

СН° 114227

D.K. Academy

НЕ СЕ ИЗНАСЯ

През очите на хакера

Второ преработено и
допълнено издание

ИЗДАТЕЛСТВО
АСЕНЕВЦИ

93580

004.056

- © D.K. Academy, 2024
- © Влади Владев, превод, 2024
- © Издателство Асеневици, 2024

ISBN: 978-619-266-045-1

инж. Ивелин Михайлов, редактор

Изданието като цяло, както и нито една част от него, не може да се възпроизвежда, съхранява или разпространява под каквато и да е форма, и по какъвто и да е начин, без изричното писмено съгласие от издателя. Някои от наименованията, споменати в книгата са запазени марки и принадлежат на техните собственици.

Изключване на гаранциите и ограничаване на отговорността:

Информацията в тази книга се разпространява на основа „такава, каквато е“ („as is“), без каквито и да било гаранции. Въпреки, че са взети всички необходими предпазни мерки при подготовката на тази книга, авторът и издателят не носят никаква отговорност спрямо което и да е физическо или юридическо лице за причинени или предполагаеми щети или вреди, възникнали пряко или косвено от инструкциите, съдържащи се в тази книга, или от компютърният софтуер или хардуер, описани в книгата.

2
27
70

133463

БИБЛИОТЕКА УНСС

Инв. №



120000133462

БИБЛИОТЕКА
УНСС
СОФИЯ

Съдържание

Въведение	8
Обзор на книгата	8
Аудитория.....	10

ЧАСТ 1. Защита на електронната поща

Глава 1. Средства и методи за защита на електронната поща ... 14

1.1. Криптографски методи. Симетрична и асиметрична криптография.....	14
1.2. Алгоритми за шифроване	15
1.3. Средства за защита на електронната поща	18
1.3.1. PGP.....	19
1.3.2. Стандартът S/MIME.....	21
1.3.3. Безопасни пощенски услуги. HushMail.....	22
1.3.4. Плъгини за браузъра	26
1.3.5. Плъгини за пощенските клиенти.....	28
1.4. Сравнение на средствата за защита. Избор на идеалното средство	29
1.4.1. Проблемът за избора.....	29
1.4.2. Изводи.....	34

Глава 2. Как да разбием електронна поща?..... 36

2.1. Троянски кон.....	36
------------------------	----

2.2. Разбиване чрез номера на телефона.....	41
2.3. Физически достъп до компютъра.....	43
2.4. Социално инженерство, или просто измама.....	46
2.5. Модерната дума "фишинг".....	47
2.6. Възстановяване паролата	52
2.7. Кражба на Cookies.....	52
2.8. XSS уязвимости	54
2.9. Метод на грубата сила	55

Глава 3. Защита на електронна поща..... 56

3.1. Малко теория. S/MIME, PKI и PGP.....	56
3.2. Как ще защитаваме пощата?	58
3.3. Използване на OpenSSL.....	59
3.4. Програмата OpenPGP. Шифроване на електронна поща с помощта на Gpg4win	61
3.5. Настройка на шифроване в Gmail	68

Глава 4. Електронен подпис..... 70

4.1. Какво е електронен подпис?	70
4.2. Случаи на използване на електронен подпис в малка компания.....	70

4.2.1. Вътрешен документооборот	70
4.2.2. Обмен на документи с филиали и партньори.....	72
4.2.3. Някои проблеми при внедряването на електронния подпис	72
4.3. Работа с електронен погнус посредством пощенски клиент.....	74
4.4. Работа с електронен погнус в Windows.....	75
4.5. Работа с цифров погнус в Linux.....	78

**ЧАСТ 2.
Месинджъри**

Глава 5. Избор на безопасен месинджър	84
5.1. Критерии за сравнение.....	84
5.2. Signal	86
5.3. Viber	88
5.4. Telegram	89
5.5. Whatsapp.....	91
5.6. Briar	92
5.7. Facebook messenger.....	93
5.8. Wire	94
5.9. Jabber.....	95
5.10. Riot Matrix.....	96
5.11. Status.....	97
5.12. Threema.....	99
5.13. Извогу	101

Глава 6. Как се разбива Telegram?	102
6.1. Начин за разбиване.....	102
6.2. Как може да се защитите от подобен вид Взлом?.....	104

Глава 7. Препоръки относно защитата на най-популярните месинджъри

7.1. Viber	106
7.1.1. Контролирайте устройствата	106
7.1.2. Деактивиране на акаунт... ..	106
7.1.3. Изчезващи съобщения по подразбиране	106
7.1.4. Включете двуфакторна верификация.....	108
7.1.5. Важни настройки за поверителност	108
7.1.5. Параметри на повикванията.....	109
7.2. WhatsApp.....	109
7.2.1. Списък с устройствата	109
7.2.2. Включете двуфакторната верификация	110
7.2.3. Изтриване на акаунт	110
7.2.4. Важни параметри за поверителност	110
7.3. Telegram	112
7.3.1. Списък с устройствата	112
7.3.2. Изтриване на акаунт	113
7.3.2. Параметри за поверителност	114
7.4. Изключваме геолокацията	114

**ЧАСТ 3.
Защита от разбиване на уеб и IP камера**

Глава 8. Практически пример за разбиване на IP камера	116
8.1. Няколко думи за разбиването на IP камери.....	116
8.2. Събиране на информация и инсталиране на програмното обезпечение	120

8.3. Последователност на действията за разбиването на камерата	121
8.4. Сканиране на диапазон с IP адреси.....	123
8.5. Получаване на списък с камери със стандартна парола	124
8.6. Презглеждане на видео от камери.....	124
Глава 9. Защита на камерата от взлом	127
9.1. Трябва ли да защитаваме камерата?	127
9.2. Откриване на взлом	128
9.3. Защита на камера с директна връзка към интернет	128
9.4. Защита на камери без пряка връзка до интернет.....	129
Глава 10. Защита на Wi-Fi	132
10.1. Защо трябва да защитаваме Wi-Fi?	132
10.2. Манипулации с името на мрежата	133
10.3. Тип безопасност.....	135
10.5. Задайте сложна парола за Wi-Fi	137
10.6. Обезопасяване на отдалечения достъп до рутера	138
10.7. Идентифицирайте всички Ваши клиенти	139
10.8. Гостуваща мрежа	141
10.9. Включване на VPN.....	142
10.10. Включване на защитната стена	142
10.11. Блокиране по MAC адрес.....	143
10.12. Обновявайте регулярно фърмуера на рутера.....	144

10.13. Някои не особено полезни съвети	144
----------------------------------------------	-----

ЧАСТ 4.

Защитаваме файловете на персоналния компютър

Глава 11. Избор на средства за защита на данните **146** |

11.1. Шифроване на диска.....	146
11.2. Криптирани контейнери или виртуални дискове	151
11.3. Прозрачно шифроване....	152

Глава 12. Шифроване със средствата на операционната система **154** |

12.1. Прозрачно шифроване посредством EFS.....	154
12.1.1. Предимства и недостатъци на EFS	154
12.1.2. Принцип на работа на EFS	157
12.1.3. Шифроване на файлове и папки	159
12.1.4. Работа със зашифровани файлове и папки.....	164
12.1.5. Настройка на политика за възстановяване.....	165
12.1.6. Архивиране на ключа за възстановяване	168
12.1.7. Възстановяване на достъпа до зашифрованите папки с помощта на агенти за възстановяване	170
12.2. Средство за шифроване на диска BitLocker	172
12.2.1. Какво е BitLocker?	172
12.2.2. Какво може да зашифровате и какво не?	173
12.2.3. Шифроване на диска.....	174

12.2.4. Работа с шифрован диск.....	181
12.2.5. Забравена парола. Какво да правим?.....	182
12.2.6. Нюанси при използването на BitLocker.....	182
12.3. Разбиване на EFS.....	187
12.4. Файлова система eCryptfs в Linux.....	187
12.4.1. Шифроване на папка.....	187
12.4.2. Съхраняваме паролата на флашка.....	190
12.5. Може ли да се доверим на стандартното шифроване?.....	192
Глава 13. Шифроване с външни програми.....	193
13.1. Избор на външна програма за шифроване.....	193
13.2. Запознаване с програмата VeraCrypt.....	194
13.3. Възможности на програмата.....	195
13.4. Използване на програмата.....	197
13.4.1. Инсталиране на програмата.....	197
13.4.2. Създаване на виртуален диск.....	198
13.4.3. Монтиране на контейнер.....	207
13.4.4. Шифроване на дял.....	209
13.5. Програмата CipherShed..	210
13.6. Шифроване на файлове за трансфер.....	211
13.7. Eraser: Изтриване на информация без възможност за възстановяване.....	212

Глава 14. Други инструменти за шифроване на файлове.....	214
14.1. Cryptomator.....	214
14.2. Duplicati.....	214
14.3. RClone.....	215
14.4. Kryptor.....	216
14.5. Dexios.....	216
14.6. Tomb.....	217
14.7. Picocrypt.....	217
14.8. Уебинтерфейси Hat.sh и Cloaker.....	218
14.9. zuluCrypt.....	218
14.10. SiriKali.....	219

ЧАСТ 5.

Защита на данните на мобилно устройство

Глава 15. Безопасност в iPhone ..	221
15.1. Актуализирайте.....	221
15.2. Изключваме контролния център.....	222
15.3. Включете сървиса Find My.....	223
15.4. Изключете предварителното преглеждане на съобщенията.....	223
15.5. Задайте сложна код-парола.....	224
15.6. Изключете Face ID в маска.....	225
15.7. Включете изтриването на данните.....	225
15.8. Включете двуфакторната авторизация.....	225
15.9. Включете сървиса Private Relay.....	226
15.10. Бележки с парола.....	228
15.11. Използвайте e-sim.....	228

Глава 16. Обзор на Android приложенията за шифроване на данни 230

- 16.1. Многообразие на избора 230
- 16.2. Приложения за шифроване на облак..... 230
- 16.3. Кратко описание на приложенията за шифроване231
- 16.4. Сравнение на приложенията за шифроване..... 233

Глава 17. Защита на предаваните по мрежата данни от подслушване236

- 17.1. Виртуална частна мрежа или VPN 236
 - 17.1.1. Защо е нужен VPN? 236
 - 17.1.2. Избор на VPN сървис 238
 - 17.1.3. Настройка на вградения VPN клиент..... 244
- 17.2. Проектът Tor 247
 - 17.2.1. Какво е Tor? 247
 - 17.2.2. Инсталиране на Tor на мобилно устройство..... 249
- 17.3. Кое е по-добре – VPN или Tor? 252

Глава 18. Защита на електронната поща. MailDroid 254

- 18.1. Необходими приложения 254

- 18.2. Настройка на Crypto Plugin..... 255
- 18.3. Настройка на MailDroid 258
- 18.4. След инсталиране на MailDroid..... 260

Глава 19. Защита на важни документи с помощта на криптиран контейнер.....261

- 19.1. Защо е необходима защита на данните на Android устройство?261
 - 19.1.1. Начини за защита на данните 261
 - 19.1.2. От кого защитаваме данните? 261
 - 19.1.3. Блокиране стартирането на приложения и забрана за разглеждане на галерията ... 263
- 19.2. Шифроване на цялото устройство..... 265
- 19.3. Избор на Android приложение за работа с криптирани данни..... 266
- 19.4. Приложението EDS Lite 268

Заклучение271

