

Haziran 2019/Sayı 1

Kadir Has Üniversitesi Siber Güvenlik ve Kritik Altyapı Koruma Uygulama ve Araştırma Merkezinde veri bilimi çalışan ekibimiz, dünyanın en büyük veri bilimi yarışma platformu Kaggle'da Microsoft'un düzenlemiş olduğu toplam 50.000 USD ödüllü "Kötücül Yazılım Tespit" (Malware Prediction) yarışmasında dünya çapında 2426 ekip arasından beşinci olarak 1000 USD ödül kazandı.



Kaggle, yayınlamış olduğu veri kümeleri ve düzenlemiş olduğu yarışmalarla dünya genelinde veri bilimi alanındaki araştırma geliştirme çalışmalarına yön vermektedir.

Etkinlik Duyurusu: 6. Uluslararası Yönetim Bilişim Konferansı: Bağlantılılık ve Sibergüvenlik (Connectedness & Cybersecurity)

6. Uluslararası Yönetim Bilişim Sistemleri Konferansı (IMISC2019) 9-12 Ekim 2019 tarihleri arasında, İstanbul'da Kadir Has Üniversitesi'nde gerçekleştirilecektir. Yönetim Bilişim Sistemleri alanında çalışan bütün disiplinlerden akademisyen, kamu, özel sektör, STK ve uygulayıcıların araştırma ve deneyimlerini paylaştıkları konferansın bu yılki teması: Bağlantılılık ve Sibergüvenlik (Connectedness and Cybersecurity) olarak belirlenmiştir.

Konferans websitesi için [linke tıklayın](#)

Analiz: Siber Dünyada Yapay Zekâ Kullanımı: Mucize mi, Tehdit mi?

Dijital çağda siber güvenlik önemli bir risk unsuru. Son dönemlerde kritik altyapıları hedef alan siber saldırılar, veri ihlalleri, kimlik hırsızlıkları gibi suçlar bireyden topluma doğru giderek büyüyen bir tehdit unsuru haline geldi. Bu suçlar milyonlarca kişiyi etkilediği gibi birçok organizasyonu da tesiri altına almaya başladı. Cybersecurity Ventures tahminlerine göre, 2021 yılında siber suçların maliyeti 6 trilyon doları bulabilir. Siber saldırılar giderek daha fazla geliyor ve Nesnelerin İnterneti dünyasının hacmi genişledikçe saldırganlar yeni açıklar keşfediyor. Bu çerçevede, özel sektör ve akademi dünyasında en sık konuşulan konulardan biri de yapay zekâ (AI) teknolojisinin siber dünya ve bu bağlamda siber güvenliği ve tehditleri nasıl dönüştüreceği.

Yazının devamı için [linke tıklayınız](#).

Haber: Mobil Uygulamaların Dörtte Üçünde Kişisel Verilerinizi Tehlikeye Atabilecek Bir Güvenlik Açığı Var

Akıllı telefonlarda kullandığımız mobil uygulamalar alışverişlerimizden, günlük attığımız adım sayısını takibe kadar sayısız yönde hayatımızı kolaylaştırıyor. Ancak bu uygulamalar sanıldığı kadar güvenli mi? ZDNet'te yayınlanan habere göre mobil uygulamaları telefonumuza indirmeden önce iki kere düşünmek gerekiyor. Habere göre, araştırmacılar mobil uygulamaların dörtte üçünde güvensiz veri depolamasına ilişkin güvenlik açıklarının var olduğunu belirtiyor.

Haberin devamı için [linke tıklayınız](#)



81 ilde 81 Siber Kahraman Siber Güvenlik Yaz Kampı

Bize Ulaşın

Kadir Has Üniversitesi Siber Güvenlik ve Kritik Altyapı Koruma Uygulama ve Araştırma Merkezi

Adres: Kadir Has Caddesi Cibali / İSTANBUL 34083

Tel: +90 (212) 533 65 32

E posta: ccip@khas.edu.tr

Websitesi: <https://ccip.khas.edu.tr/>

Cybersecurity Ventures tahminlerine göre, 2021 yılında siber suçların maliyeti 6 trilyon doları bulabilir.

Etkinlik: 81 ilde 81 Siber Kahraman Siber Güvenlik Yaz Kampı Başarıyla Tamamlandı

81 ilde 81 Siber Kahraman Projesi tarafından, T.C Cumhurbaşkanlığı Dijital Dönüşüm Ofisi himayelerinde ve Türkiye Siber Güvenlik Kümelenmesi desteğiyle Kadir Has Üniversitesinde gerçekleştirildi. Etkinliğe, 19 farklı ilden, 40 tane lise öğrencisi katıldı. Ücretsiz verilen eğitim sonunda sertifika alan katılımcılar siber güvenliğe ilişkin teknik ve teorik bilgiler kazanmış ve bu bilgileri uygulamalı olarak hayata geçirme şansı buldu.



Analiz: Dijital Soğuk Savaşın Yeni Hedefi Kritik Altyapılar mı?

Siber dünya, insan yaşamının ve modern ekonominin işleyişinin önemli bir parçası haline geldi. Symantec'in verilerine göre, 2025 yılında IoT'nin hacmi (Nesnelerin İnterneti) 21 milyar cihaza ulaşacak. Bu çerçevede, IoT devriminin günlük hayatımıza getirdiği, akıllı şebekeler, akıllı şehirler ve otonom araçlar gibi çok sayıda faydadan söz etmek mümkün. Bununla beraber, bu yeni dünyanın keşfi, birçok güvenlik zafiyetini de beraberinde getirdi. Buna ek olarak, bu dönüşümden derinden etkilenen kritik altyapılar da siber risklere ve saldırganlara karşı doğrudan tehdit altında. Öte yandan, son dönemde, jeopolitik gerginliklerin artmasına paralel olarak, kritik altyapılardaki siber güvenlik tehditleri önemli bir araştırma konusu haline geldi. Acaba, kritik altyapılar "dijital soğuk savaşın" yeni unsuru haline mi geldi?

Yazının devamı için [linke tıklayınız](#)