

Siber Güvenlik ve Savunma: Standartlar ve Uygulamalar

Editör

Prof. Dr. Şeref SAĞIROĞLU

Yazarlar

Prof. Dr. Şeref SAĞIROĞLU
Doç. Dr. Gökhan ŞENGÜL
Doç. Dr. Ali Hakan IŞIK
Doç. Dr. Gülüstan DOĞAN
Dr. Öğr. Üyesi Atıla BOSTAN
Dr. Öğr. Üyesi Eyüp Burak CEYHAN
Dr. Öğr. Üyesi İsmail Fatih CEYHAN
Dr. Öğr. Üyesi Onur ÇAKIRGÖZ
Dr. Öğr. Üyesi Mehmet DEMİRCİ
Dr. Öğr. Üyesi Muharrem Tuncay GENÇOĞLU
Dr. Öğr. Üyesi A. Nurdan SARAN
Onur AKTAŞ
A. Oğuzhan ALKAN
Bilgehan ARSLAN
Sedef DEMİRCİ
Burak ÖZÇAKMAK
Seda YILMAZ
Özgür YÜREKTEN

ISBN: 978-605-2233-42-9

1. Baskı

Aralık, 2019 / Ankara
1500 Adet



Grafiker®

Yayınları

Yayın No: 334

Web: grafikeryayin.com

Kapak, Sayfa Tasarımı, Baskı ve Cilt



Grafiker®

Grafik-Ofset Matbaacılık Reklamcılık San. ve Tic. Ltd. Şti.

1. Cadde 1396. Sokak No: 6

06520 (Oğuzlar Mahallesi) Balgat-ANKARA

Tel : 0 312. 284 16 39 Pbx - Faks : 0 312. 284 37 27

E-posta : grafiker@grafiker.com.tr

Web : grafiker.com.tr



HAVELSAN® Bu kitap HAVELSAN'ın katkılarıyla basılmıştır.

İÇİNDEKİLER

EDİTÖRDEN.....	11
BİLGİ GÜVENLİĞİ DERNEĞİ'NDEN.....	15
ÖN SÖZ.....	19

1. BÖLÜM

SİBER GÜVENLİK MATEMATİĞİ

1.1. Giriş.....	23
1.2. Siber Güvenlik için Matematğin Önemi.....	25
1.3. Siber Savunmada Matematiksel Modelleme.....	27
1.3.1. Matematiksel Modelleme.....	27
1.3.2. Siber Savunma Sistemi Modelleme Prensipleri.....	28
1.3.3. Kötü Niyetli Nesnelere ve Savunma.....	29
1.3.3.1. Taylor Serisi Genişlemesi.....	30
1.3.3.2. Sonlu Fark Yaklaşım Yöntemleri.....	30
1.3.3.3. Yüksek Dereceden Türevler.....	31
1.3.4. Değerlendirmeler.....	32
1.4. Sosyal Medya.....	33
1.5. Örnekler.....	34
1.6. Kuantum Kriptoloji.....	38
1.7. Kuantum Bilgisayar ve Algoritmaları.....	40
1.7.1. Deutsch Algoritması.....	42
1.7.2. Shor Algoritması.....	43
1.7.3. Grover Algoritması.....	45
1.8. Değerlendirmeler.....	46

2. BÖLÜM

SİBER GÜVENLİK STANDARTLARI

2.1. Giriş.....	51
2.2. Güvenlik Politikaları.....	54
2.3. Güvenlik Standartlarını Destekleyen Organizasyonlar.....	54
2.4. Bilgi Güvenliği Standartları.....	56
2.4.1. ISO/IEC Standartları.....	57
2.4.2. Türk Standartları (TSE Standartları).....	58

2.5. Bilgi Güvenliği Standartları Ailesi.....	58
2.6. Açık Anahtar Şifreleme Standartları (PKCS-Public Key Crypto Standard).....	62
2.7. ISO/IEC 15408: 2016 Ortak Kriterler.....	63
2.8. Müttefik Kalite Güvence Yayınları Standardı (Allied Quality Assurance Publications-AQAP).....	69
2.9. IEEE Standartları.....	70
2.10.ETSI Standartları.....	72
2.11.ITU (Uluslararası Telekomünikasyon Birliği) Standatları ve Siber Güvenlik Faaliyetleri.....	76
2.12.PCI Güvenlik Standartları Konseyi.....	79
2.13.NIST Siber Güvenlik Platformu (NIST Cybersecurity Framework).....	80
2.14.Bilişim Teknolojileri Yönetim ve Denetim Enstitüsü (ISACA) Standartları.....	80
2.15.ENISA (European Union Agency For Cybersecurity).....	81
2.16.Değerlendirmeler.....	83

3. BÖLÜM

BİLGİ, ÜRÜN VE SİSTEM AÇISINDAN SİBER GÜVENLİK STANDARTLARI

3.1. Giriş.....	89
3.2. Siber Güvenlik ve Standartlar.....	90
3.2.1. Sistem Güvenliği Standartları.....	91
3.2.2. Ürün Güvenliği Standartları.....	93
3.2.3. Bilgi Güvenliği Tetkik Standartları.....	95
3.3. Sektörde Kullanılan Diğer Siber Güvenlik Standartları ve Yayımcı Kuruluşlar.....	96
3.4. Değerlendirmeler.....	98

4. BÖLÜM

SİBER GÜVENLİKTE ASKERİ STANDARTLAR KAPSAMINDA AQAP İNCELEMESİ

4.1. Giriş.....	103
4.2. AQAP (Müttefik Kalite Güvence Yayınları - The Allied Quality Assurance Publications).....	104
4.3. Ülkemizdeki Etkin Kullanılan AQAP'lar.....	105

4.3.1. AQAP-110 NATO Tasarım, Geliştirme ve Üretim Kalite Güvencesi Koşulları.....	106
4.3.2. AQAP-120 NATO Üretim Kalite Güvencesi Koşulları.....	107
4.3.3. AQAP-130 NATO Muayene ve Test Kalite Güvencesi Koşulları.....	108
4.3.4. AQAP-150 NATO Yazılım Geliştirme Kalite Güvencesi Koşulları.....	108
4.3.5. AQAP-160 NATO Yazılım Ömür Devri Boyunca Birleştirilmiş Kalite Gereksinimleri.....	110
4.3.6. AQAP-2000 Ömür Devri Boyunca Kaliteye Bütünleşik Sistemler Yaklaşımına İlişkin NATO Politikası.....	111
4.3.7. AQAP-2009 AQAP 2000 Serisinin Kullanımı İçin NATO Rehberi.....	114
4.3.8. AQAP-2105 Devredilebilir Kalite Planları İçin NATO Gereklere.....	114
4.3.9. AQAP-2110 Tasarım, Geliştirme ve Üretim İçin NATO Kalite Güvence Gereklere.....	115
4.3.10. AQAP-2120 Üretim İçin NATO Kalite Güvence Gereklere.....	116
4.3.11. AQAP-2130 Muayene ve Test İçin NATO Kalite Güvence Gereklere.....	116
4.3.12. AQAP-2210 AQAP 2110'a NATO Yazılım Kalite Güvence Gereklere İlavesi.....	116
4.4. Değerlendirmeler.....	117

5. BÖLÜM

YAZILIM TANIMLI AĞLAR VE SİBER GÜVENLİK

5.1. Yazılım Tanımlı Ağların Temelleri.....	123
5.1.1. Kontrol ve Veri Düzlemlerinin Ayrılması.....	126
5.1.2. Veri Katmanı.....	127
5.1.3. Kontrol Katmanı.....	127
5.1.4. Güney Arayüzü (Southbound API).....	127
5.1.5. Uygulama Katmanı.....	128
5.1.6. Kuzey Arayüzü (Northbound API).....	128
5.2. Yazılım Tanımlı Ağların Siber Güvenlik İçin Önemi.....	129
5.2.1. Siber Güvenliğin Sağlanmasına Ne Katkı Sağlar?.....	129

5.2.2. Siber Güvenlik Açısından Ne Tür Yeni Zorluklara Yol Açar?	130
5.3. Yazılım Tanımlı Ağlarda Siber Güvenlik Fonksiyonları	132
5.3.1. Saldırı Tespit Fonksiyonları	132
5.3.1.1. Saldırı Tespit Sistemi	132
5.3.1.2. Zararlı Yazılım Tarayıcılar	133
5.3.1.3. DDoS Tespit Sistemi	133
5.3.1.4. Derin Paket İnceleme	134
5.3.2. Saldırı Engelleme Fonksiyonları	134
5.3.2.1. Güvenlik Duvarı	134
5.3.2.2. Saldırı Engelleme Sistemi	135
5.3.3. Saldırı Yakalama Fonksiyonları	136
5.4. Yazılım Tanımlı Ağlar ve DDoS	136
5.4.1. DDoS Saldırılarının Tespitinde Yazılım Tanımlı Ağ Tabanlı Çözümler	138
5.4.1.1. Güvenlik Fonksiyonu Çözümleri	138
5.4.1.2. Mimari Çözümleri	140
5.4.2. Yazılım Tanımlı Ağlarda Gerçekleştirilen DDoS Saldırılarının Tespiti	142
5.5. Değerlendirmeler	144

6. BÖLÜM

WEB UYGULAMA ZAFİYETLERİ VE ÖNLEMLER

6.1. Web Uygulamaları ve Tehditler	155
6.2. Web Uygulamalarını Anlamak	158
6.2.1. Web Uygulama Geliştirilmelerinde Kullanılan Diller ve Bağlantı Yapıları	159
6.2.2. Web Sunucuları ve Veri Tabanları	161
6.2.3. HTTP Protokolü	162
6.2.4. Robots Exclusion Protokolü	164
6.3. Web Uygulama Güvenliği	165
6.3.1. Siber Güvenlik Tanımları	165
6.3.2. Güvenlik Testi ve Zafiyet Analizi	167
6.3.3. Aktif ve Pasif Bilgi Toplama	169
6.4. Web Uygulama Zafiyetleri ve Çözüm Önerileri	171
6.4.1. Siteler Arası Betik Çalıştırma Zafiyeti	171
6.4.2. SQL Enjeksiyonu Zafiyeti	175
6.4.3. Sitelere Arası İstek Sahteciliği	178

6.4.4. Basit Parola Denemeleri ve Kaba Kuvvet Saldırıları.....	180
6.4.5. Yetkisiz Erişim Zafiyeti.....	181
6.4.6. Dosya Çağırma.....	182
6.4.7. Diğer Enjeksiyon Zafiyetleri.....	185
6.5. Web Zafiyetlerini Önleme.....	187
6.5.1. Bağlantılarda Kullanılan Türkçe Kelime Listesinin Belirlenmesi.....	189
6.5.2. Web Uygulamalarından Bilgi Toplanması ve Bağlantı Tahmini.....	190
6.6. Değerlendirmeler.....	194

7. BÖLÜM

KABLOSUZ ALGILAYICI AĞLARINDA GÜVEN

7.1. Tanımlar: Güven, Güvenilirlik ve İtibar.....	205
7.2. Farklı Alanlarda Güven.....	206
7.2.1 Sosyal Bilimler ve E-Ticarette Güven.....	206
7.2.2 Dağıtık ve Akran Sistemlerde Güven.....	207
7.2.3 Ad-Hoc Ağlarda Güven.....	208
7.3. Siber Güvenlikte Güven Kavramı.....	208
7.4. Kablosuz Algılama Ağlarında Güven.....	210
7.5. Kablosuz Algılama Ağları İçin Geliştirilen Bazı Güven Uygulamaları.....	214
7.5. Değerlendirmeler.....	217

8. BÖLÜM

FİDYE YAZILIMLAR

8.1. Giriş.....	227
8.2. Fidye Yazılım Saldırısının İşleyiş Aşamaları.....	229
8.3. Fidye Yazılımlarının Evrimi.....	230
8.3.1. AIDS (1989).....	230
8.3.2. GPCode.....	231
8.3.3. Reveton (2012).....	232
8.3.4. Cryptolocker (2013).....	232
8.3.5. Kovter (2013).....	234
8.3.6. SimpLocker (2014).....	235
8.3.7. CTBLocker (2014).....	235
8.3.8. Locky (2016).....	235
8.3.9. Cerber Version 6.0 (2016).....	236
8.3.10. SamSam-Samas, Samsa (2016).....	236

8.3.11. WannaCry (2017).....	236
8.3.12. Petya/NotPetya (AxPetr) (2017).....	236
8.3.13. BadRabbit (2017).....	237
8.4. Fidyeye Yazılımlarına Karşı Alınabilecek Önlemler	237
8.5. Değerlendirmeler	240

9. BÖLÜM

WANNACRY VE PETYA FİDYE YAZILIMLARI

9.1. Giriş	245
9.2. Petya ve WannaCry Fidyeye Yazılımları	250
9.3. WannaCry ve Petya Fidyeye Yazılımlarının Çalışma Mekanizmaları	253
9.3.1. WannaCry.....	253
9.3.2. Petya.....	258
9.4. Fidyeye Yazılımlarından Korunma ve Alınması Gereken Önlemler	264
9.5. Değerlendirmeler	366

10. BÖLÜM

SİBER PARA

10.1. Paranın Tarihçesi	273
10.2. Kripto Para	274
10.3. En Çok İşlem Gören Sanal Para Çeşitleri	275
10.3.1. Bitcoin.....	276
10.3.1.1. Bitcoin Tasarım İlkeleri.....	278
10.3.1.2. Bitcoin Yazılımı ve Bitcoin Adresi.....	279
10.3.2. Ethereum.....	279
10.3.3. Ripple.....	281
10.4. Kripto Paranın Özellikleri ve Normal Paraya Göre Üstünlükleri	282
10.5. Sanal Paranın Türkiye’de ve Dünya’da Kullanımı ve Ülkelerin Yaklaşımları	282
10.6. Blokzincir ve Blokzincirde Ortaya Çıkabilecek Riskler	285
10.6.1. Genel Riskler.....	286
10.6.1.1. Gizli Anahtar Güvenliği.....	286
10.6.1.2. %51 Güvenlik Açığı.....	287
10.6.1.3. İlgil Faaliyetler.....	287
10.6.1.4. İşlem Gizliliği Sorunu.....	289
10.6.1.5. Çift Harcama.....	289

10.6.2. Blokzincir 2.0'a Özgü Riskler.....	290
10.6.2.1. Zeki Sözleşmedeki Güvenlik Zaafları.....	290
10.6.2.2. Düşük Fiyatlı İşlemler.....	290
10.6.2.3. Optimize Edilmemiş Zeki Sözleşme.....	291
10.7. Blokzincir Sistemlerine Yapılmış Saldırı Örnekleri.....	292
10.7.1. DAO Saldırısı.....	292
10.7.2. BGP Ele Geçirme Saldırısı.....	292
10.8. Blokzincirde Güvenlik Geliştirmeleri.....	292
10.8.1. SmartPool.....	293
10.8.2. Nicel Yapı.....	293
10.8.3. Oyente.....	294
10.9. Sanal Para İle Siber Güvenlik Arasındaki İlişki.....	294
10.9.1. Kripto Para Borsalarına Saldırı Örnekleri.....	296
10.9.2. Siber Güvenlik Açısından Alınması Gereken Önlemler.....	297
10.10. Değerlendirmeler.....	298

11. BÖLÜM

TWITTER'DA ARKADAŞ ÖNERİLERİNİN TEKNOLOJİ VE BİLGİ YÖNETİMİ BAKIŞ AÇISIYLA SİBER GÜVENLİĞE ETKİSİ

11.1. Giriş.....	307
11.2. Problem Tanımı.....	309
11.3. Teknoloji Yönetimi ile Arkadaş Tavsiyesi.....	310
11.3.1. Kullanılan Yöntemler.....	311
11.3.2. Önerilen Sistem.....	312
11.3.2.1. Filtreleme.....	313
11.3.2.2. Karar Verme.....	313
11.4. Siber Güvenlik Bakış Açısıyla Değerlendirme.....	314
11.4.1. Genel Değerlendirmeler.....	314
11.4.2. Siber Güvenlik ve Mahremiyet Çözümleri.....	316
11.5. Değerlendirmeler.....	317

12. BÖLÜM

SİBER GÜVENLİK TEKNOLOJİLERİ

12.1. Giriş.....	325
12.2. Güvenlik Teknolojileri.....	326
12.2.1. Anti-virüs Yazılımları.....	326

12.2.2. Anti-casus Yazılımlar.....	327
12.2.3. Mesaj Sağanağı (Anti-spam) Filtreler.....	329
12.2.4. Saldırı Tespit ve Önleme Sistemleri (IDS/IPS).....	330
12.2.5. Güvenlik Duvarları ve Hibrit Sistemler.....	331
12.2.6. Şifreleme Teknolojileri.....	331
12.2.7. Açık Anahtar Altyapısı.....	332
12.2.8. Erişim Kontrol Teknolojileri.....	333
12.3. Güncel Siber Güvenlik Teknolojileri.....	334
12.3.1. Sosyal Siber Güvenlik Teknolojileri.....	334
12.3.2. Nesnelerin İnterneti için Siber Güvenlik Teknolojileri.....	335
12.3.3. Sağlık için Siber Güvenlik Teknolojileri.....	336
12.3.4. Büyük Veri için Siber Güvenlik Teknolojileri.....	336
12.7. Değerlendirmeler.....	338

13. BÖLÜM

BİYOMETRİK SİSTEMLERDE GÜVENLİK VE MAHREMİYET

10	13.1. Giriş.....	348
	13.2. Biyometrik Tanıma ve Bireysel Çeşitliliğin Temelleri.....	349
	13.3. Biyometrik Sistemler ve Güvenilirlik.....	352
	13.4. Biyometrik Sistem Güvenliğini Tehdit Eden Unsurlar.....	354
	13.5. Biyometrik Saldırı Modelleri.....	361
	13.6. Biyometrik Sistemlerin Güvenliği ve Mahremiyeti.....	364
	13.6.1. Veri Edinim Aşamasında Oluşabilecek Tehditler ve Çözüm Önerileri.....	365
	13.6.2. Yazılım Bileşenlerini Tehdit Eden Unsurlar ve Çözüm Önerileri.....	366
	13.6.3. Depolama Aşamasında Oluşabilecek Tehditler ve Çözüm Önerileri.....	369
	13.7. Biyometrik Sistemlerinde Güvenlik Standartları.....	370
	13.8. Yeni Trendler.....	371
	13.8.1. Davranışsal Biyometri.....	372
	13.8.2. Sosyal Ağ Biyometrisi: Sosyometrik Biyometri.....	374
	13.8.3. Siber Antropolojinin Gerçeği: Toplumsal Biyometri.....	376
	13.8.4. Kuantum Biyometrisi.....	378
	13.9. Değerlendirmeler.....	379
	YAZARLARIN ÖZGEÇMİŞLERİ.....	387

EDİTÖRDEN

Bilgi Güvenliği Derneği (BGD), kuruluşundan bugüne kadar ülkemizin **bilgi ve siber güvenliği ile savunmasının** gelişimine katkı sağlamakta, birikimini çevreye aktarmakta, bilgi güvenliği alanında açık kaynak yaklaşımını benimseyen ve bu kapsamda içerik üretilmesine ve geliştirilmesine destek vermekte, bunları yaymakta, paylaşmakta ve kamuoyunun kullanımına sunmaktadır. Düzenlediği ulusal ve uluslararası etkinliklere ait bildiri kitapları serisi, hazırladığı raporlar, taslak strateji dokümanları, eylem planları vb. bunların başında gelmektedir. **Siber Güvenlik ve Savunma Kitapları Serisi** ise BGD'nin ülkemizin siber güvenliğine önemli bir katkısıdır.

Tehditlerin, saldırıların ve açıklıkların artması, boyut ve yön değiştirmesi, farklılaşması, siber tehdit ekosisteminin gittikçe güçlenmeye başlaması, kritik altyapıların hedef haline gelmesi, bilgi ve kaynak hırsızlıklarının çoğalması, yeraltı yapıların etkinleşmesi, siber saldırıların artık savaşa dönüşmesi, siber suç ve suçlarının çoğalması, siber terörün yaygınlaşması vb. olumsuzlukların hızla artması, yapılacak mücadele, alınacak önlem ve karşı koymak için yaklaşımlara duyulan ihtiyacı artırmıştır. Kapsamlı bir mücadele için; ulusal strateji ve eylem planlarına, araştırma merkezlerine, gelişmiş altyapı ve araçlara, lisans ve lisansüstü programlara, nitelikli insan kaynağına, yerli ve milli ürünlerin geliştirilmesine, siber güvenlik ve savunma ekosisteminin oluşturulmasına, ulusal siber olaylara müdahale ekiplerinin sayısının ve niteliğinin artırılmasına, Ulusal Siber Olaylara Müdahale Merkezinin (USOM) kapsamının büyütülmesine, siber güvenliğin ulusal güvenlikle bütünleşmesine ihtiyaç vardır. Duyulan bu ihtiyacı bir nebze de olsa karşılamak için bu kitap serisi hazırlanmıştır. Bu kitap serisinde, 100'e yakın konu başlığı irdelenmektedir. Her bölümde, farklı bir konu siber güvenlik ve sa-

vunma kapsamında ele alınmakta, değerlendirilmekte ve alınması gereken önlemlere yer verilmektedir.

Bu kitap serisinde sunulan konu başlıkları, ülkemizde bu alanda çalışan akademisyenler, uzmanlar ve çalışanlar ile paylaşılmış ve bu kitap serisine katkı sağlamaları istenilmiştir. Zamanı uygun olan, katkı vermek isteyen uzman veya akademisyenler belirlenen bir konuda bölüm yazarı olmaları için davet edilmişlerdir. Belirlenen süre içerisinde bölümlerini tamamlayan yazarlarımızın eserleri ise uygun olan ciltlerde basılmaktadır. Bundan sonraki süreçte, belirlenen diğer konular belirli sürelerde tamamlanıp takip eden ciltlerde yayımlanacaktır. Siber güvenlik ve savunmaya çok kapsamlı bir bakış sunmayı amaçlayan ve farklı başlıkları bir araya getiren bu kapsamlı eserin, ülke siber güvenliğimiz ve savunmasına katkı sağlaması beklenmektedir.

Kitap serimizin üçüncü cildinde, 13 farklı bölüm sunulmuştur. Siber güvenliğin farklı açılardan irdelendiği bu ciltte; siber güvenliğin kapsamı ve boyutu, "standartlar ve uygulamalar" açısından değerlendirilmiştir. Ayrıca, alınabilecek önlemler, karşılaşılan yeni riskler ve problemlere yer verilmiş, karşılaşılabilecek risklere dikkat çekilmiş ve sonuçta alınması gereken önlemler ve yapılması gerekenler özetlenmiştir. Her bir bölüm; ülkemizde bu alana katkı sağlayan, bu alanda eğitim almış, tez hazırlamış, çalışmalar yapmış değerli akademisyen, kamu çalışanı ve üst düzey yöneticiler tarafından hazırlanmıştır. Her bir bölüm, birbirinden bağımsız olarak hazırlansa da konu bütünlüğü ve devamlılığının sağlanmasına mümkün olduğunca dikkat edilmiştir. Her bölüm editörler olarak tarafımızdan değerlendirilmiş, yazarlara konu içeriği ve başlıklarla ilgili olarak önerilerde bulunulmuş, düzeltmeler yapılması istenilmiş ve sonuçta yapılan değişiklikler dikkate alınarak bu kitap hazırlanmıştır. Kitapta yazılan bölümler tekrar tekrar kontrol edilmiş, yapılan çalışmalar ise her bölümün sonunda bölüm yazarları tarafından değerlendirilmiştir.

Bu kitabın, siber güvenlik ve savunma konusunda yapılacak çalışmalara ışık tutması, yeni çalışmaların yapılmasına katkı sağlaması, bu konuda yapılacak olan işbirliklerini geliştirmesi, bu konunun boyutunun ve kapsamının daha iyi anlaşılmasına katkı sağlaması ve en önemlisi ise bilgi güvenliği ve siber güvenlik alanında duyulan ihtiyacı karşılamanın yanında açık kaynak olarak sunulması ile de kaynaklara erişimi kolaylaştırıcı **bir başvuru kitabı serisi** olması

beklenmektedir. **Bu eser serisi açık kaynak olarak**, Bilgi Güvenliği Derneği internet sayfasında (www.bilgiguvenligi.org.tr) yayımlanmaktadır.

Kitap bölüm yazarlarımız; alan uzmanlıklarına göre her bir bölümü hazırlamışlar, kişisel bilgi birikimlerini hazırladıkları bölümlerde sunmuşlar, eserlerinin açık kaynak olarak yayımlanmasını kabul etmişler ve bu kitabın basımı ve dağıtımı ile ilgili olarak herhangi bir telif hakkı talep etmemişlerdir. Yazarlarımıza, bu kitap serisinin editörü olarak çok özel teşekkürlerimizi ve şükranlarımızı sunarız.

Kitabın titizlikle hazırlanmasında, kontrolünde ve basılmasında başta yazarlarımız olmak üzere emeği geçen tüm paydaşlarımıza, kitap serisi fikrimizi hayata geçiren Bilgi Güvenliği Derneği Yönetim Kuruluna teşekkürlerimizi sunarız.

Prof. Dr. Şeref SAĞIROĞLU
BGD Kurucu Üyesi ve II. Başkanı
Gazi Üniversitesi MF Bilgisayar Mühendisliği Bölüm Başkanı
FutureTech Genel Müdürü

BİLGİ GÜVENLİĞİ DERNEĞİ'NDEN

Bilgi Güvenliği Derneği (BGD); 22 Temmuz 2007 tarihinde, Bilgi Güvenliği ve Siber Güvenlik alanında toplumun her kesiminde bilgi ve bilinç düzeyini arttırmak, bu konu ile ilgili teknolojik gelişmeleri izlemek, yerli ve milli teknolojilerin geliştirilmesine katkı sağlamak; bireysel, kurumsal ve ulusal düzeydeki riskler konusunda farkındalık oluşturmak ve kamu-sektör-üniversite işbirliklerini geliştirmek amacı ile kurulmuştur.

BGD'nin vizyonu; "bilgi güvenliği alanında ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal sivil toplum kuruluşu olmaktır." BGD vizyonu doğrultusunda; tüm paydaşlarla işbirliği yaparak mevzuatın oluşturulmasında ve geliştirilmesinde aktif rol almakta, gerçekleştirdiği konferans, sempozyum, çalıştay ve eğitimler, yayımladığı rapor ve yazılar ile farkındalığın oluşmasına ve bunun davranışa dönüştürülmesine katkılar sağlamaktadır.

Derneğimiz bu kapsamda; "Ulusal Siber Güvenlik Strateji Belgesi" ve "Ulusal Siber Güvenlik Eylem Planı" hazırlanmasına öncülük etmiş, hazırladığı taslak metinler kabul görmüş ve sonuçta ülkemizin siber güvenlik stratejisi ve eylem planlarının gecikmeden yayımlanmasına katkı sağlamıştır. Aynı zamanda; bu alanda nitelikli insan kaynağı yetiştirilmesi, mesleki yeterliliklerin belirlenmesi, kamu-endüstri-üniversite işbirliklerinin geliştirilmesi, kümelenme çalışmalarının başlaması gibi önemli politika ve stratejilerin oluşturulmasında etkin rol üstlenmektedir.

BGD, "Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı", "Ulusal Siber Güvenlik Stratejisi Çalıştayı", "Veri Merkezleri ve Siber Güvenlik Çalıştayı", "Siber Güvenlik Hukuku Çalıştayı", "Mobil Dünyada Çocuk ve Gençlerin Güvenliği Sempozyumu", "IPv6 Konferansı", "Kritik Enerji Altyapılarının Korunması Sempozyumu", "Ulusal Siber Terör Konferansı", "Siber Güvenlik Yaz Kampı" gibi

etkinlikleri düzenleyerek ve destekleyerek bilgi güvenliğine ihtiyaç duyulan her alanda çalışmalar yürütmüştür. Cumhurbaşkanlığı, Milli Eğitim Bakanlığı, Ulaştırma ve Altyapı Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu, Sosyal Güvenlik Kurumu ve Üniversiteler gibi farklı paydaşlar ile çalışmalar yürütmektedir.

BGD, **CyberMag Dergisi** ile toplumun tüm kesimlerine ulaşmaya çalışmaktadır. 2019 yılında 12'ncisini düzenleyeceğimiz "Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı" kısaca **ISCTurkey Konferansı** olarak bilinen uluslararası etkinlik ile kurulduğu günden bu yana kamu kurumları, özel sektör ve üniversiteleri bir araya getirmeyi başarmıştır.

Bununla birlikte, bilgi güvenliği ve siber güvenlik alanında **ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal sivil toplum kuruluşu olan Bilgi Güvenliği Derneği**, bünyesinde oluşturulan BGD Genç ile; bireysel, kurumsal, ulusal ve evrensel boyutlarda bilgi ve iletişim güvenliği alanında teknik, bilimsel, sosyal ve kültürel faaliyetler yürütmek, orta ve yüksek öğrenim gören genç üyelerimizin mesleki gelişimini artırmak, siber güvenlik alanında farkındalık oluşturmak, ülkemizin siber güvenlik uzman kaynağını oluşturmak için gençlerimizin bu alana ilgisini artırmak için faaliyet göstermektedir.

ISCTurkey etkinlikleri, Gazi Üniversitesi, İstanbul Teknik Üniversitesi ve Ortadoğu Teknik Üniversitesi işbirliği ile düzenlenmekte, Ulaştırma ve Altyapı Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu tarafından sürekli desteklenmektedir. Bu etkinlik, Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından "Avrupa Siber Güvenlik Ayı" platformu etkinliklerine dâhil edilen ilk ve tek etkinliktir. Ayrıca, düzenlendiği ilk yıldan beri ülkemizin siber güvenlik alanındaki bilimsel ve sektörel çalışmaların paylaşıldığı, üniversite-kamu-endüstri işbirliğinin geliştirildiği, kamunun bilgilendirildiği, paydaşların eğitildiği, tüm bilim insanları, araştırmacılar ve sektörel uygulayıcılar arasında bilgi alışverişinin sağlandığı ülkemizde bu alandaki en önemli etkinliktir.

Şubat 2019'da yeni bir yönetim kuruluyla göreve başlayan BGD Yönetimi, yapılan çalışmalara yenilerinin eklenmesi, açık kaynak olarak paylaşılacak olan çalışmaların artması ve ülkemizin bu alanda

ihtiyaç duyduğu Türkçe kaynak ihtiyacına katkı sağlanmasını desteklemektedir.

Bu kitabın hazırlanmasında katkı sağlayan başta editörlerimize, hiç bir beklenti içerisinde olmadan bölüm yazan ve bunu kamuoyu ile ücretsiz paylaşılması konusunda destek veren saygıdeğer yazarlarımıza, destekleyicimize ve bugüne kadar ülke bilgi güvenliği ve siber güvenliğinin gelişimine katkı sağlayan BGD yöneticilerimize ve üyelerimize bu vesile ile şükranlarımı sunarım.

Bu kitap serisinin üçüncüsünün, ülkemiz siber güvenlik ve savunma çalışmalarına katkı sağlaması dileğiyle.

Ahmet Hamdi ATALAY
Bilgi Güvenliği Derneği YK Başkanı

ÖN SÖZ

Günümüzde siber güvenlik, beşinci savaş ortamı olarak kabul edilmenin ötesinde tüm ülkeler için ulusal güvenliđin ayrılmaz ve en önemli bileşeni olarak değerlendirilmektedir.

Yerli, güvenilir, yenilikçi ve yüksek kaliteli Siber Güvenlik çözümleri geliştirerek ülkemizin siber güvenliđinin sağlanmasında ana unsur; uluslararası pazarlarda güçlü ve güvenilir Siber Güvenlik teknoloji ve hizmet sağlayıcısı olmak vizyonu ile çalışmalarını yürüten HAVELSAN, ülkemizin siber uzayda güvenliđini sağlayacak bir mükemmeliyet merkezi olmak, ülkemizin yetenek ve kaynaklarının etkin kullanılmasına öncülük etmek adına var gücüyle çalışmalarını sürdürmektedir.

Bir Türk Silahlı Kuvvetlerini Güçlendirme Vakfı şirketi olan HAVELSAN tarafından hayata geçirilen Siber Savunma Teknoloji Merkezi çatısı altında siber güvenlik operasyon merkezi hizmetleri, kurumsal siber güvenlik danışmanlık ve destek hizmetleri, güvenlik analiz ve test hizmetleri, siber güvenlik eğitimleri ve yerli siber güvenlik ürünleri geliştirme faaliyetleri yürütölmektedir.

Siber güvenlik alanında ülkemizin nitelikli insan kaynađını artırmak için Türkçe kaynak ihtiyacının en az bu alanda verilen eğitimler kadar değerli olduđunun bilincinde olan HAVELSAN, bu ihtiyacı karşılamada katkı sağlayacak değerli bir yayın olarak gördüğü bu kitabı desteklemektedir.

Ahmet Hamdi ATALAY
HAVELSAN Genel Müdürü