Содержание

Предисловие 19

Глава 1. Электронная коммерция и принципы информационной безопасности 21

Введение 22

Безопасность как фундамент системы 23

Конфиденциальность 23

Целостность 24

Доступность 24

Безопасность – не просто звучное слово 26

Цели безопасности в системах электронной коммерции 28

Разрабатывая систему, думайте о безопасности 29

Обеспечение безопасности на стадии разработки системы 31

Воплощение решений безопасности 33

Управление информационными системами в защищенном режиме 34

Защита систем, находящихся в эксплуатации 38

Все начинается с риска 39

Внесение изменений в систему 41

Регулирование расходов на безопасность 44

Метод эталона 45

Метод оказания давления 49

Ограничивающие свойства защиты 52

Способствующие свойства защиты 53

Резюме 55

Понятие целей безопасности в контексте коммерческой деятельности

- Защита конфиденциальной информации клиента в момент совершения покупки.
- Защита клиентской информации во время хранения и обработки.
- Обеспечение безопасности покупателей, поставщиков и персонала организации.
- Предотвращение мошенничества, организационная защита от злоупотреблений и излишних расходов.
- Защита информационных активов от несанкционированного доступа и раскрытия третьим лицам.
- Сохранение целостности информационных активов предприятия.
- Обеспечение доступности систем и процессов, необходимых в работе с клиентами и партнерами.

Конспекты 56
Часто задаваемые вопросы 59

Разделы «Безопасный совет» содержат дополнительные данные о способах снижения информационных рисков

Безопасный совет: Управление конфигурациями

Изменение конфигурации ключевых устройств, таких как маршрутизатор или сервер, может кардинальным образом отразиться на степени, в которой ваш сайт подвержен угрозе DoS-нападения. Таблицы маршрутизации, реестры, конфигурационные базы данных и conf-файлы – вот неполный список рычагов изменения параметров системы и ее окружения. Стоит ли говорить о том, что все устройства, подключающиеся к Internet, должны тщательным образом контролироваться на предмет изменения их параметров. Кроме того, администратор всегда должен иметь под рукой резервные копии безопасных и проверенных на практике конфигураций.

Глава 2. Распределенная атака «отказ в обслуживании». Цели, средства нападения и методы защиты 61

Введение 62
Что такое распределенная атака 63
Все начинается с DoS 63
Анатомия распределенной атаки «отказ в обслуживании» 73
Атаки февраля 2000 года 76
DDoS и сайты электронной коммерции 79
Проблемы роста 80
Проблемы СМИ 80
Хакер и мотивы, приводящие к взлому коммерческих систем 81
Этика взлома или путаница в терминологии? 81
Хактивизм 83
Пятнадцать минут славы 83
Нет ничего страшнее униженного хакера 84
Деньги 84
Злой умысел 85
Средства осуществления DDoS-атаки 85
Trinoo 86
Портативный монстр TFN2K 88
Stacheldraht 90
Другие разновидности DDoS-систем 95
Защита сайта от распределенного нападения 95
Основные методы защиты 97
Резюме 111
Конспекты 112
Часто задаваемые вопросы 117

Ошибки HTML-программирования

В HTML-формах могут использоваться скрытые метки, содержащие название и значение параметра. После заполнения формы эти данные передаются программе-обработчику. К примеру, следующая строчка обозначает параметр «цена» величиной $100:

```
<input type=hidden
name="cost"
value="100.00">
```

Хакер, используя простой текстовый редактор, может заменить это значение, скажем, на $1. Это позволит ему купить товар гораздо дешевле.

Глава 3. Разработка защищенного Web-сайта 119

Введение 120

Выбор Web-сервера 120
- Web-сервер или Web-сервис 121
- Поддерживаемые платформы и цены 122
- Сравнение защитных свойств Web-серверов 124

Основы разработки защищенного сайта 136
- Создание плана безопасности 136
- Внедрение слоя безопасности, закрывающего Web-сервер 139
- Apache или Internet Information Services 141
- Установка сервера 143
- Повышение надежности сервера 156
- Укрепление всей системы 158
- Вскрытие и аудит паролей 160
- Проблемы разработки, связанные с HTML 163

Введение в Java, JavaScript и ActiveX 167
- Проблемы, связанные с применением Java, JavaScript и ActiveX 167
- Предупреждение атак с использованием Java, JavaScript и ActiveX 169

Программирование защищенных скриптов 171

Программные подписи: проблема или решение 173
- Коротко о программных подписях 174

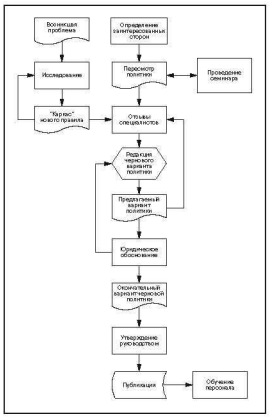
Аутсорсинг работ по созданию сайта 176
- Определение необходимых знаний 177
- Достоинства и недостатки аутсорсинга 178
- Проверьте выполненную работу перед тем, как ввести сайт в эксплуатацию 180

Резюме 182

Конспекты 182

Часто задаваемые вопросы 186

Создание политики сетевой безопасности



Глава 4. Разработка и внедрение политики сетевой безопасности 189

Введение 190

Зачем нужна политика безопасности 190

Что такое политика сетевой безопасности 191

Из чего состоит политика безопасности 197

Политика конфиденциальности и приватности 198

Политика целостности информации 206

Политика гарантии качества 207

Политика доступности 210

Можно ли найти в сети готовую политику безопасности? 211

Разные организации – разные политики безопасности 212

Примеры и структура политики безопасности 212

Несколько слов о привлечении специалистов со стороны 213

Использование политики безопасности в реализации технических решений 214

Как ознакомить клиентов с политикой безопасности 216

Получение доверия путем огласки данных 217

Резюме 219

Конспекты 219

Часто задаваемые вопросы 222

Глава 5. Реализация защищенного сайта электронной коммерции 225

Введение 226

Компоненты коммерческого сайта 226

Создание зон безопасности 227

Зоны демилитаризации 229

Дополнительные потребности – новые зоны безопасности 231

Многозональные сети

Глава 5 отвечает на вопросы, которые могут возникнуть при разработке защищенного сайта

Вопрос: Как определить нужное количество информации, заносимой в протоколы событий?
Ответ: Протоколируйте то, что помогает принимать решения. Если возникают проблемы с выявлением нужной информации, постарайтесь сократить количество протоколируемых событий или используйте автоматизированные средства анализа. Как правило, если вы не имеете четкого представления о поведении систем и пользователей, то в протокол заносится данных меньше, чем того требует безопасность.

и связанные с ними трудности 233
Межсетевое экранирование 234
Возможности систем межсетевого экранирования 235
Создание набора фильтрующих правил 236
Размещение сетевых компонентов 240
Профилирование систем по критерию риска 240
Определение требований к управлению рисками 241
Создание зон безопасности на основе предъявляемых требований 242
Системы обнаружения вторжения 242
Что такое «обнаружение вторжения» 244
Выбор системы IDS 244
Пример сетевой IDS 249
Пример локальной IDS 250
Управление и контроль 251
Управленческие задачи, решаемые администратором 252
Что должен контролировать администратор 253
Зачем нужны аутсорсинг-партнеры 256
Достоинства и недостатки аутсорсинга 257
Использование мощностей выделенных подстанций 257
Выбор аутсорсинг-партнера 258
Резюме 259
Конспекты 259
Часто задаваемые вопросы 264

Глава 6. Защита финансовых операций 265

Введение 266
Принцип и системы оплаты через Internet 267
Кредитные, расходные или дебетные карты 267
Процесс оплаты на пункте продажи 269
Особенности обработки расходных карт 270
Обработка и окончательный расчет 271

Обзор торговых POS-терминалов

Перечислим некоторые возможности ICVERIFY:

- Импортирование транзакций из других приложений (электронные таблицы и базы данных).
- Группировка транзакций для единовременной авторизации.
- Поддержка систем адресной проверки (AVS), розничной AVS, CVV2 и CVC2 для уменьшения угроз, связанных с подделками и кражами пластиковых карт.

Анализ данных и предотвращение ошибок на этапе импортирования транзакционной информации.

Стадии процесса оплаты через Internet 272
Осторожно, опасная информация! 276
Подходы к решению проблем оплаты через Internet 277
Варианты и выбор способа коммерческой оплаты 278
Провайдеры коммерческого сервера 279
Использование собственных ресурсов 280
Обеспечение надежности процесса оплаты 282
Дополнительные средства управления сервером 285
Управление на прикладном уровне 286
Понятие криптографии 286
Методология 287
Роль ключей в криптосистемах 290
Принципы криптографии 292
Цифровые сертификаты 296
Криптография в электронной коммерции 299
Функции хэширования 299
Блочные шифры 300
Системы, реализующие PPK-криптографию 300
Протокол SSL 301
Протокол защищенных транспортных уровней 302
Система PGP 304
S/MIME 305
Протокол защищенных электронных транзакций 305
Цифровые подписи на языке XML 307
Реализация виртуального POS 309
Программа ICVERIFY 310
Альтернативные системы оплаты 312
Разработки на основе использования смарт-карт 312
Системы proxy-обслуживания 316
Забавные деньги 317

Разделы «Безопасный совет» или «Инструментарий» предоставляют дополнительную информацию

Инструментарий: Использование Honeypot для измерения потенциальной угрозы

В контексте информационной безопасности «горшком меда» (honeypot) или «ловушкой» принято называть систему, созданную для взлома. Установка такой системы в вашей сети позволит изучить тактику взломщиков и, возможно, узнать несколько новых видов атак. Хорошо, если злоумышленник не подозревает, что залез в «горшок с медом». Он должен вести себя естественно, как в случае проникновения в обычную систему без специального мониторинга. В рамках концепции Honeypot такой мониторинг подразумевает детальное протоколирование всех действий нападающего. Причем функцию слежения может выполнять как сам узел-ловушка, так и любая другая машина в сети. Главное, что эффективность «горшка меда» всегда зависит от количества и качества собранной информации.

Резюме 319
Конспекты 320
Часто задаваемые вопросы 325

Глава 7. Взлом собственного сайта 327

Введение 328
Различные виды атак 328
Отказ в обслуживании 328
Утечка информации 330
Получение доступа к файловой системе 331
Дезинформация 332
Получение доступа к служебным файлам 333
Расширение привилегий 334
Планирование риска 335
Определение количества вложенных средств 336
Каким образом хакеры могут угрожать сайту и как обнаружить угрозу 337
Выявление уязвимостей сайта 340
Основы техники проведения аудита 341
Изучение уязвимостей системы 344
Использование средств автоматического сканирования 352
Наем команды аудиторов 357
Резюме 360
Конспекты 361
Часто задаваемые вопросы 365

Глава 8. Чрезвычайное планирование 367

Введение 368
Что такое чрезвычайное планирование 368
Структура чрезвычайного плана 370
Чрезвычайный план и соответствие стандартам качества 377
Обеспечение резервного копирования и восстановления данных 378

Аспекты безопасности в применении распределителей нагрузки

Заметьте, что в списке недостатков были упомянуты проблемы безопасности. На самом деле распределители вряд ли способны увеличить риски, связанные с безопасностью системы, тем более что можно расширить функциональность этих устройств до функциональности простейшего межсетевого экрана. Однако давайте посмотрим, какие именно проблемы могут возникнуть.

Нетрудно себе представить, что некоторые распределители уязвимы с точки зрения защиты. Здесь возможны атаки на предоставляемый интерфейс управления устройством или на адрес устройства. Как и любая дополнительная подсистема, распределитель предоставляет взломщику возможности для совершения атаки на другие компоненты системы. Если злоумышленник получит административные права доступа к распределителю, он, к примеру, сможет осуществить «виртуальный подлог», перенаправив ваш трафик на другие серверы.

Необходимость сверки резервной копии с оригиналом 379
Защита резервных копий конфиденциальной информации 383
Планирование действий при отказе оборудования или прекращении обслуживания 388
Проблема отказа ключевого элемента 388
Как защититься от стихийных бедствий 394
«Горячие» сайты: альтернативный путь к спасению 395
Как выбрать «горячий» сайт 395
Тестирование «горячего» сайта 396
Страхование рисков электронной коммерции 397
Страхование профессиональной ответственности 398
Страхование интеллектуальной собственности 399
Защита собственности и доходов 400
Выбор страхования 401
Страхование, которое может и не понадобиться 404
Резюме 406
Конспекты 407
Часто задаваемые вопросы 411

Глава 9. Поддержка больших объемов сетевого трафика 413

Введение 414
Что делать, если популярность сайта превзошла все ожидания 414
Определение загрузки сайта 415
Повышение производительности Web-сервера 424
Управление пропускной способностью 428

Составление цепи доступа

- Кто имел доступ к улике?
- Где находилась улика?
- Какие меры безопасности применялись в месте хранения улики?
- Какие доказательства есть на данный момент?

Заключение договора с провайдером 429
Когда скорости не хватает 432
Растут потребности – увеличиваются скорости 433
Распределение нагрузки 435
Что подразумевается под распределением нагрузки 435
Преимущества и недостатки использования распределителя нагрузки 440
Аспекты безопасности в применении распределителей нагрузки 440
Резюме 443
Конспекты 444
Часто задаваемые вопросы 447

Глава 10. Чрезвычайное реагирование, сетевая криминалистика и закон 449

Введение 450
Зачем нужна политика чрезвычайного реагирования 450
Решайте сами – паниковать или сохранять спокойствие 450
Чего делать не стоит 451
Хорошая политика окупается сторицей 452
Краткое резюме политики чрезвычайного реагирования 457
Создание команды чрезвычайного реагирования 458
Определение рамок преследования 460
Хакеры, переступившие черту 460
Понятие цепи доступа 462
Процесс чрезвычайного реагирования 463
Введение в сетевую криминалистику 464
Отслеживание инцидентов 470
Ресурсы 472
Юридические документы 472

Резервное копирование/сетевая криминалистика 473
Системы отслеживания инцидентов 474
Разное 474
Резюме 475
Конспекты 476
Часто задаваемые вопросы 479

Приложение А. Методы доставки информации, предлагаемые компанией Cisco 481

Введение 482
Модернизация защиты с использованием Cisco LocalDirector 482
Технология LocalDirector 483
Краткое описание продукта LocalDirector 483
LocalDirector: опции повышения безопасности системы 484
Cisco DistributedDirector и системы географически разрозненных серверов 489
Краткое описание продукта DistributedDirector 490
Механизмы обеспечения безопасности 490
Информационные коммутаторы Cisco 494
Технология информационной коммутации 494
Краткое описание продукта 495
Информационные коммутаторы: опции повышения безопасности системы 496
Резюме 501
Часто задаваемые вопросы 501

Приложение В. Защита от хакеров коммерческого сайта. Конспекты 503

Предметный указатель 541