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 Atila 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

3. BÖLÜM
BİLGİ, ÜRÜN VE SİSTEM AÇISINDAN SİBER GÜVENLİK STANDARTLARI

4. BÖLÜM
SİBER GÜVENLİKTE ASKERİ STANDARTLAR KAPSAMINDA AQAP İNCELEMESİ

5. BÖLÜM
YAZILIM TANIMLI AĞLAR VE SİBER GÜVENLİK

6. BÖLÜM
WEB UYGULAMA ZAFİYETLERİ VE ÖNLEMLER

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 suçlularının 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 arttırılmasına, 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 yayımlanasına 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 katkılar 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 katkılar 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 güvenliğin ayrılmaz ve en önemli bileşeni olarak değerlendirilmektedir.

Yerli, güvenilir, yenilikçi ve yüksek kaliteli Siber Güvenlik çözümleri geliştirerek ülkemizin siber güvenliğinin sağlanmasında ana unsur; uluslararası pazarlarda güçlü ve güvenilir Siber Güvenlik teknoloji ve hizmet sağlayıcısı olmak vizyonu ile çalışmalarını yürüten HAVELSAN, ülkemizin siber uzayda güvenliğini 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 yürütülmektedir.

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

Ahmet Hamdi ATALAY
HAVELSAN Genel Müdürü