

# Содержание

<b>Об авторах .....</b>	11
<b>О рецензентах .....</b>	12
<b>Предисловие .....</b>	13
<b>Глава 1. Стратегия безопасности .....</b>	17
Текущий ландшафт киберугроз .....	17
Учетные данные – аутентификация и авторизация .....	20
Приложения .....	21
Данные .....	23
Проблемы кибербезопасности .....	24
Старые методы и более широкие результаты .....	24
Изменение ландшафта угроз .....	25
Улучшение стратегии безопасности .....	26
Красная и Синяя команды .....	27
Подразумеваем взлом .....	30
Справочные материалы .....	31
Резюме .....	33
<b>Глава 2. Процесс реагирования на компьютерные инциденты .....</b>	34
Процесс реагирования на компьютерные инциденты .....	34
Причины иметь в своем распоряжении процесс реагирования на компьютерные инциденты .....	35
Создание процесса реагирования на компьютерные инциденты .....	37
Команда реагирования на компьютерные инциденты .....	39
Жизненный цикл компьютерного инцидента .....	40
Обработка инцидента .....	40
Передовые методы оптимизации обработки компьютерных инцидентов .....	43
Деятельность после инцидента .....	44
Реальный сценарий .....	44
Выводы .....	45
Реагирование на компьютерные инциденты в облаке .....	46
Обновление процесса реагирования, чтобы включить облако .....	47
Справочные материалы .....	48
Резюме .....	48

<b>Глава 3. Жизненный цикл атаки .....</b>	50
Внешняя разведка.....	50
Сканирование .....	51
Доступ и повышение привилегий .....	61
Вертикальное повышение привилегий .....	62
Горизонтальное повышение привилегий.....	63
Проникновение и утечки .....	63
Тыловое обеспечение .....	64
Штурм .....	65
Обфускация .....	66
Управление жизненным циклом угроз.....	67
Справочные материалы .....	70
Резюме.....	72
<b>Глава 4. Разведка и сбор данных.....</b>	73
Внешняя разведка.....	73
Копание в мусоре.....	73
Социальные сети .....	74
Социальная инженерия.....	75
Внутренняя разведка.....	82
Анализ трафика и сканирование.....	83
Вардрайвинг.....	89
Завершая эту главу .....	91
Справочные материалы .....	92
Резюме.....	93
<b>Глава 5. Компрометация системы.....</b>	94
Анализ современных тенденций.....	94
Вымогательство .....	95
Манипулирование данными.....	96
Атаки на IoT-устройства.....	97
Бэкдоры .....	98
Атаки на мобильные устройства .....	99
Взлом повседневных устройств.....	99
Взлом облака.....	100
Фишинг.....	102
Эксплуатация уязвимостей.....	104
Уязвимость нулевого дня .....	104
Фаззинг.....	105
Анализ исходного кода.....	105
Типы экспloitов нулевого дня .....	106
Перезапись структурированного обработчика исключений.....	107

---

Выполнение шагов, направленных на компрометацию системы .....	107
Развертывание полезных нагрузок.....	108
Компрометация операционных систем.....	111
Компрометация удаленной системы .....	114
Компрометация веб-приложений.....	116
Справочные материалы .....	118
Резюме.....	120
<b>Глава 6. Охота на пользовательские реквизиты.....</b>	<b>121</b>
Реквизиты доступа – новый периметр .....	121
Стратегии компрометации реквизитов доступа пользователя .....	124
Получение доступа к сети .....	125
Сбор учетных данных.....	126
Взлом реквизитов доступа пользователя .....	128
Полный перебор .....	128
Социальная инженерия.....	130
Атака Pass-the-hash .....	136
Другие способы взлома реквизитов доступа.....	139
Справочные материалы .....	139
Резюме.....	139
<b>Глава 7. Дальнейшее распространение по сети .....</b>	<b>141</b>
Инфильтрация .....	142
Построение карты сети .....	142
Избежать оповещений .....	143
Дальнейшее распространение .....	144
Сканирование портов .....	144
Sysinternals .....	145
Общие файловые ресурсы.....	147
Удаленный доступ к рабочему столу.....	148
PowerShell.....	150
Инструментарий управления Windows.....	150
Запланированные задачи .....	151
Кражा авторизационных токенов .....	153
Атака Pass-the-hash .....	153
Active Directory.....	154
Удаленный доступ к реестру .....	155
Анализ взломанных хостов .....	155
Консоли центрального администратора.....	156
Кражा сообщений электронной почты .....	156
Справочные материалы .....	156
Резюме.....	157

<b>Глава 8. Повышение привилегий .....</b>	158
Инфильтрация .....	158
Горизонтальное повышение привилегий.....	159
Вертикальное повышение привилегий .....	159
Как избежать оповещений .....	160
Выполнение повышения привилегий.....	161
Эксплуатация неисправленных операционных систем .....	162
Манипулирование маркерами доступа .....	163
Эксплуатация специальных возможностей.....	164
Application Shimming.....	165
Обход контроля над учетной записью пользователя.....	169
Внедрение DLL-библиотек .....	170
Перехват порядка поиска DLL .....	172
Перехват поиска dylib.....	172
Исследование уязвимостей.....	173
Запускаемые демоны .....	174
Практический пример повышения привилегий в Windows 8.....	175
Выводы .....	176
Справочные материалы .....	177
Резюме.....	178
<b>Глава 9. Политика безопасности .....</b>	179
Проверка политики безопасности.....	179
Обучение конечного пользователя .....	181
Рекомендации по безопасности для пользователей социальных сетей ....	182
Тренинг по безопасности.....	183
Использование политики.....	183
Белый список приложений .....	185
Усиление защиты.....	187
Мониторинг на предмет соответствия.....	191
Справочные материалы .....	195
Резюме.....	195
<b>Глава 10. Сегментация сети .....</b>	197
Глубоко эшелонированная защита.....	197
Инфраструктура и службы .....	198
Документы в процессе передачи.....	199
Конечные точки .....	201
Сегментация физической сети .....	201
Открывая схему сети .....	203
Обеспечение удаленного доступа к сети .....	206
VPN типа «сеть–сеть» .....	207
Сегментация виртуальной сети.....	208

---

Безопасность гибридной облачной сети.....	210
Справочные материалы .....	212
Резюме .....	213
<b>Глава 11. Активные сенсоры .....</b>	<b>214</b>
Возможности обнаружения.....	214
Индикаторы компрометации .....	216
Системы обнаружения вторжений .....	218
Система предотвращения вторжений.....	219
Обнаружение на основе правил .....	220
Обнаружение на основе аномалий.....	221
Поведенческая аналитика внутри организации .....	221
Размещение устройств.....	226
Поведенческая аналитика в гибридном облаке .....	226
Центр безопасности Azure .....	226
Справочные материалы .....	232
Резюме .....	232
<b>Глава 12. Киберразведка .....</b>	<b>233</b>
Введение в киберразведку .....	233
Инструментальные средства киберразведки с открытым исходным кодом .....	237
Средства киберразведки компании Microsoft .....	242
Центр безопасности Azure .....	242
Использование киберразведки для расследования подозрительной деятельности.....	245
Справочные материалы .....	248
Резюме.....	248
<b>Глава 13. Расследование инцидента .....</b>	<b>249</b>
Масштаб проблемы .....	249
Ключевые артефакты .....	250
Исследование скомпрометированной системы внутри организации .....	255
Исследование скомпрометированной системы в гибридном облаке .....	259
Ищите и обрящете .....	266
Выводы .....	267
Справочные материалы .....	268
Резюме.....	268
<b>Глава 14. Процесс восстановления .....</b>	<b>269</b>
План послеаварийного восстановления .....	269
Процесс планирования послеаварийного восстановления.....	270
Вызовы .....	274

Восстановление без перерыва в обслуживании .....	274
Планирование на случай непредвиденных обстоятельств.....	276
Процесс планирования на случай непредвиденных обстоятельств в сфере ИТ.....	277
Передовые методы восстановления.....	282
Справочные материалы .....	283
Резюме.....	283
<b>Глава 15. Управление уязвимостями.....</b>	<b>285</b>
Создание стратегии управления уязвимостями .....	285
Инвентаризация ресурсов .....	286
Управление информацией.....	286
Оценка рисков .....	288
Оценка уязвимостей.....	290
Отчеты и отслеживание исправлений .....	291
Планирование реагирования.....	292
Инструменты управления уязвимостями.....	293
Реализация управления уязвимостями .....	300
Передовые методы управления уязвимостями.....	302
Реализация управления уязвимостями с помощью Nessus .....	304
Flexera (Secunia) Personal Software Inspecto .....	310
Заключение .....	312
Справочные материалы .....	313
Резюме.....	314
<b>Глава 16. Анализ журналов.....</b>	<b>315</b>
Сопоставление данных.....	315
Журналы операционной системы .....	316
Журналы Windows .....	317
Журналы Linux .....	320
Журналы брандмауэра .....	320
Журналы веб-сервера .....	322
Справочные материалы .....	323
Резюме .....	323
<b>Предметный указатель .....</b>	<b>324</b>

# 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 помошь 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 ИТ-индустрии. Является лицензированным специалистом по тестированию 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 ИТ-специалистов, которые хотят узнать больше о кибербезопасности.

## О чём 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 «Киберразведка» рассказывается о различных аспектах киберразведки, 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\\_ColrImages.pdf](http://www.packtpub.com/sites/default/files/downloads/CybersecurityAttackandDefenseStrategies_ColrImages.pdf).

## Используемые условные обозначения

В этой книге используется ряд текстовых обозначений.

**Код в Тексте:** 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](http://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](mailto: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/](http://dmkpress.com/authors/publish_book/) или напишите в издательство по адресу [dmkpress@gmail.com](mailto:dmkpress@gmail.com).

## Скачивание исходного кода примеров

Скачать файлы с дополнительной информацией для книг издательства «ДМК Пресс» можно на сайте [www.dmkpress.com](http://www.dmkpress.com) или [www.dmk.ru](http://www.dmk.ru) 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](mailto: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 Packt 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](mailto: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 обеспечивают 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).

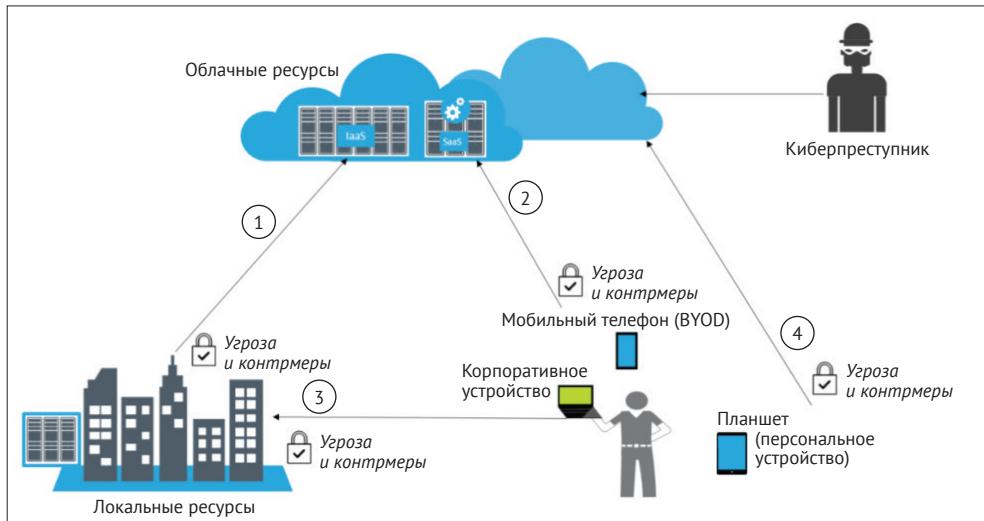


Рис. 1.1

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 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 нужнонейтрализовать, описан на рис. 1.3.

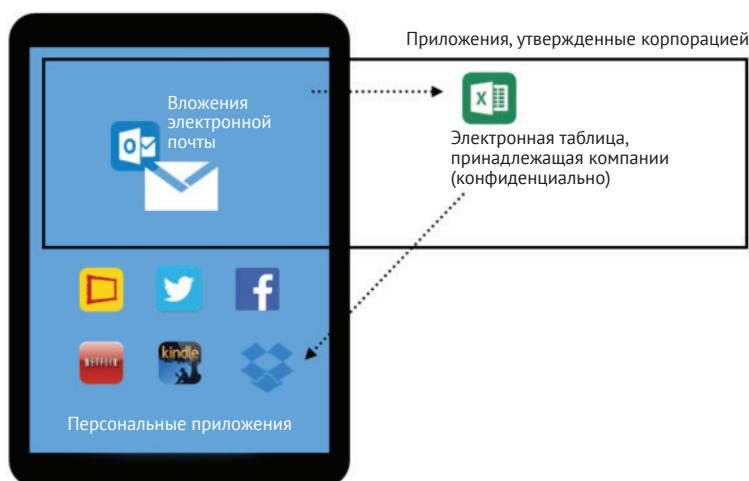


Рис. 1.3

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 по-средника 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, расположенному локально, либо в облаке (путь 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 путей передачи данных, соответствия, правил и положения. Крайне важно понять эти требования еще до начала проекта.

Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

[e-Univers.ru](http://e-Univers.ru)