

# Kurumsal BİLGİ Güvenliđi

Teknik ve Yönetimsel Yönleriyle

Dr. Mehmet KARA



© **PAPATYA YAYINCILIK EĞİTİM**

Ankara Caddesi, Prof. Fahreddin Kerim Gökay Vakfı İşhanı Girişi  
No: 11/6, Cağaloğlu (Fatih) / İstanbul

Tel : (+90 212) 527 52 96 (+90 532) 311 311 0  
Faks : (+90 212) 527 52 97  
e-mail : admin@papatyabilim.com.tr  
Web : www.papatyabilim.com.tr  
Dağıtım : TDK Bilim – www.tdk.com.tr

**Kurumsal Bilgi Güvenliği – Dr. Mehmet KARA**

1. Basım Eylül 2018

Yayın Danışmanı : Toros Rifat ÇÖLKESEN (Ph. D)  
Yayına Hazırlayan : Cengiz UĞURKAYA (Ph.D)  
Üretim : Necdet AVCI  
Pazarlama : Mustafa DEMİR  
Satış : TDK Bilim [www.tdk.com.tr](http://www.tdk.com.tr)  
Sayfa Düzenleme : Papatya ve Kelebek Tasarım  
Basım ve Ciltleme : Özkaracan Matbaacılık (Sertifika No: 12228)  
Evren Mah. Gülbahar Cad. No:62 Güneşli/İstanbul

© Bu kitabın her türlü yayın hakkı Papatya Yayıncılık Eğitim AŞ'ye aittir. Yayınevinden yazılı izin alınmaksızın alıntı yapılamaz, kısmen veya tamamen hiçbir şekil ve teknikle ÇOĞALTILAMAZ, BASILAMAZ, YAYIMLANAMAZ. Kitabın, tamamı veya bir kısmının fotokopi makinesi, ofset gibi teknikle çoğaltılması, hem çoğaltan hem de bulunduranlar için yasadışı bir davranıştır.

Kara, Mehmet

Kurumsal Bilgi Güvenliği / Mehmet Kara - İstanbul: Papatya Yayıncılık Eğitim, 2018.

xvi, 344 s.; 24 cm.

Kaynakça ve Dizin var.

Sertifika No: 11218

ISBN 978-605-9594-50-9

1. OSI 2. Kriptografi 3. Ağ Güvenliği 4. Saldırı Atakları

I. Title

*Bu kitabımı;  
Yaşamın bütün zorluklarına karşı dimdik duran,  
iyi yetişmemiz için her türlü fedakarlığı gösteren  
Sevgili annem  
Döndü KARA'ya  
ithaf ediyorum.  
Seni her geçen gün daha çok özliyorum.*



# İÇİNDEKİLER

## Önsöz

<b>Bölüm 1. Bilgi Sistemleri Güvenlik Yönetimi</b>	<b>15</b>
1.1. Güvenlik Yönetimi Kavramları	15
1.2. Güvenlik Kontrolünün Amaçları	16
1.3. Bilgi Sınıflandırma	17
1.3.1. Bilgi Sınıflandırmanın Amaçları ve Yararları	17
1.3.2. Bilgi Gizlilik Seviyeleri	18
1.3.3. Bilgi Sınıflandırma Kriterleri	19
1.3.4. Gizlilik Seviyeli Bilgilerin Dağıtımı	20
1.3.5. Bilgi Sınıflandırma Roller	20
1.4. Güvenlik Politikası	22
1.5. Roller ve Sorumluluklar	25
1.6. Bilgi Güvenliği Risk Yönetimi	26
1.7. Güvenlik Bilinçlendirmesi	36
1.8. Özet	37
1.9. Çalışma Soruları	38
<b>Bölüm 2. Erişim Kontrolü ve Kimlik Doğrulama</b>	<b>39</b>
2.1. Prensipler (İlkeler)	41
2.1.1. Bilmesi Gereken Prensipleri	41
2.1.2. Geçmiş Değerlendirmesi	42
2.1.3. Erişim Matrisi	42
2.2. Erişim Kontrolü Tekniklerinin Özellikleri ve Uygulanabilirliği	44
2.3. Mevcut Erişim Kontrolü Teknikleri	44
2.3.1. Erişim Kontrolü Listeleri	44
2.3.2. Yetenek Listeleri	46
2.3.3. Yetki İlişkileri	46
2.4. Geliştirilen Erişim Kontrol Teknikleri	47
2.4.1. Şifreleme Tekniği	47
2.5. Erişim Kontrolü Tekniklerinin Özellikleri ve Uygulanabilirliği	47
2.5.1. İsteğe Bağlı Erişim Kontrolü	48
2.5.2. Zorunlu Erişim Kontrolü	49
2.5.3. Rol Temelli Erişim Kontrolü	51

2.6. Eriřim Kontrol Türleri	53
2.6.1. Önleyici/Yönetimsel	54
2.6.2. Önleyici/Teknik	54
2.6.3. Önleyici/Fiziksel	54
2.6.4. Algılayıcı Yönetimsel	54
2.6.5. Algılayıcı/Teknik	55
2.6.6. Algılayıcı/Fiziksel	55
2.7. Kimlik ve Kimlik Doğrulama	55
2.7.1. Parola	55
2.7.2. Biometrikler	58
2.7.3. Tek Noktadan Giriř (Single Sign On-SSO)	60
2.7.4. Kerberos	61
2.7.5. SESAME	68
2.8. Eriřim Kontrol Metodolojileri	68
2.8.1. Merkezi Eriřim Kontrolü	68
2.8.2. Dağıtık Eriřim Kontrolü	69
2.9. Eriřim Kontrolü İle İlgili Konular	69
2.10. Özet	70
2.11. Çalışma Soruları	70
<b>Bölüm 3. OSI Başvuru Modeli ve Ağ Teknolojileri</b>	<b>71</b>
3.1. Teknik Kavramlar	71
3.1. Protokoller	72
3.2. OSI Başvuru Modeli	72
3.2.1. OSI'nin Katmanları	74
3.2.1.1. Fiziksel Katman	75
3.2.1.2. Veri Bağlama Katmanı	76
3.2.1.3. Ağ Katmanı	77
3.2.1.4. İletim Katmanı	77
3.2.1.5. Oturum Katmanı	78
3.2.1.6. Sunu Katmanı	78
3.2.1.7. Uygulama Katmanı	78
3.3. TCP/IP Model	79
3.3.1. Uygulama Katmanı	80
3.3.2. İletim Katmanı	81
3.3.3. İnternet Katmanı	82
3.3.4. Ağ Eriřim Katmanı	85

3.4. Güvenliđi Geniřleten ve Güvenlik Odaklı Protokoller	85
3.5. Veri Ađları Temelleri	86
3.6. Veri Ađları Teknolojileri	88
3.6.1. Yerel Alan Ađı Teknolojileri	88
3.6.1.1. Yerel Alan Ađı İletim Protokolleri	91
3.6.1.2. LAN İletim Metotları	92
3.6.1.3. LAN Topolojileri	93
3.6.1.4. LAN Cihazları	95
3.6.2. Geniř Alan Ađı Teknolojileri	97
3.6.2.1. WAN Protokol ve Topolojileri	97
3.6.3. Uzak Eriřim Teknolojileri	99
3.6.4. Kablosuz İletişim Teknolojileri	102
3.6.4.1. Kablosuz Yerel Alan Ađı Güvenliđi	104
3.6.4.2. Bluetooth Güvenlik Mekanizmaları	106
3.7. Bulut Biliřim Teknolojileri	107
3.7.1. Bulut Biliřim Servis Modelleri	109
3.7.1.1. Yazılım Servisi (SaaS)	109
3.7.1.2. Platform Olarak Servis (PaaS)	110
3.7.1.3. Altyapı Servisi (IaaS)	111
3.7.2. Bulut Türleri	111
3.7.2.1. Genel Bulutlar	112
3.7.2.2. Özel Bulutlar	112
3.7.2.3. Melez Bulutlar	112
3.8. Mobil Biliřim Teknolojileri	112
3.8.1. GSM Temelleri	113
3.8.2. Akıllı Telefonlar	116
3.8.3. Android İşletim Sistemi	117
3.8.3.1. Android İşletim Sistemi Katmanları	117
3.8.3.2. Android Güvenliđi	118
3.8.4. IOS İşletim Sistemi	122
3.8.4.1. IOS Katmanları	123
3.9. Özet	126
3.10. Çalışma Soruları	126

<b>Bölüm 4. Bilgi Sistemlere Yönelik Ataklar</b>	<b>127</b>
4.1. Keşif Saldırıları	127
4.1.1. Web Tabanlı Keşif ve Saldırı Araçları	128
4.2. Tarama Saldırıları	133
4.3. Açıklık Taraması	137
4.4. Giriş Yetkisi Kazanma	141
4.5. Fidyecilik Saldırıları	149
4.6. Servis Dışı Bırakma Saldırıları	153
4.7. Erişimi Devam Ettirme Saldırıları	155
4.8. Sosyal Mühendislik Saldırıları	160
4.9. İçeriden Gelen Tehditler	162
4.10. Özet	163
4.11. Çalışma Soruları	164
<b>Bölüm 5. Kriptografi ve Ağ Güvenliği</b>	<b>165</b>
5.1. Kriptografi Tanımları	165
5.2. Kriptografinin Tarihçesi	168
5.3. Kriptografik Teknolojiler	170
5.3.1. Simetrik Anahtarlı Kriptoloji	170
5.3.1.1. DES	171
5.3.1.2. 3DES	173
5.3.1.3. International Data Encryption Algorithms (IDEA)	173
5.3.1.4. Blowfish	173
5.3.1.5. CAST 128	174
5.3.1.6. Advanced Encryption Standard (AES)	174
5.3.2. Asimetrik Anahtarlı Kriptolama	175
5.3.2.1. RSA Algoritması	177
5.3.2.2. Diffie-Hellman Anahtar Değişimi	179
5.2.3.2. El Gamal	180
5.3.2.4. Eliptik Eğri	180
5.3.3. Açık Anahtar Kripto Sistem Algoritma Kategorileri	180
5.3.4. Sayısal İmzalar	181
5.3.4.1. Sayısal İmza ve Güvenli Özet Standardı	182
5.3.4. Kriptografik Ataklar	182



5.4. Ağ Güvenliği Cihazları	184
5.4.1. Sanal Özel Ağ Cihazları (VPN)	184
5.4.1.1. VPN Türleri	185
5.4.1.2. İkinci Katman VPN Tünelleri	185
5.4.1.3. IPSec Tabanlı VPN Bağlantı Türleri	186
5.4.1.4. IPSec Protokolleri	189
5.4.1.5. Güvenlik Politikası Veritabanı	193
5.4.1.6. Anahtar Yönetimi	196
5.4.1.7. IPSEC Protokollerinde Kullanılan Algoritmalar	197
5.4.2. Güvenlik Duvarları	199
5.4.2.1. Bastion Host	199
5.4.2.2. Paket Filtreleme Güvenlik Duvarları	199
5.4.2.3. Uygulama Katmanı Güvenlik Duvarları	200
5.4.2.4. Durumsal Güvenlik Duvarı	200
5.4.2.5. Dinamik Paket Filtreleme Güvenlik Duvarları	200
5.4.2.6. Çekirdek Vekil Sunucu	201
5.4.2.7. Yeni Nesil Güvenlik Duvarları	201
5.4.2.8. Güvenlik Duvarı Mimarileri	202
5.4.2.9. Ağ Adres Dönüşümü	203
5.4.3. Saldırı Tespit/Önleme Sistemleri	204
5.4.3.1. Ağ Tabanlı Saldırı Önleme Sistemleri	205
5.4.3.2. Sunucu Tabanlı Saldırı Önleme Sistemleri	206
5.4.3.3. SÖS Algılama Yöntemleri	206
5.5. Özet	207
5.6. Çalışma Soruları	207
<b>Bölüm 6. Güvenlik Mimarisi ve Modelleri</b>	<b>209</b>
6.1. Bilgisayar Mimarisi	209
6.1.1. Merkezi İşlem Birimi	210
6.1.2. Bellekler	212
6.1.3. Giriş/Çıkış Yapıları	214
6.1.4. İşletim Sistemi	214
6.1.5. Yazılım ve Programlama	218
6.1.6. Dağıtık Mimari	219
6.2. Güvenli Mimari Gereksinimi	220
6.3. Önemli Güvenlik Koruma Mekanizmaları	221

6.4. Güvenlik Garanti Sistemleri	222
6.4.1. Ortak Kriterler	223
6.4.1.1. Ortak Kriterlerin İçeriği	225
6.4.1.2. Ortak Kriterlerin Yapı Taşları	226
6.4.1.3 Ortak Kriterlerin Tarafları	231
6.4.1.4. Akreditasyon ve Onay	233
6.4.2. Yetenek ve Olgunluk Modeli ( CMMs)	234
6.4.3. Microsoft Güvenli Geliştirme Yaşam Döngüsü	236
6.4.4. OWASP SAMM Güvenlik Modeli	240
6.5. Özet	241
6.6. Çalışma Soruları	242
<b>Bölüm 7. İş Sürekliliği ve Felaketten Kurtarım Planlaması</b>	<b>243</b>
7.1. Tanımlar	244
7.2. İş Sürekliliği Planı	246
7.2.1. Sürekliliği Bozucu Olaylar	245
7.2.2. İş Sürekliliği Planlamasının Elemanları	246
7.2.2.1. Kapsam ve Plan Başlatma	246
7.2.2.2. İş Etki Analizi	248
7.2.2.3. İş Sürekliliği Planı Geliştirme	252
7.2.2.4. Plan Onaylatma ve Gerçekleme	253
7.3. Felaketten Kurtarma Planı	254
7.3.1. Felaketten Kurtarma Planının Amaç ve Hedefleri	254
7.3.2. Felaketten Kurtarma Planı Süreçleri	254
7.3.2.1. Veri İşleme Sürekliliği Planlaması	255
7.3.2.2. Felaket Kurtarma Planı Bakımı	259
7.3.2.3. Test Belgelerinin Oluşturulması	259
7.3.2.4. Felaketten Kurtarım Planı Tipleri	260
7.3.2.5. Felaketten Kurtarım Prosedürleri	261
7.4. İş Sürekliliği Standartları	262
7.5. Özet	263
7.6. Çalışma Soruları	264

<b>Bölüm 8. İşletme Güvenliği</b>	<b>265</b>
8.1. İdari Yönetim	266
8.1.1. Güvenlik ve Ağ Yönetimi	267
8.1.2. İzlenebilirlik	268
8.1.3. İşlem Sorumluluğu	269
8.1.4. Veri Kaçağı	269
8.2. Varlık İşletim Güvenliği Kontrolleri	270
8.2.1. Garanti Seviyeleri	270
8.2.2. Varlık Tanıma ve Yönetimi	270
8.2.3. Sistem Kontrolleri	270
8.2.4 Giriş Çıkış Kontrolleri	271
8.2.5. Sistem Sıkılaştırma	271
8.3. Ağ Güvenliği Yönetim Konseptleri	272
8.3.1. Uzak Erişim Güvenlik Yönetimi	272
8.3.2. Saldırı Tespiti/Önleme ve Cevaplama	272
8.3.3. Bilgisayar Olaylarına Müdahale Ekibi	274
8.3.3. Ağ Sürekliliği	274
8.3.4. Tek Nokta Hatasının Yönetilmesi	278
8.3.4.1. Kablolama Hataları	278
8.3.4.2. Topoloji Hataları	279
8.3.5. DDoS Engelleme Sistemi	279
8.4. Güvenlik Test ve Denetimleri	280
8.4.1. Bilgi Sistem Güvenlik Denetimi	283
8.4.2. Bilgi Sistemleri Sızma Testi	283
8.5. Özet	284
8.6. Çalışma Soruları	284
<b>Bölüm 9. Yasalar, Uyumluluk ve Delil Toplama ve Etik</b>	<b>285</b>
9.1. Siber Hukukun Değişik Yönleri	286
9.1.1. Etik	286
9.1.2. İnternet Mimarisi Yönetim Kurulu	288
9.2. Motivasyon, Fırsat ve Suç İşleme	288
9.2.1. Bilgisayar Korsanları ve Siber Saldırganlar	289
9.2.2 İşlem Güvenliği	291
9.3. Bilişim Suçlarını Hukuki Yönden Takip Etme	293
9.3.1. Sorumluluk ve Sonuçları	295

9.4. Kanun Tipleri	296
9.5. Bilgisayar Suçlarını Soruşturma	301
9.5.1. Kanıt	302
9.5.2. Kanıtın Kabul Edilebilirliği	303
9.5.3. Kanıt Türleri	303
9.6. Yasalar, Düzenlemeler ve Uyumluluk	306
9.7. Türk Ceza Kanunundaki Bilişim ve Bilişim Suçları	306
9.8. Özet	309
9.9. Çalışma Soruları	309
<b>Bölüm 10. Fiziksel Güvenlik</b>	<b>311</b>
10.1. Fiziksel Güvenliğe Yönelik Tehditler	312
10.2. Fiziksel Güvenlik Kontrolleri	313
10.2.1. Yönetimsel Kontroller	314
10.2.2. Çevresel ve Yaşam Güvenliği Kontrolleri	318
10.2.3. Yangın Tespiti ve Söndürme	319
10.2.4. Isıtma, Havalandırma ve Klima	323
10.2.5. Fiziksel ve Teknik Kontroller	324
10.2.6. Bilgisayar Envanter Kontrolü	330
10.2.7. Saklama Ortamı Gereksinimleri	331
10.3. Özet	334
10.4. Çalışma Soruları	334
Kaynakça	335
Dizin	341

## ÖNSÖZ

Bilgi güvenliğinin önemi her geçen gün daha çok anlaşılıyor. Ama bilişim uygulamaları hep bir adım önde gidiyor. Çünkü bilişim teknolojileri askeri, sağlık, enerji üretim ve dağıtımı, haberleşme, devlet uygulamaları, ticaret, bankacılık gibi hayatın her alanında yeni uygulamaları hizmete sunuyor. Bunu da klasik bir sunucu istemci uygulaması ile değil, bulut bilişim, nesnelerin İnternet’i, endüstriyel kontrol sistemler gibi değişik bakış ile sunuluyor. Bu da güvenliğin sürekli ve bütüncül bakış açısı ile ele alınmasını gerektiriyor. Önceki dönemlerde güvenlikten beklenen iyi yönetilen bir güvenlik duvarı, aktif bir antivirüs programı, güncel işletim sistemi, güçlü kimlik doğrulama ve bunları yönetimiydi. Günümüzde ise hem teknik hem yönetsel taraflarıyla güvenliği tümenden ele alan yaklaşımlar gerekiyor. Hatta bu o kadar ileri gidiyor ki ağda kullanılan yazılım ve donanımların güvenli geliştirme metodolojileri ile geliştirilmesi, bağımsız laboratuvarlar tarafından test edilip sertifikalandırılması isteniyor. İstenilen güvenliğin sağlanması için bazen ülkedeki kurumlar arasında, bazen uluslararası düzeyde iş birliği ve koordinasyon gerekiyor.

Bu kapsamda bu kitapta bilgi güvenliği konusu hem yönetsel hem teknik yönleriyle ele alındı. Bir kurumda bilgi sistemin güvenli olarak tasarlanması, kurulması ve işletilmesi için gerekli tüm adımlar anlatıldı. Ağ cihazları, sınır güvenliği cihazları, saldırı yöntem ve araçları, fiziksel güvenlik gibi teknik konular yanında, olay kayıtlarının değerlendirilmesi ve yönetilmesi, risk analizi, iş sürekliliği ve felaketten kurtarma, bilişim hukuku, personellerin eğitilmesi gibi yönetsel konular da ele alındı. Uygulamaya yönelik teknik ve yönetsel konuların yanısıra OSI referans modeli, kriptografi, erişim kontrolü, kimlik doğrulama gibi bilgi güvenliğiyle ilgili kavramlar derinlemesine anlatıldı. Bu bakış açılarıyla Üniversitelerde bilgi güvenliğinin tüm yönüyle el almak isteyen dersler için kaynak kitap olarak okutulabilir.

Kitap ISO/IEC 27001 Bilgi güvenliği Yönetim Sistemi standardının kurumda kurulup güvenli olarak işletilmesinde veya tüm dünyada bilgi güvenliği konusunda önemli prestiji olan CISSP (Computer Information System Security Professional) gibi sertifikasyon sistemlerinin konu ve kavramlarının anlaşılmasında önemli bir kaynak niteliğindedir.

Dr. Mehmet KARA

## Kısaltmalar

AES	Advanced Encryption Standard
AH	Authentication Header
CISSP	Computer Information System Security Professional
DDoS	Distributed Denial Of Service
DoD	Department of Defence
DoS	Denial of Service
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
GSM	Global System for Mobile Communication
IDEA	International Data Encryption Algorithms
ITSEC	Information Technology Security Evaluation Criteria
OSI	Open System Interconnection
PAP	Password Authentication Protocol
PCI	Payment Card Industry
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
RFC	Request For Comments
RSA	Rivest, Shamir, Adleman
SDL	Security Development Lifecycle
SHA	Secure Hash Algorithms
SOME	Siber Olaylara Müdahale Ekibi
SÖS	Saldırı Önleme Sistemi
SSL	Secure Socket Layer
TACACS	Terminal Access Controller Access Control System
TCSEC	Trusted Computer Security Evaluation Criteria
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access