

6261

004.056

3
27
4

БИБЛИОТЕКА - УНСС

Инв. №



120000133537

133539

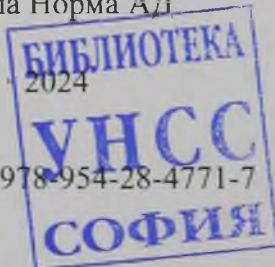
© проф. д-р Владимир Димитров, автор

© Дамян Дамянов, дизайн на корицата

© Сиела Норма АД

София 2024

ISBN: 978-954-28-4771-7



проф. г-р Владимир Димитров

ОСНОВИ НА КИБЕР- СИГУРНОСТТА

Том 1

СЪДЪРЖАНИЕ

НЕОБХОДИМОСТ ОТ КИБЕРСИГУРНОСТ	9
Ръст на необходимостта от засилване на киберсигурността.....	9
Компрометиране сигурността на данните.....	17
Увеличаване на предизвикателствата пред сигурността с напредъка на технологиите	19
Въвеждане в действие на сигурността	22
КОНЦЕПЦИИ И ПРИНЦИПИ НА СИГУРНОСТТА.....	25
Еволюция на инфраструктурата за информационна сигурност	25
Мерки и категории услуги за сигурност	31
Термини и съображения за сигурност	41
Хакери	42
Задачите в областта на киберсигурността	43
Управление на уязвимостите	44
1. Идентификация и валидация	45
2. Оценка на риска и приоритизация	45
3. Лекуване (саниране)	46
4. Непрекъснати подобрения	46
Инструменти за атака и категории атаки	47
Видове зловреден софтуер.....	49
Типове мрежови атаки.....	52
ISO 27001/27002. СИСТЕМИ ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ. КОДЕКС ОТ ПРАКТИКИ ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ	56
Въведение.....	56
Ползите от ISO 27001	58
ISO 27001 изисквания и контроли.....	60
Клауза 4. Контекст на организацията	61
Клауза 5. Водачество	61
Клауза 6. Планиране.....	62
Клауза 7. Поддръжка.....	63
Клауза 8. Оперирание	64
Клауза 9. Оценка на работата.....	64
Клауза 10. Подобрения	65
КОНТРОЛ НА ДОСТЪПА.....	66
Дефиниция и основни понятия	66
Ключови концепции и принципи	67
Изискванията към контрола на достъпа.....	68
Политики за контрол на достъпа	69
Модел за контрол на достъпа и терминология	70
Разрешения и списъци за контрол на достъпа.....	72
Контрол на достъпа, базиран на роли	72
Концепции, свързани с модела на достъп.....	72

ЦИФРОВИ СЕРТИФИКАТИ И ИНФРАСТРУКТУРА НА ПУБЛИЧНИЯ КЛЮЧ.....	74
Асиметрична криптография – частни и публични ключове	74
Цифрови сертификати.....	74
Тристранен модел на доверие – база на доверие.....	76
Сертификационни власти.....	76
Инфраструктура на публичния ключ	82
Описание на PKI компонентите.....	84
Съображения, свързани с PKI	86
 УДОСТОВЕРЯВАНЕ	87
Въведение в удостоверяването – дефиниции и основни постановки	87
Фактори на удостоверяване	88
Характеристики на службите за удостоверяване	89
Технологии и протоколи за удостоверяване	90
Kerberos	90
LDAP	91
Метадиректории и виртуални директории.....	96
Допълнителни ресурси.....	97
 ЦИФРОВАТА ИДЕНТИЧНОСТ И УПРАВЛЕНИЕТО ѝ.....	98
Основни определения.....	98
Концепции на цифровата идентичност	98
Управление жизнения цикъл на идентичността	99
Първични и вторични контроли.....	99
Роли и задължения при управлението на идентичността.....	103
Важност на разделяне на задълженията.....	104
Спогодби, ресертификация и докладване	106
Групи, домейни и управление на привилегированите идентичности.....	107
Водене на идентичността и достъпа	110
 ФЕДЕРИРАНЕ.....	111
Определение и основни постановки.....	111
Бизнес модели за федерирана идентичност	116
Концепции и протоколи на федериране	123
Федерация и доверие	127
 ЕДНОКРАТНО ВЛИЗАНЕ	136
Необходимост от еднократно влизане	136
Кога разбираме, че се нуждаем от еднократно влизане?.....	137
Изискванията към еднократното влизане вътре, вън и между организациите.....	137
 ВЪВЕДЕНИЕ В СИГУРНОСТТА НА УЕБ ПРИЛОЖЕНИЯТА.....	140
Сигурност на Уеб приложенията.....	140
Заплахи за сигурността: SQL инжекции и XSS.....	143
Технологии за автоматично сканиране на сигурността.....	147
Усъвършенствани техники за сканиране	150

УЕБ СИГУРНОСТ ЧРЕЗ СКЕНЕРИ ЧЕРНА И БЯЛА КУТИЯ.....	151
Откриване на SQL инжекции със скенер черна кутия и със скенер бяла кутия	151
Сравняване на технологиите и предизвикателства при скенерите черна и бяла кутия	154
Работа с кода.....	155
 СИГУРНОСТ НА ПРИЛОЖЕНИЯТА С ИЗПОЛЗВАНЕ НА ХИБРИДЕН АНАЛИЗ.....	157
Хибриден анализ.....	158
Технологии на хибридния анализ	159
Хибриден анализ на сигурността от клиентската страна за XSS	160
 ПРИЛОЖЕНИЕ. КОНТРОЛИ ЗА ИНФОРМАЦИОННА СИГУРНОСТ.....	164
5. Организационни контроли	164
6. Контроли върху хората	166
7. Физически контроли	166
8. Технологични контроли	167
 ПРИЛОЖЕНИЕ. OWASP JUICE SHOP.....	169
 ПРИЛОЖЕНИЕ. OWASP ZAP И CODIGA.....	170
ZAP.....	170
CODIGA	171