Аудит информационной безопасности

173 стр. | PDF | 2012 г.

Пособие ориентировано на следующие основные группы читателей:

- **менеджеров высшего эшелона управления компанией;**
- **руководителей служб автоматизации и служб информационной безопасности;**
- **специалистов в области безопасности компьютерных систем, ИТ-менеджеров;**
- **разработчиков средств защиты информационных систем и начинающих аудиторов;**
- **студентов и аспирантов соответствующих технических специальностей.**

Введение

Глава 1. Актуальность аудита безопасности для корпоративных пользователей

1.1. Безопасность электронной почты

1.1.1. Что подстерегает корпоративных пользователей
1.1.2. Администраторы на страже
1.1.3. Мой сервер – моя крепость
1.1.4. Открытые ретрансляторы и борьба со спамом
1.1.5. Электронная почта и брандмауэры

1.2. Безопасность WWW

1.2.1. Экскурс в технологию WWW
1.2.2. Посторонним вход воспрещен?
1.2.3. Пользователи сети вновь под ударом
1.2.4. Возможное решение – SSL
1.2.5. Атаки на HTTP-серверы
1.2.6. Прокси-сервер – контролер и защитник

1.3. Безопасность DNS

1.3.1. Методы и задачи злоумышленника
1.3.2. Технология подлога
1.3.3. Технологии защиты
1.3.4. Открытость данных зоны
1.3.5. DNS и брандмауэры

1.4. Возможности аудита безопасности

1.4.1. Фильтрация на маршрутизаторе
1.4.2. Анализ сетевого трафика
1.4.3. Защита маршрутизатора
1.4.4. Защита хоста
1.4.5. Превентивное сканирование

Глава 2. Практика аудита безопасности корпоративных систем Internet/Intranet

2.1. Оценка информационной безопасности российских компаний

2.1.1. Пример 1. Корпоративная информационная система финансовой группы «Балт-Эксперт»
2.1.2. Пример 2. Корпоративная информационная система информационного агентства «Информ-Экспресс Новости»
2.1.3. Пример 3. Корпоративная информационная система коммерческого банка «РосБалт»
2.1.4. Общие проблемы представителей отечественного бизнеса

2.2. Выработка рекомендаций по результатам аудита безопасности

2.2.1. Эволюция взглядов на обеспечение информационной безопасности компании
2.2.2. Облик корпоративной системы защиты
2.2.3. Централизованное управление информационной безопасностью компании

2.3. Межсетевое экранирование

2.3.1. Специфика Internet/Intranet технологий
2.3.2. Защита периметра корпоративной сети
2.3.3. Межсетевые экраны

2.3.4. Возможные варианты защиты сети
2.3.5. Примеры защиты периметра сети
2.3.6. Защита внутренних корпоративных информационных ресурсов
2.3.7. Возможные варианты защиты корпоративных серверов
2.3.8. Особенности распределенных экранов

2.4. Антивирусная защита предприятия

2.4.1. Состояние антивирусной защиты в российских компаниях
2.4.2. Методика построения корпоративных систем антивирусной защиты
2.4.3. Примеры возможных решений антивирусной защиты

2.5. Проектирование виртуальных частных сетей

2.5.1. Построение безопасной корпоративной сети
2.5.2. Возможные рекомендации по выбору VPNрешений

Глава 3. Методологические основы аудита безопасности

3.1. Влияние аудита безопасности на развитие компании

3.1.1. Как оценить уровень безопасности корпоративной системы Internet/Intranet?
3.1.2. Новые возможности развития компании
3.1.3. Практические шаги аудита безопасности

3.2. Новое поколение стандартов информационной безопасности

3.2.1. Стандарты BS ISO/IEC 27001:2005 (BS 7799-1:2008) и BS 7799-2:2008
3.2.2. Стандарт COBIT 5.1

3.3. Планирование аудита информационной безопасности компании

3.4. Управление аудитом информационной безопасности компании

3.5. Соотношение отечественной и международной терминологии аудита

Глава 4. Возможный алгоритм аудита безопасности компании

4.1. Аудит безопасности в российских условиях

4.1.1. Анализ требований информационной безопасности
4.1.2. Инструментальные проверки уровня безопасности компании
4.1.3. Анализ информационных рисков компании

4.2. Методы оценивания информационных рисков компании

4.2.1. Табличные методы оценки рисков
4.2.2. Перспективные методы оценивания информационных рисков компании

4.3. Возможная методика модернизации корпоративной системы информационной безопасности

4.3.1. Уточнение основных целей и задач обеспечения безопасности
4.3.2. Модель построения системы информационной безопасности
4.3.3. Каркас методики проведения аналитических работ
4.3.4. Методология анализа информационных рисков компании
4.3.5. Проектирование системы обеспечения информационной безопасности предприятия
4.3.6. Возможный алгоритм аудита безопасности компании
4.3.7. Состав информации, необходимой для аудита безопасности

Заключение

Приложение

Приложение 1. Методы информационно-технического воздействия на киберсистемы и возможные способы противодействия

Приложение 2. Методы обнаружения вторжений в киберсистемы цифровой обработки сигналов