

# Съдържание

|                                                                                            |    |
|--------------------------------------------------------------------------------------------|----|
| КРИПТОГРАФИЯ.....                                                                          | 7  |
| История и концепции .....                                                                  | 7  |
| Основни определения.....                                                                   | 7  |
| Необходимостта от криптография.....                                                        | 8  |
| Криптографията – защита на конфиденциалността и цялостността .....                         | 9  |
| Криптографски алгоритми .....                                                              | 10 |
| Симетрична криптография .....                                                              | 10 |
| Асиметрична криптография .....                                                             | 11 |
| Цифрови сертификати.....                                                                   | 14 |
| Криптиране, дайджести на съобщения, хеш функции и цифрови подписи .....                    | 15 |
| Цифрови подписи.....                                                                       | 19 |
| Удостоверяване на произхода с НМАС.....                                                    | 22 |
| Съображения при използването на криптографията.....                                        | 23 |
| Добри практики и допълнителна крипто терминология.....                                     | 25 |
| Добри практики.....                                                                        | 25 |
| Допълнителна крипто терминология .....                                                     | 25 |
| Обобщение .....                                                                            | 29 |
| Управление на публичните ключове .....                                                     | 31 |
| Инфраструктура на публичните ключове .....                                                 | 32 |
| <br>СИГУРНОСТ НА ДАННИТЕ И СИСТЕМИТЕ БАЗИ ОТ ДАННИ.....                                    | 34 |
| Текущо състояние и тенденции в индустрията.....                                            | 34 |
| Откриване на данни и класификацията им.....                                                | 37 |
| Архитектура на сигурността на системите за управление на бази от данни.....                | 38 |
| Трансгранични потоци от данни .....                                                        | 43 |
| Е-откриване.....                                                                           | 44 |
| Анонимизация на данните.....                                                               | 45 |
| Регулаторно определени обекти на анонимизация.....                                         | 47 |
| General Data Protection Regulation .....                                                   | 47 |
| Маскиране на данни .....                                                                   | 48 |
| Пример за преобразуване на данни с IBM InfoSphere Optim .....                              | 49 |
| Други продукти за маскиране на данни .....                                                 | 53 |
| <br>МОНИТОРИНГ НА ДОСТЪПА ДО ДАННИТЕ И НА СЪОТВЕТСТВИЕТО ПРИ ОДИТ .....                    | 54 |
| Състояние и проблеми на мониторинга и следенето на съответствие за одит .....              | 54 |
| Пълен жизнен цикъл на сигурността и съответствието на базите от данни .....                | 58 |
| Технологии, затрудняващи мониторинга.....                                                  | 61 |
| Намаляване на разходите чрез интеграция и автоматизация .....                              | 61 |
| Интеграция със среда за Големи данни на примера на InfoSphere Guardium и Big Insights..... | 66 |
| Интеграция на InfoSphere Guardium с Optim .....                                            | 67 |
| Интегриране на InfoSphere Guardium с QRadar .....                                          | 69 |
| Управление на Главните данни.....                                                          | 69 |
| Z интеграция.....                                                                          | 70 |

|                                                          |     |
|----------------------------------------------------------|-----|
| СИГУРНОСТ НА ИНФРАСТРУКТУРАТА .....                      | 71  |
| Мрежова сигурност .....                                  | 71  |
| TLS/SSL .....                                            | 73  |
| IPSec .....                                              | 74  |
| Сигурност на границите .....                             | 77  |
| Защитна стена .....                                      | 81  |
| Филтриране на пакети в защитната стена .....             | 84  |
| NAT.....                                                 | 84  |
| Разделяне с DNS .....                                    | 85  |
| Откриване на нахлуванията .....                          | 86  |
| Мрежово откриване на нахлуванията.....                   | 87  |
| Пример за мрежово откриване на нахлуванията .....        | 90  |
| Други услуги за сигурност, спецификации и протоколи..... | 91  |
| Мониторинг на мрежата.....                               | 98  |
| Уязвимости на мрежата.....                               | 101 |
| Уязвимости, базирани на IP адресите .....                | 101 |
| ICMP атаки .....                                         | 101 |
| Атаки за усилване и отразяване .....                     | 102 |
| Атаки с подправяне на адреси.....                        | 103 |
| Уязвимости в TCP и UDP .....                             | 104 |
| Уязвимости на ARP .....                                  | 106 |
| DNS атаки.....                                           | 108 |
| Атаки срещу DHCP.....                                    | 109 |
| Атаки на HTTP(S).....                                    | 109 |
| Атаки на е-пощата.....                                   | 111 |
| Други атаки.....                                         | 111 |
| Удостоверяване, даване на разрешение и отчитане .....    | 113 |