной безопасности связаны с ненадлежащим обменом данными через мобильные устройства. IT-отделам необходимо получать контроль над приложениями и применять политику безопасности на всех устройствах, принадлежащих компании и BYOD. Один из ключевых сценариев, который вам нужно нейтрализовать, описан на рис. 1.3.

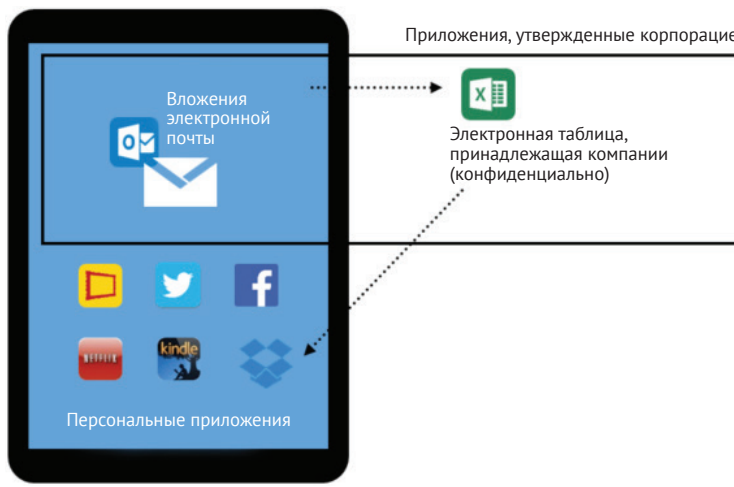

Рис. 1.3

В этом сценарии у нас имеется личный планшет пользователя, на котором есть утвержденные, а также персональные приложения. Без платформы, которая могла бы интегрировать управление устройствами с управлением приложениями, эта компания подвержена потенциальной утечке данных. В этом случае, если пользователь скачивает электронную таблицу Excel на свое устройство и загружает ее в персональное облачное хранилище Dropbox, а электронная таблица содержит конфиденциальную информацию компании, он создает утечку данных без ведома или возможности компании обезопасить себя.

Данные

Поскольку мы закончили предыдущий раздел, говоря о данных, следует убедиться, что данные всегда защищены, причем независимо от их текущего состояния (*в пути* или *в состоянии покоя*). В зависимости от состояния данных угрозы будут разными. Ниже приведены примеры потенциальных угроз и контрмеры.

Состояние	**Описание**	**Угрозы**	**Контрмеры**	**Нарушение трех ключевых принципов информационной безопасности**
Данные в состоянии покоя на устройстве пользователя	В настоящее время данные находятся на устройстве пользователя	Несанкционированный или вредоносный процесс может прочитать либо изменить данные	Шифрование данных в состоянии покоя. Это может быть шифрование на уровне файлов или шифрование диска	Конфиденциальность и целостность
Данные в пути	В настоящее время данные передаются с одного хоста на другой	В ходе атаки посредника данные могут быть прочитаны, изменены или похищены	Для шифрования данных при передаче могут быть использованы протоколы SSL/TLS	Конфиденциальность и целостность
Данные в состоянии покоя локально (сервер) или в облаке	Данные находятся в состоянии покоя либо на жестком диске сервера, расположенном локально, либо в облаке (пул хранения)	Несанкционированные или вредоносные процессы могут прочитать или изменить данные	Шифрование данных в состоянии покоя. Это может быть шифрование на уровне файлов или шифрование диска	Конфиденциальность и целостность

Это всего лишь несколько примеров потенциальных угроз и предлагаемых контрмер. Для полного понимания пути передачи данных в соответствии с потребностями клиента необходимо провести более глубокий анализ. У каждого клиента будут свои особенности, касающиеся пути передачи данных, соответствия, правил и положения. Крайне важно понять эти требования еще до начала проекта.

Проблемы кибербезопасности

Для анализа проблем кибербезопасности, с которыми сталкиваются компании в настоящее время, необходимо получить реальные данные и доказательства того, что в настоящее время происходит на рынке. Не во всех отраслях будут одинаковые проблемы в области кибербезопасности. По этой причине мы перечислим угрозы, которые по-прежнему наиболее распространены в различных отраслях. Это кажется самым подходящим подходом для аналитиков кибербезопасности, не специализирующихся на определенных отраслях, но в какой-то момент своей карьеры им, возможно, придется иметь дело с определенной отраслью, с которой они не очень знакомы.

Старые методы и более широкие результаты

Согласно отчету о глобальных рисках в сфере IT от лаборатории Касперского за 2016 г. (14), основные причины наиболее дорогостоящих утечек данных связаны со старыми атаками, которые развиваются с течением времени в следующем порядке:

- вирусы, вредоносные программы и трояны;
- недостаток усердия и неподготовленность сотрудников;
- фишинг и социальная инженерия;
- целевая атака;
- программы-вымогатели.

Хотя первые три в этом списке – старые знакомые и хорошо известны в сообществе кибербезопасности, они все еще преуспевают и по этой причине являются частью текущих проблем. Настоящая проблема состоит в том, что обычно они связаны с человеческими ошибками. Как объяснялось ранее, все может начинаться с фишингового сообщения по электронной почте, использующего социальную инженерию, чтобы заставить сотрудника щелкнуть ссылку, которая может загрузить вирус, вредоносное ПО или троян. В последнем предложении мы рассмотрели всех троих в одном сценарии.

Термин *целевая атака* (или продвинутая постоянная угроза) иногда не слишком понятен отдельным лицам, но есть некоторые ключевые атрибуты, которые могут помочь вам определить этот тип атаки. Первый и самый важный атрибут заключается в том, что у злоумышленника есть конкретная цель, когда он или она начинает составлять план атаки. Во время этой начальной фазы злоумышленник потратит много времени и ресурсов на проведение публичной разведки для получения информации, необходимой для осуществления атаки. Мотивом для этой атаки обычно является эксфильтрация данных, другими словами, их кража. Еще один атрибут этого типа атаки – срок службы или период времени, в течение которого они поддерживают постоянный доступ к сети цели. Намерение злоумышленника состоит в том, чтобы продолжать дальнейшее распространение по сети, взламывая различные системы, пока цель не будет достигнута.

Одна из самых больших проблем в этой области – идентификация злоумышленника, когда он уже находится в сети. Традиционных систем обнаружения, таких как **системы обнаружения вторжений** (IDS), может быть недостаточно для оповещения о подозрительных действиях, особенно при шифровании трафика. Многие специалисты уже отмечали, что между проникновением и обнаружением может пройти до 229 дней (15). Сокращение этого разрыва, безусловно, является одной из важнейших задач для специалистов в области кибербезопасности.

Программы-вымогатели – это новые и растущие угрозы, которые создают совершенно новый уровень проблем для организаций и специалистов по кибербезопасности. В мае 2017 г. мир был потрясен крупнейшей в истории атакой с использованием программы-вымогателя под названием Wannacry. Вирус эксплуатировал известную уязвимость в Windows, SMBv1, исправление для которой было выпущено в марте 2017 г. (за 59 дней до атаки) в бюллетене MS17-010 (16). Злоумышленники использовали эксплойт EternalBlue, выпущенный в апреле 2017 г. хакерской группой Shadow Brokers. Согласно MalwareTech (18), этот вымогатель заразил свыше 400 000 компьютеров по всему миру. Это гигантская цифра, которой никогда не наблюдалось в подобных атаках. Один из уроков, извлеченных в ходе этой атаки, заключался в том, что компаниям по всему миру по-прежнему не удается внедрить эффективную программу управления уязвимостями, о чем мы более подробно расскажем в главе 15 «Управление уязвимостями».

Очень важно отметить, что фишинговые письма по-прежнему являются средством доставки номер один для программ-вымогателей, а это означает, что мы снова возвращаемся к тому же циклу обучения пользователя, чтобы снизить вероятность успешной эксплуатации человеческого фактора с помощью социальной инженерии и иметь жесткие технические средства контроля безопасности для защиты от угроз и их обнаружения.

Изменение ландшафта угроз

В 2016 г. также получила широкую известность новая волна атак, когда компания «CrowdStrike» сообщила, что идентифицировала двух отдельных противников, связанных с российской разведкой, присутствующих в сети **Демократического национального комитета** США (DNC) (19). Согласно отчету, компания обнаружила доказательства того, что в сети DNC были две русские хакерские группы: Cozy Bear (также классифицированная как APT29) и Fancy Bear (APT28). Cozy Bear не был новым субъектом в этом типе атаки, т. к. доказательства показали, что в 2015 г. (20) они стояли за атакой на систему электронной почты Пентагона посредством фишинговых атак.

Этот тип сценария называется кибератаками, спонсируемыми правительством, но некоторые специалисты предпочитают изъясняться более общими терминами и называют их *данными, используемыми в качестве оружия*, поскольку их цель состоит в том, чтобы украсть информацию, которая может

быть использована против скомпрометированной стороны. Частный сектор не должен игнорировать эти признаки.

В настоящее время непрерывный мониторинг безопасности должен использовать как минимум три метода, показанных на рис. 1.4.

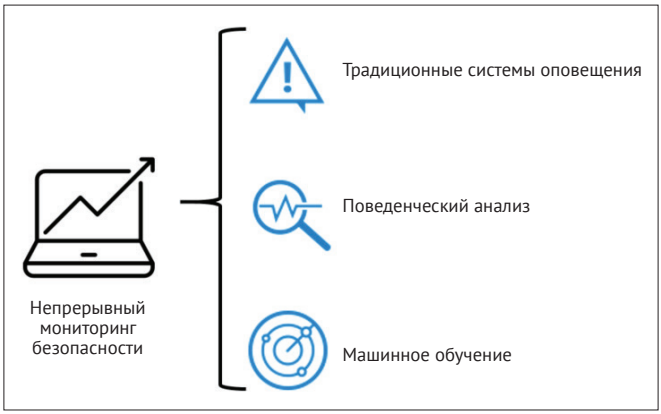

Рис. 1.4

Это только одна из причин, по которой организации начинают вкладывать больше средств в анализ угроз, машинное обучение и аналитику для защиты своих ресурсов. Мы рассмотрим это более подробно в главе 12 «Кибербразведка».

Улучшение стратегии безопасности

Если вы внимательно прочитаете всю эту главу, то совершенно четко поймете, что нельзя использовать старый подход к безопасности в противостоянии сегодняшним вызовам и угрозам. По этой причине важно убедиться, что ваша система безопасности готова справиться с этими проблемами. Для этого вы должны укрепить текущую систему защиты на разных устройствах независимо от форм-фактора.

Также важно, чтобы IT-отделы и службы безопасности могли быстро идентифицировать атаку, улучшив систему обнаружения. И последнее, но не менее важное: необходимо сократить время между заражением и сдерживанием, быстро реагируя на атаку путем повышения эффективности процесса реагирования.

Исходя из этого, можно с уверенностью сказать, что стратегия безопасности состоит из трех основных столпов, как показано на рис. 1.5.

Эти столпы нужно укреплять, и если в прошлом большая часть бюджета направлялась на защиту, то теперь существует еще большая необходимость распределять эти инвестиции и объем работ по другим областям. Эти инвестиции не относятся исключительно к техническому контролю безопасности, они так-

же должны осуществляться в других сферах бизнеса, включая административный контроль.

Рис. 1.5

Рекомендуется выполнить самопроверку, чтобы определить пробелы в каждом столпе с инструментальной точки зрения. Многие компании развивались с течением времени и никогда не обновляли свои средства безопасности, чтобы приспособиться к новой среде угроз и тому, как злоумышленники эксплуатируют уязвимости.

Компания, где большое внимание уделяется вопросам безопасности, не должна быть частью ранее упомянутой статистики (229 дней между проникновением и обнаружением). Этот разрыв должен быть резко сокращен, а ответ должен быть немедленным. Чтобы достичь этого, нужно разработать процесс реагирования на инциденты с использованием передовых и современных инструментальных средств, которые могут помочь инженерам по безопасности исследовать связанные с безопасностью проблемы. В главе 2 «Процесс реагирования на компьютерные инциденты» будет более подробно рассказано о реагировании на компьютерные инциденты, а глава 13 «Расследование инцидента» расскажет о тематических исследованиях, связанных с текущими расследованиями в области безопасности.

Красная и Синяя команды

Понятие «Красная/Синяя команда» (Red/Blue Team) не является чем-то новым. Первоначальная концепция была введена во время Первой мировой войны и, как и многие термины, используемые в информационной безопасности, появилась в армии. Общая идея заключалась в том, чтобы продемонстрировать эффективность нападения посредством симуляции.

Например, в 1932 г. контр-адмирал Гарри Э. Ярнелл продемонстрировал эффективность нападения на Перл-Харбор. Девять лет спустя, когда японцы напали на Перл-Харбор, можно было сравнить оба нападения и увидеть, насколько похожая тактика использовалась (22).

Эффективность симуляций, основанных на реальной тактике, которая может быть использована противником, хорошо известна и применяется в армии. Университет иностранных военных и культурных исследований проводит специализированные курсы только для подготовки участников и руководителей Красной команды (23). Хотя концепция чтения электронных сообщений в армии шире, интеллектуальная поддержка посредством эмуляции угроз похожа на то, что пытается сделать Красная команда. **Программа учений и оценки национальной безопасности** (**HSEEP**) (24) также использует Красные команды во время упражнений по предотвращению, чтобы отслеживать, как движутся противники, и создавать контрмеры на основе результатов этих учений.

В области кибербезопасности принятие подхода «Красная команда» также помогло организациям обеспечить безопасность своих ресурсов. Красная команда должна состоять из высококвалифицированных специалистов с разными наборами навыков, причем они должны быть полностью осведомлены о существующем ландшафте угроз для отрасли организации. Команда должна быть в курсе тенденций, а также ей необходимо понимать, как происходят текущие атаки. В некоторых обстоятельствах и в зависимости от требований организации члены Красной команды должны обладать навыками кодирования, чтобы создать свой собственный эксплойт и настроить его для более эффективной эксплуатации соответствующих уязвимостей, которые могут затронуть организацию.

Основной рабочий процесс Красной команды осуществляется с использованием подхода, показанного на рис. 1.6.

Красная команда осуществит атаку и проникнет в среду, пытаясь прорвать текущие средства контроля безопасности, известные как тестирование проникновения. Цель миссии – найти уязвимости и эксплуатировать их для получения доступа к ресурсам компании. Фаза атаки и проникновения обычно следует подходу корпорации «Lockheed Martin», опубликованному в докладе *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains* (25). Мы обсудим kill chain более подробно в главе 3 «Жизненный цикл атаки».

Красная команда также несет ответственность за регистрацию своих основных показателей, которые очень важны для бизнеса. Основные показатели выглядят так:

- **среднее время компрометации** (отсчет начинается с минуты, когда Красная команда начала атаку, до того момента, когда она смогла успешно скомпрометировать объект);
- **среднее время повышения привилегий** (начинается в той же точке, что и предыдущий показатель, но идет до момента полной компрометации, и именно в этот момент Красная команда получает административные привилегии для цели).

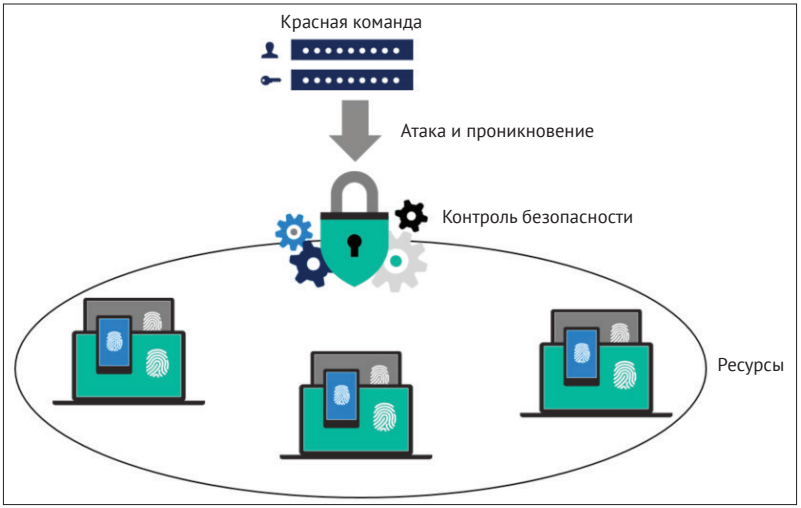

Рис. 1.6

До сих пор мы обсуждали возможности Красной команды, но упражнение считается выполненным не до конца без встречного партнера, Синей команды. Синей команде необходимо обеспечить безопасность ресурсов, и в том случае, если Красная команда обнаружит уязвимость и будет ее эксплуатировать, ей нужно быстро исправить сей факт и задокументировать как часть выводов.

Ниже приведены примеры задач, выполняемых Синей командой, когда злоумышленник (в данном случае Красная команда) может скомпрометировать систему:

- **сохранение улик** (обязательно сохраняйте свидетельства этих инцидентов, чтобы у вас была реальная информация для анализа, рационализации и принятия мер по нейтрализации угроз в будущем);
- **проверка улик** (не каждое отдельное оповещение, или в данном случае улика, приведет вас к действительной попытке взломать систему. Но если это произойдет, необходимо каталогизировать это как **индикатор компрометации**);
- **привлекайте тех, кого необходимо** (на данном этапе Синяя команда должна знать, что делать с этим индикатором и какая команда должна быть в курсе этой компрометации. Привлеките все соответствующие команды, которые могут варьироваться в зависимости от организации);
- **сортировка по инциденту** (иногда Синей команде может потребоваться содействие правоохранительных органов или ордер для проведения дальнейшего расследования, правильная сортировка поможет в этом процессе);
- **охват нарушения** (на данный момент у Синей команды достаточно информации, чтобы охватить нарушение);

- **создание плана исправления** (Синяя команда должна составить план исправления, чтобы изолировать или выгнать противника);
- **выполнение плана** (после того как план будет готов, Синей команде необходимо осуществить его и выполнить восстановление после нарушения).

Члены Синей команды также должны обладать широким набором навыков и состоять из профессионалов из разных отделов. Помните, что в некоторых компаниях существует Красная/Синяя команда специального назначения, а в других – нет. Компании собирают эти команды только во время учений. Как и Красная, Синяя команда также несет ответственность за показатели безопасности, которые в данном случае не являются точными на 100 %. Причина, по которой это произошло, заключается в следующем: реальность такова, что Синяя команда может не знать точно, в какое время Красная команда смогла скомпрометировать систему. При этом оценка для данного вида упражнений уже достаточно хороша. Эти оценки самоочевидны, как видно из следующего списка:

- расчетное время до обнаружения;
- расчетное время до восстановления.

Работа Синей и Красной команд не заканчивается, если Красной команде удается скомпрометировать систему. На этом этапе предстоит еще много работы, что потребует полного сотрудничества между этими командами. Должен быть создан окончательный отчет, чтобы выделить детали относительно того, как произошло нарушение, предоставить документированный график атаки, подробности уязвимостей, которые подверглись эксплуатации для получения доступа и повышения привилегий (если это применимо), и определить влияние бизнеса на компанию.

Подразумеваем взлом

В связи с возникающими угрозами и проблемами в области кибербезопасности необходимо было изменить методологию, перейдя с модели «предотвратить взлом» (prevent breach) на модель «подразумевать взлом» (assume breach). Традиционный подход «предотвратить взлом» сам по себе не способствует непрерывному тестированию, и для борьбы с современными угрозами всегда нужно совершенствовать свою защиту. По этой причине принятие данной модели в области кибербезопасности было естественным шагом.

Во время интервью в 2012 г. бывший директор ЦРУ и Агентства национальной безопасности в отставке генерал Майкл Хейден сказал (26):

> *«По сути, если кто-то хочет войти, он входит. Ладно, хорошо. Примите это».*

Многие не совсем поняли, что он на самом деле имел в виду, но это высказывание является основой подхода «assume breach». Эта модель проверяет средства защиты, обнаружения и реагирования, чтобы убедиться, что они реа-

лизованы должным образом. Но для того, чтобы ввести все это в действие, становится жизненно важным использование упражнений для Красной и Синей команд с целью симуляции атак на собственную инфраструктуру и тестирования средств контроля безопасности компании, сенсоров и процесса реагирования на инциденты.

На рис. 1.7 показан пример взаимодействия фаз в упражнении для Красной и Синей команд.

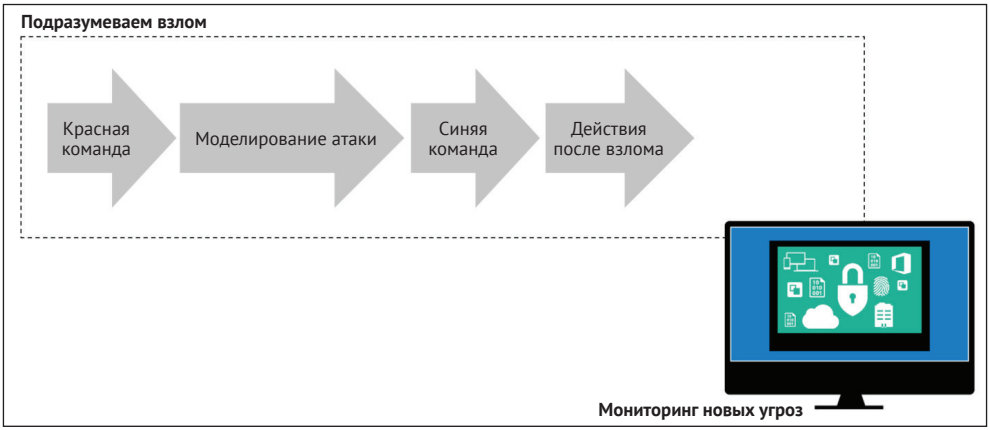

Рис. 1.7

На этапе действий после взлома Красная и Синяя команды будут работать сообща для подготовки окончательного отчета. Важно подчеркнуть, что это должно быть не одноразовым упражнением, а непрерывным процессом, который будет дорабатываться и совершенствоваться с течением времени, используя передовой опыт.

Справочные материалы

Можно ознакомиться с материалами, доступными по приведенным ниже ссылкам:

1. **https://www.darkreading.com/attacks-breaches/new-iot-botnet-discovered-120k-ip-cameras-at-risk-of-attack/d/d-id/1328839**.
2. **https://www.welivesecurity.com/2014/11/11/website-reveals-73000-unprotected-security-cameras-default-passwords/**.
3. **https://threatpost.com/20-linksys-router-models-vulnerable-to-attack/125085/**.
4. **https://www.nytimes.com/2017/02/15/us/remote-workers-work-from-home.html**.
5. Ознакомьтесь с независимыми от поставщиков инструкциями по внедрению BYOD, опубликованными в ISSA Journal: **https://blogs.technet.microsoft.com/yuridiogenes/2014/03/11/byod-article-published-at-issa-journal/**.

6. **https://www.csoonline.com/article/3154714/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html**.
7. **http://blog.trendmicro.com/ransomware-growth-will-plateau-in-2017-but-attack-methods-and-targets-will-diversify/**.
8. Прочтите эту статью для получения дополнительной информации об опасных аспектах использования одного и того же пароля для разных учетных записей: **https://www.telegraph.co.uk/finance/personalfinance/bankaccounts/12149022/Use-the-same-password-for-everything-Youre-fuelling-a-surge-in-current-account-fraud.html**.
9. Загрузите отчет с сайта **https://enterprise.verizon.com/resources/reports/dbir/**.
10. Узнайте больше о Security Development Lifecycle на странице **https://www.microsoft.com/en-us/securityengineering/sdl/**.
11. Сведения о Microsoft Office 365 Security and Compliance можно найти по адресу **https://docs.microsoft.com/ru-ru/office365/securitycompliance/go-to-the-securitycompliance-center?redirectSourcePath=%252fen-us%252farticle%252fOffice-365-Security-Compliance-Center-7e696a40-b86b-4a20-afcc-559218b7b1b8**.
12. **https://downloads.cloudsecurityalliance.org/initiatives/surveys/capp/Cloud_Adoption_Practices_Priorities_Survey_Final.pdf**.
13. **http://www.kasperskyreport.com/?gclid=CN_89N2b0tQCFQYuaQodAQoMYQ**.
14. Можно скачать отчет на странице **http://www.kasperskyreport.com/?gclid=CN_89N2b0tQCFQYuaQodAQoMYQ**.
15. **https://info.microsoft.com/ME-Azure-WBNR-FY16-06Jun-21-22-Microsoft-Security-Briefing-Event-Series-231990.html?ls=Social**.
16. Прочтите бюллетень Microsoft для получения дополнительной информации: **https://www.microsoft.com/en-us/msrc?rtc=1**.
17. Прочтите статью для получения дополнительной информации об этой группе: **https://www.symantec.com/connect/blogs/equation-has-secretive-cyber espionage-group-been-breached**.
18. **https://twitter.com/MalwareTechBlog/status/865761555190775808**.
19. **https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/**.
20. **https://www.cnbc.com/2015/08/06/russia-hacks-pentagon-computers-nbc-citing-sources.html**.
21. **https://www.theverge.com/2017/5/17/15655484/wannacry-variants-bitcoin-monero-adylkuzz-cryptocurrency-mining**.
22. **https://www.quora.com/Could-the-attack-on-Pearl-Harbor-have-been-prevented-What-actions-could-the-US-have-taken-ahead-of-time-to-deter-dissuade-Japan-from-attacking#!n=12**.
23. Можно скачать руководство Red Team по адресу **http://usacac.army.mil/sites/default/files/documents/ufmcs/The_Applied_Critical_Thinking_Handbook_v7.0.pdf**.
24. **https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf**.

25. Загрузите статью на странице **https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf**.
26. **http://www.cbsnews.com/news/fbi-fighting-two-front-war-on-growing-enemy-cyber-espionage/**.

Резюме

В этой главе вы узнали больше о текущем ландшафте угроз и о том, как эти новые угрозы используются для компрометации различных типов данных, включая учетные, и приложений. Во многих сценариях используются старые методы взлома, такие как фишинговые письма, но с более сложным подходом. Вы также познакомились с реальностью, касающейся общенационального типа угроз и правительственных атак. Чтобы защитить свою организацию от новых угроз, вы узнали о ключевых факторах, которые могут помочь вам повысить уровень безопасности. Важно, чтобы часть этого усовершенствования переключала внимание с защиты только на обнаружение и реагирование. Для этого использование Красной и Синей команд становится обязательным условием. То же самое относится и к подходу «assume breach».

В следующей главе вы продолжите изучать, как улучшить свою безопасность. Тем не менее эта глава будет посвящена процессу реагирования на компьютерные инциденты. Этот процесс имеет первостепенное значение для компаний, которым необходимы передовые методы обнаружения и реагирования на киберугрозы.