MARMARA
BELEDİYELER BİRLİĞİ

Bilgi Teknolojileri Platform Bülteni

Ekim-Aralık 2018 | Sayı 4

AÇIK KAYNAK KOD NEDİR, SİZE DE GEREKLİ Mİ? S: 5

ASELSAN'DAN GOLED EKRAN TEKNOLOJİSİ S: 7

STARBUCKS KRİPTO PARA PİYASASINA GİRİYOR S: 13

Editörden...

Marmara Belediyeler Birliği Bilgi Teknolojileri Platformu, MBB üye belediyelerinin bilgi işlem daire başkanları ve bilgi işlem müdürlerinden oluşmaktadır. Belirli periyotlarla bir araya gelen platform üyeleri ile güncel konuların yanı sıra bilgi işlem birimlerinde yaşanılan sıkıntılar ve bu sıkıntıların çözümü istişare edilmektedir. Bilgi eksikliği yaşanılan konularda da eğitim ve seminerler düzenlemektedir. Bunların yanı sıra platform üyelerinin desteğiyle 3 ayda bir platform bülteni yayınlamaktadır.

Bilgi Teknolojileri Platform Bülteninin yılın son sayısında siber güvenlik ve blockchaine ağırlık vermenin yanı sıra gündemi bir hayli meşgul eden yerli Pardus dağıtımının felsefesini oluşturan açık kaynak kod ile ilgili bir yazıya yer verdik. Bunun yanı sıra ASELSAN'ın Sabancı Üniversitesi ile işbirliği sonucu ilginizi çekeceğini düşündüğümüz bir teknoloji haberini de bültenimizde bulabilirsiniz.

En dikkat çekici haber ise Starbucks'tan geldi. Kahve eşliğinde kod yazanlar için sevindirici bir gelişmeyi de 4. Sayımızda okuyabilirsiniz.

Bu da olsaydı güzel olurdu diyeceğiniz ne varsa hepsine talibiz. Önerileriniz ve eleştirilerinizle büyüyecek bültenimiz için katkılarınızı bekliyoruz.

Editör
Yunus Demiryürek
MBB Bilgi Teknolojileri Koordinatörü

KÜNYE

Bu bülten yılda 4 adet yayınlanmak üzere Marmara Belediyeler Birliği Bilgi Teknolojileri Platformu tarafından hazırlanmıştır.

Genel Yayın Yönetmeni | M. Cemil Arslan

Editör | Yunus Demiryürek

Katkıda Bulunanlar

Kerem Ulusoy

İsmail Hakkı Polat

Sayı | 4, 2018

Bu sayıda...

TÜBİTAK'A İŞ DÜNYASINDAN ATAMALAR YAPILDI

Cumhurbaşkanlığı Hükümet Sistemi'ne geçilmesiyle birlikte yönetim kurulu ataması gerçekleşmesi beklenen TÜBİTAK için beklenen görev paylaşımları, dün yayınlanan belgeyle resmi olarak yapıldı.

Mevcut sisteme geçilmeden önce 'TÜBİTAK Bilim Kurulu' olarak adlandırılan bir üst karar organı bulunan TÜBİTAK, Cumhurbaşkanı Erdoğan'ın resmi atamasıyla birlikte yönetim kurulu sistemine geçti. Bu dönemden sonra direkt olarak Sanayi ve Teknoloji Bakanlığı'na bağlı olarak çalışacak olan TÜBİTAK'ta 3 yıl süre ile görev yapacak üyeleri açıklandı.

Daha önce Bilim Kurulu'nun başkanlığını yürüten Prof. Dr. Hasan Mandal, yeni dönemde de başkanlık görevine devam edecek. Listede en dikkat çeken isimse Arçelik Üretim ve Teknolojiden sorumlu Genel Müdür Yardımcısı Cemal Şeref Oğuzhan Öztürk oldu. 35 yıldan fazla süredir sanayi alanında çalışmaları bulunan Öztürk, İstanbul Teknik Üniversitesi mezunu, uçak ve yüksek makine mühendisi. Bu bağlamda kurulun hem iş dünyasında hem de yeni dönemdeki inovatif çalışmalarda önemli roller alacak.

Listede iş dünyasından dikkat çeken bir başka isim de Medyasoft Yönetim Kurulu Başkanı ve Genel Müdürü Mehmet İhsan Taşer oluyor. Halen TÜBİMER'in İtiraz Kurulu Üyesi olarak görevine devam eden Taşer, bu güne değin birçok bilişim şirketin üst düzey yöneticilik yaptı.

Cumhurbaşkanlığından:
Karar Sayısı: 2018/198

3 sayılı Cumhurbaşkanlığı Kararnamesinin 2 ve 3 üncü maddeleri ile 4 sayılı Cumhurbaşkanlığı Kararnamesinin 586 ncı maddesi gereğince, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Yönetim Kurulu Üyeliklerine ekli listede yer alan kişiler atanmıştır.

23 Ekim 2018

Recep Tayyip ERDOĞAN
CUMHURBAŞKANI

23/10/2018 TARİHLİ VE 2018/198 SAYILI KARARIN EKİ
LİSTE

1- Prof. Dr. Mehmed ÖZKAN
2- Prof. Dr. Metin ORHAN
3- Mehmet İhsan TAŞER
4- Lütfü Haluk BAYRAKTAR
5- Cemal Şeref Oğuzhan ÖZTÜRK
6- Aydın ÜNAL

Kaynak: **http://quq.la/OVMhr**

AÇIK KAYNAK KOD NEDİR, SİZE DE GEREKLİ Mİ?

Sıkça duyduğumuz "açık kaynak kodlu yazılım" tam olarak ne anlama geliyor? Size gerçekten lazım mı?

"Açık kaynak kodlu yazılım" terimini sıkça duyuyoruz. Android, Linux gibi yazılımların açık kaynak kodlu olduğunu biliyoruz. Peki açık kaynak kodlu tam olarak ne demek ve açık kaynaklı yazılımlar sizi gerçekten de ilgilendiriyor mu?

Açık kaynak kodlu yazılım nedir?

Programlar, yani .exe dosyaları, binlerce "kaynak kodu" satırından derlenmiştir. Programlama dilini bilmeyenler için fazlasıyla karışık görünebilecek bu kodlar, bir uygulama dosyası olarak "derlenir". Derleme işleminden sonra artık kaynak koduna ihtiyaç duyulmaz.

Dolayısıyla iTunes gibi bir yazılımı çalıştırırken kaynak kodunu görmez, sadece ürünün son halini görürsünüz. Çoğumuz için bu zaten olması gereken şeydir. Açık kaynak kodlu yazılımlar ise kaynak kodlarıyla beraber yayınlanırlar. Geliştirici, bazen onları derleyip, kaynak kodlarının yanında bir uygulama dosyası da sunabilir. Bazı durumlarda ise derleme işi kullanıcıya bırakılır.

Açık kaynak kodlu yazılım, kaynak kodları herkese açık olan yazılımdır. Bunun anlamı, onun üzerinde herhangi bir değişiklik yaparak kendi sürümünüzü meydana getirebileceğinizdir.

Neden açık kaynak kodlu yazılım?

Normalde bir programı çalıştırdığınızda onun kaynak kodlarına erişemezsiniz. Yani uygulamanın size sunduğu işlevleri nasıl sunduğunu göremez, onun özelliklerinde herhangi bir değişiklik yapamazsınız.

Bunu taşındığınız, yeni yapılmış bir ev örneğine benzetebiliriz. Evin her şeyi hazırdır, elektrik hattı, su boruları ve diğer altyapı duvarların arkasına gizlenmiştir. Örneğin elektrik hattınızda bir sorun meydana geldiğinde, hatlara erişemiyorsanız yapabileceğiniz çok fazla şey yoktur. Elektrikçinin gelip sorunu gidermesinden etmesinden başka.

Kapalı kaynak kodlu yazılımlarda da durum buna benzer. Bu tür programlarda programın geliştiricisine bağlısınızdır, herhangi bir sorun gördüğünüzde onu düzeltmeniz mümkün olmaz.

AÇIK KAYNAK KODLU YAZILIMIN AVANTAJLARI

Açık kaynak kodlu yazılımların faydaları, sadece programcılara dokunmaz. İşte açık kaynak kodlu yazılımın faydalarından bazıları.

Açık kaynak kodlu yazılımlar, programcı topluluğunun gelişimini sağlar. Bu sayede eğitime, yaratıcılığa ve ilham almaya yardımcı olur.

Açık kaynak kodlu yazılımlarda örneğin bir açık bulunduğunda, onunla ilgilenen çok daha fazla kişi olduğundan çok daha çabuk kapatılabilir. Kapalı kaynak kodlu yazılımlarda ise uzun bir süre beklemeniz gerekebilir.

Yazılımların farklı çeşitlerinin ortaya çıkmasını sağlar. Örneğin Mozilla Firefox, Chromium ve Linux'dan türeyen birçok yazılım var.

Yazılım geliştiricisinin PC'nizde şüpheli işler çevirmediğinden emin olmanızı sağlar. Kaynak kodu kapalı bir yazılımın yaptığını iddia ettiği şeyleri gerçekten güvenilir yoldan yaptığını anlamanın çok fazla yolu olmayabilir.

BİTCOİN'İN CAN SİMİDİ: Bakkt

İsmail Hakkı Polat - Kadir Has Üniversitesi

Ağustos ayı başında sessiz sedasız hizmete başlayan Bakkt, hayatın günlük akışının içinde kullanım arayışında olan Bitcoin için bir can simidi olabilir.

Yaz ayları boyunca Kriptopara piyasalarında en çok konuşulan konu olan ve yeni bir boğa sezonu için işaret fişeği olacağı söylenen ABD'li kimi yatırım kuruluşlarının Bitcoin için yaptığı ETF (Borsa Yatırım Fonu) başvuruları, geçtiğimiz hafta ABD Menkul Kıymetler ve Borsa Komisyonu SEC'in yedi başvurunun hepsini reddetmesi, yatırımcıları hüsrana uğrattı. Komisyonun ret gerekçeleri arasında KriptoPara borsalarının denetlenebilirliğinin azlığı ve manipülasyonlara açık olması gibi makul hususlar yer almasına karşın, ret duyurusunun hemen ardından başvuruları bir kez daha gözden geçirebileceğini duyurması da kafaları karıştırdı.

Aslında bu durum, komisyon üyesi Hester Pierce'in de daha önceki ret kararındaki "SEC, ürünün kendisine değil piyasadaki işleyişine göre kararını vermeliydi" şeklindeki muhalefet şerhiyle düşünüldüğünde KriptoParaların sonsuza dek finans piyasalarının dışında tutulması pek de mümkün görünmüyor.

Bu bağlamda, komisyonun Eylül ayında değerlendirmeye alacağı 2 ETF başvurusu daha var ve özellikle Chicago Vadeli İşlemler Borsası'nın (CBOE) başvurusuna ilişkin karar heyecanla beklenmekte. SEC erteleme kararı vermezse 30 Eylül'e kadar sonuçlandırılması gereken başvurunun, kendi içindeki yatırım piyasasının düzenleme sorumluluğu olan bir kurum tarafından yapılması çok önemli ve buna ek olarak komisyonun ret gerekçelerindeki kaygılarını giderecek argümanlar bulunduğu söylenmekte.

SEC'in önümüzdeki dönemde de sayısı artarak sürecek Bitcoin ETF başvuruları için eninde sonunda vermesi beklenen olumlu karar, ellerindeki Bitcoinlerin değerlenmesi hevesindeki KriptoPara yatırımcıları için kuşkusuz spekülatif bir 'nefes alma' imkanı sağlayabilir.

Ancak Bitcoin'in temel sorunu, kuruluşundan bu yana neredeyse 10 yıl geçmesine karşın (sınırlı bir değer saklama ve transfer işlevinin dışında) günlük hayatın akışında yaygın bir kullanım alanı bulamamış olması.

Bitcoin'i geniş kitlelerle buluşturabilecek böyle bir fırsat ise, Ağustos ayında sessiz sedasız hizmete girdi. New York Stock Exchange (NYSE) sahipliğindeki Kıtalararası Borsalar Birliği (ICE) tarafında kurulan Bakkt adlı girişim, Bitcoin'in günlük hayatta bir ödeme aracı olarak kullanımını yaygınlaştıracak gibi görünüyor.

Kabaca "Bitcoin temelli bir alışveriş ödeme sistemi" olarak tanımlayabileceğimiz Bakkt'ın, bu konuda kendinden önce bunu deneyen Bitpay, Xapo gibi bu işin öncülerinden farkı, Starbucks ve Microsoft gibi yaygınlığı yüksek iş ortaklarıyla işe başlaması ve SEC'in ETF ret kararlarında vurguladığı fiyat istikrar riskini iş ortaklarına yansıtmadan kendi ekosistemi içinde bir iş modeliyle yönetmesi. Bu sayede örneğin Starbucks, (aynı kredi kartı ödemelerindeki gibi) Bitcoin ile hiç bir ilişkisi olmadan kendi ödemesini dolar olarak alıp kahve satışlarına devam edecek ve Bakkt da tüm bu ekosistem için bir tampon vazifesi görerek arka plandaki süreci yönetecek ve düzenleyecek. Ayrıca Bakkt, Bitcoin'i bir para birimi (currency) olarak değil bir dijital varlık (asset) olarak konumladığını ve kendi hizmetleri üzerinden yapılacak tüm işlemlerin 'fiziksel' Bitcoin karşılığının ayırılacağını da açıklayarak düzenleyici kurumlara da rahatlatıcı bir mesaj verdi.

Kasım ayında hizmet vermeye başlayacak girişim, iş ortaklarını arttırır ve günlük hayatta giderek yaygınlaşan bir kullanım miktarına ulaşırsa bu, Bitcoin için yeni bir dönüm noktası olabilir ve hatta bu modelle çalışacak yeni Kriptopara girişimlerine de ilham verebilir.

Kuşkusuz böylesi bir kullanım yaygınlığının, devletlerin itibari paraları ile eninde sonunda karşı karşıya geleceğini de gözden uzak tutmamak lazım. Tabii o zamana geldiğince, atı alan Üsküdar'ı geçmiş de olabilir!

ASELSAN'DAN GOLED EKRAN TEKNOLOJİSİ

ASELSAN ve Sabancı Üniversitesi'nin ortak işbirliği sonucunda önemli bir ekran teknoloji kazanılmış oldu.

Elmas Projesi kapsamında üretilen grafen ekran dünyanın en yüksek çözünürlüğüne sahip ekranı olma özelliğine sahip.

ASELSAN GRAFEN EKRAN: GOLED

Savunma Sanayii, "Ekran Teknolojileri" adı altındaki ilk projesini ve prototiplerini "ELMAS Projesi" adıyla bizlerle buluşturdu. ASELSAN ve Sabancı Üniversitesi Nanoteknoloji Araştırma ve Uygulama Merkezi'nde kurulan altyapılar sayesinde Türkiye'de ilk defa OLED ekran ve grafen malzeme üzerine çalışmalar yapıldı.

Bu dev çalışmanın bir ödülü olarak askeri standartlarda, arka ışık olmadan çalışabilen (OLED çalışma mantığı) ilk monokrom minyatür ekranlar üretildi. Üstelik OLED ekranların işlenme süreçleri tamamen özgün bir şekilde geçekleştirildi.

Burada en önemli noktayı grafen oluşturuyor. Bu yeni ekran teknolojisinin esnek yapısı sayesinde, özellikle giyilebilir teknoloji alanında aktif olarak kullanılması bekleniyor.

İlk kez 2004 yılında keşfedilen grafen malzemesi de böylece akıllı cihazların ekranlarında etkin rol oynamış oldu.

TÜRK ŞİRKETLER VERİ İHLALİNİ 225 GÜN SONRA FARKEDİYOR

IBM Güvenlik İş Birimi ve Ponemon Institute, "Veri İhlalinin Maliyeti" adlı yıllık araştırmasını yayınladı. Bu araştırmada bir veri ihlalinin, Türkiye dâhil olmak üzere on üç ülkedeki ve iki bölgedeki şirketlerin kâr-zarar haneleri üzerinde yaptığı etkinin tamamı incelendi. Türkiye'deki bir veri ihlalinin ortalama toplam maliyeti 9,26 milyon TL olduğu ortaya çıktı.

IBM Güvenlik iş biriminin sponsorluğunda Ponemon Institute tarafından yürütülen çalışma 13 ülkede ve 2 bölgede gerçekleştirildi: ASEAN (Güney Doğu Asya Ülkeleri Birliği), Avustralya, Brezilya, Kanada, Fransa, Almanya, Hindistan, İtalya, Japonya, Güney Afrika, Güney Kore, Orta Doğu (Suudi Arabistan Krallığı ve Birleşik Arap Emirlikleri dahil), Türkiye, Birleşik Krallık ve ABD. Bu yılki araştırmada, geçtiğimiz 12 ay içinde bir veri ihlali yaşamış olan 477 şirketten 2 bin 200 BT, veri koruması ve uyumluluk uzmanıyla mülakatlar yapıldı.

Türkiye'nin ilk kez dâhil olduğu bu araştırmada ihlallerin şirketlere, her bir kayıp ya da çalınan kayıt için kişi başına 451 TL'ye mal olduğu ortaya çıkarıldı. Aynı zamanda Türkiye'deki ihlallerin yüzde 38'inin temel olarak kötü amaçlı veya suç niteliğindeki saldırılardan kaynaklandığı, bunu yüzde 33 oranıyla sistem arızalarının ve yüzde 29 oranıyla insan hatasının izlediği ortaya çıktı.

Bu araştırmada aynı zamanda ihlal maliyetini artıran veya azaltan faktörler de incelendi ve maliyetlerin, bir veri ihlalinin kapsama alınması için harcanan sürenin miktarından ve bunun yanı sıra müdahale süresini azaltan teknolojilere yapılan yatırımlardan büyük ölçüde etkilendiği ortaya çıkarıldı. Türkiye'de, araştırmada bir veri ihlalinin belirlenmesi için gereken ortalama süre 225 gündü ve belirlendiğinde bir veri ihlalini kapsama almak için gereken ortalama süre 86 gündü.

Bir ihlali 30 günden daha kısa sürede kapsama alan şirketler, bu sürenin 30 günden fazla olduğu şirketlere kıyasla 1 milyon ABD Doları tasarruf etti.

Araştırmada aynı zamanda bir veri ihlalinin sektörler üzerindeki etkisi de ortaya kondu. Türkiye'de veri ihlalleri için en pahalı sektörler listesinin başında finans, hizmetler ve teknoloji sektörlerinin yer aldığı ve kuruluşlara kişi başına maliyetin sırasıyla 615 TL, 560 TL ve 558 TL olduğu belirlendi.

Kaynak: **http://quq.la/Jm0ew**

SİBER SALDIRGANLAR YAZ TATİLİ YAPMADI

Yaz mevsimi, tatili ve dinlenmeye ayrılan zamanları çağrıştırdığı gibi bazı siber risklerin arttığı bir dönem olarak da dikkat çekiyor. Siber suçlular kullanıcıların parasını, finansal bilgilerini ve kimlik bilgilerini ele geçirmek istiyor. Eğer doğrudan para çalamazlarsa diğer bilgileri ele geçirerek karanlık ağda satışa çıkarıyorlar.

Giderek başarıları artan siber saldırılar nedeniyle siber suçların küresel maliyeti geçtiğimiz yıl 600 milyar doları aştı. Fortinet, kullanıcıların siber güvenliği tehlikeye atmadan yaz tatillerini geçirebilmeleri için çözüm önerileri sunuyor. Yoğun geçen uzun bir yılın ardından tatile gidip gündelik yaşamın telaşına ara vermek isteyen kullanıcıların yaz döneminde siber güvenlik önlemlerini ihmal etmemesi gerekiyor.

Siber suçların her yerde kullanıcıların karşısına çıkabileceğine değinen Fortinet Bölge Teknoloji Direktörü Melih Kırkgöz, "Dijital bir dünyada yaşıyoruz ve siber suçlar da bu dünyanın bir parçası. Dijital ortamda gezinirken temkinli olma dürtümüzü geliştirmemiz gerekiyor. Çocuklarınız ve siz, evinizde veya otel odanızda güvende olabilirsiniz, ancak tam da fiziksel dünyada olduğu gibi siber dünyada da hiçbir zaman yüzde 100 güvende değilsiniz. Her yeni alana açılmayla birlikte risk de artar. Ancak biraz daha dikkatli olup siber sağduyumuzu geliştirirsek, kullandığımız araç ve uygulamalar üzerinde daha dikkatli inceleme yaparsak; işte o zaman içinde yaşadığımız dijital dünya hızla daha güvenli hale gelebilir" dedi.

1. GÜVENLİ Wİ-Fİ KULLANIMI

Kullanıcılar, yaz tatillerinde her yerde "bağlantıda kalmak" istiyor. Bu nedenle bazı durumlarda halka açık veya ortak wi-fi erişim noktaları kullanarak internet bağlantısı kurmayı tercih edebiliyorlar. Bu erişim noktalarının her zaman çok güvenli olmama ihtimalleri de var. Siber saldırganlar verileri çalmak için pek çok yolu deniyor. Halka açık erişim noktasına bağlanabiliyor ve ardından kendilerini o erişim noktasıymış gibi gösterebiliyorlar. Böylece kullanıcılar farkında olmadan bu noktalar üzerinden internete bağlanıyor. Ardından siber saldırganlar online alışveriş sitesi, banka, ev güvenlik sistemi veya kullanıcının o anda göz attığı tüm sitelerdeki verilere müdahale edebiliyorlar.

2. DAHA GÜVENLİ ŞİFRELER BELİRLEMEK

Kullanıcıların yaptıkları en büyük hatalardan biri, tüm online hesaplarında aynı şifreyi kullanmaları. Çok sayıda farklı siteye üye olan kullanıcılar için, dolayısıyla her siteye özel farklı bir şifreyi akılda tutmak imkânsız olabiliyor.

Bu noktada iki seçenek mevcut. İlki, kullanıcının her hesabı için seçtiği kullanıcı adını ve şifresini saklayan bir şifre saklama uygulaması kullanmak. Böylece hatırlanması gereken tek şifre, bu uygulamanın şifresi oluyor ve gerisini uygulama hallediyor. Diğer seçenek ise, bir uygulama katmanı oluşturmak ve daha sonra her grup için daha karmaşık şifreler kullanmak.

Pek çok sosyal medya sitesi artık iki-faktörlü kimlik doğrulama özelliğini de destekliyor. Bu özellik, şifre girildikten sonra mobil cihazlara gönderilen bir kodun girilmesi gibi kimlik doğrulamanın başka bir yönteminin kullanılarak giriş yapanın kimliğini doğrulayan, böylece hesapların ve verilerin güvenliğini büyük ölçüde artıran ekstra bir güvenlik adımı olarak ön plana çıkıyor.

3. E-POSTA YOLUYLA VE WEB'DE KARŞI KARŞIYA KALINABİLECEK OLASI SAHTEKARLIKLARIN FARKINDA OLMAK

Kullanıcıların, öncelikli olarak kontrol etmeden e-postalarına gönderilen veya web sitelerinde yayınlanan ilanlardaki bağlantılara tıklamaması gerekiyor. Ne kadar cezbedici olursa olsun, kullanıcının tanımadığı birinden gelen bir e-postayı asla açmaması gerekiyor. Özellikle de nakit ödülü veya kullanıcının satın almadığı bir ürünün faturası gibi bir konu başlığı varsa bu e-postaların açılmaması gerekiyor. Ayrıca kullanıcıların tanıdığı kişilerden gelen e-postalara da göz atmak için bir dakikalarını ayırması tavsiye ediliyor.

4. VİRÜSLERDEN VE ZARARLI YAZILIMLARDAN KORUNMAK

Kullanıcıların, güvenilir ve iyi yorumlar alan bir zararlı yazılım önleme programı yüklemesi, bu programın sürekli güncel tutması ve düzenli olarak çalıştırılması önem arz ediyor. Hiçbir yazılım yüzde 100 etkili olmadığı için cihazların veya ağların taranmak üzere ikinci veya üçüncü bir güvenlik çözümü yüklenerek çalıştırılması da güçlü bir önlem olarak öne çıkıyor. (Birçok virüs koruma çözümünün ücretsiz online versiyonu mevcut veya kısa bir süre için ücret-

siz demo kullanımına izin veriliyor.) Dizüstü bilgisayar veya masaüstü bilgisayar kullanan daha ileri düzeydeki kullanıcılar ise cihazlarında daha güvenli bağlantılar veya online alışveriş ve işlemler için kullanabilecekleri temiz bir sanal makineye sahip olmayı düşünebilirler.

5. CİHAZLARIN GÜNCEL TUTULMASI

Bilgisayar korsanlarının kullandığı en başarılı saldırı vektörlerinden biri, zaten iyi bilinen ancak korunma önlemi alınmayan güvenlik açıklarını hedeflemektir. Cihazların geliştiricileri ve kullanılan uygulamalar, kullanıcıları bilinen tehditlerden korumak için tasarlanmış düzenli güvenlik güncellemeleri yayınlar. Bu güncellemelerin, kullanıma sunulduğu an vakit kaybetmeden yüklenmesi ve çalıştırılması gerekiyor.

6. SOSYAL MEDYA HESAPLARININ KONTROL ALTINDA TUTULMASI

Bilgisayar korsanları çoğu kez tıklanma ihtimalinin daha yüksek olduğu linkleri kullanıcıların önüne çıkarmak için kullanıcılarla ilgili bilgileri kullanır. Bu kişisel bilgilere sahip olmak için başvuracakları en yaygın ve kolay kaynak ise sosyal medya siteleridir. Bunu önlemenin en kolay yolu, yalnızca önceden seçilmiş kişilerin sosyal medya sayfalarını görmesine izin veren katı gizlilik ayarlarını yapmaktır.

Kullanıcıların seyahat ederken, sosyal sitelerde paylaştığı tatil mesajlarına bir sınır getirmesi de tavsiyeler arasında yer alıyor. Kullanıcıların gittikleri yerleri ve yaptıklarını herkesle paylaşması eğlenceli olsa da bu bilgiler kötü niyetli kişilerin bu durumdan haberdar olmasına sebep olarak tatilde olan kullanıcıların evlerinin soyulması riskini dahi ortaya çıkarabilir.

7. KULLANICILARIN EĞİTİLMESİ

Bireysel olarak kullanıcıların siber farkındalıklarını artırmanın yanı sıra kullanıcıların bu bilgileri çocukları dahil yakın çevreleriyle paylaşmaları da siber güvenliği olumlu yönde etkiliyor. Böylece hem daha çok kişinin bilinçlenmesi sağlanmış oluyor hem de sosyal medya ortamında birbirine bağlı kişiler için güvenlik de artırılmış oluyor.

Kaynak: **http://quq.la/FGGpX**

SİBER GÜVENLİĞE AYRILAN BÜTÇE DOĞRU YÖNETİLMİYOR

Kurumların, siber güvenliğe yeterli bütçe ayırmadığı bir gerçek ve bu nedenle verilen bütçenin en etkili şekilde yönetilmesi gerekiyor. Kurumlardaki çoğu BT Uzmanı ise kendilerine verilen bütçeyi doğru yönetemiyor. Anderson Araştırma Şirketi'nin konu hakkındaki araştırmasına göre şirketler, sadece saldırıları önlemeye yatırım yapmakla yetinerek saldırı sırasında veya sonrasında ihtiyaç duyacakları araçlara bütçeden pay ayırmıyor. Bu nedenle hem siber saldırılar çok geç fark ediliyor hem de saldırı sonrası eski iş düzenine dönmek oldukça uzun zaman alıyor. Ağ güvenliği çözümlerinde lider olan WatchGuard,

Bu bağlamda, doğru siber güvenlik bütçesi yönetimi, 3 başlıkta ele alınabilir.

Bilgi güvenliği uzmanları, sahip oldukları bütçeyi, kurumları için ne kadar iyi kullanırsa, daha sonrası için bütçe artırma talepleri de bir o kadar olumlu karşılanıyor. Ancak günümüzde kurumlardaki çoğu bilgi güvenliği çalışanı bu bütçeyi doğru kullanamıyor. Bütçenin büyük bir kısmı siber saldırıları önlemeye ayrıldığı için sorunu fark edip savunmayla karşılık vermeye ve iş sürekliliğini sağlamaya daha az bütçe ayrılıyor. Bu durumda saldırının oluşturduğu zarar hem çok şiddetli yaşanıyor hem de oldukça uzun sürüyor.

Siber güvenlik bütçesinin kendi içindeki ideal paylaşımı ise aşağıdaki gibi olmalıdır:

• %50, saldırıları önlemek

• %30, sorunu fark ederek savunmaya geçmek

• %20, saldırı sonrası sistemi düzeltmek

Siber Güvenlik Bütçesi Üç Başlıkta Değerlendirilmeli

Siber güvenlik alanında hizmet veren önemli şirketlerden biri olan WatchGuard, siber güvenliğe ayrılan bütçenin en etkin şekilde kullanılabilmesi için dikkat edilmesi gereken üç başlığı paylaşarak hiçbirinin atlanmaması konusunda kurumları uyarıyor.

1. SALDIRILARI ÖNLEME

Sisteminizi güvenli kılacak ürün ve servislere ayrılacak bütçe, güvenliğe yatırımın ilk adımını oluşturuyor. Güvenlik duvarları, antivirüs programları, yetkisiz erişimleri engelleme sistemleri, gelişmiş kötü niyetli yazılımlara karşı koruma çözümleri, bulut sistemindeki e-postalar için filtreleme sistemleri gibi araçlara ayrılan bütçe pek çok saldırıyı uzak tutuyor. WatchGuard, güvenlik bütçenizin yarısının saldırıları önlemek için kullanılabileceğini belirtiyor.

2. SORUNU FARK ETME VE SAVUNMAYLA KARŞILIK VERME

Bir siber saldırı gerçekleştiğinde fark etmenizi ve savunmaya geçmenizi sağlayacak araçlara da yatırım yapılması oldukça önemli. Bu alandaki ürünlere ayrılan bütçe, bilgi teknolojileri uzmanlarının problem hakkında bilgi sahibi olmasına ve sistemi iyileştirmesine yardımcı oluyor. Uç nokta güvenliğini sağlayan araçlar, cihazdaki hareketleri inceleyen sistemler ve vaka çözücü ürünler bu kapsama giriyor. Ponemon Araştırma Şirketi ve IBM'in beraber hazırladığı rapora göre, bir siber saldırıyı fark etmek ortalama 190 gün sürüyor ve 190 gün içinde siber saldırganlar şirketlere tahmin edilemeyecek derecede zararlar veriyor. Bu nedenle bu tür takip edici ve çözüm üretici araçlara şimdikinden daha fazla bütçe ayrılması gerekiyor. WatchGuard, eldeki miktarın %30'unun bu kısma ayrılmasını öneriyor.

3. SALDIRI SONRASI DÜZELME

İş sürekliliği sağlayan teknolojilere yatırım yapmak zaman ve para kaybı yaşamamak için gereklidir. Her ne kadar çoğu şirket en azından verilerini yedekliyor olsa da çok azının felaket sonrası nasıl toparlanacaklarına dair bir planı bulunuyor. Yedekleme servisleri dışında sanal ya da bulut teknolojisine dayalı hosting sistemleri, siber sigortalar gibi çözümler bu kısmı oluşturuyor. WatchGuard, saldırı yaşansa bile iş sürekliliği sağlayacak ve iş yerindeki genel durumu toparlayacak bu tür araç ve servislere güvenlik bütçenizin en az %20'sinin ayrılması gerektiğini öneriyor.

Kaynak: **http://quq.la/hl2kl**

TÜRKLERİN YARISI BLOCKCHAİN'İ PARA BİRİMİ SANIYOR

Kripto para birimlerinin temelinde yatan blockchain teknolojisi günümüzde neredeyse Bitcoin'le özdeşleşmiş olsa da IBM, Sony, Maersk Line gibi çok uluslu şirketlerin de test ettiği bir teknoloji.

Dağıtılmış veri tabanı olarak tanımlayabileceğimiz bu teknoloji, verilerin güvenli ve daha uygun maliyetle saklanmasını ve transfer edilmesini sağlıyor. Tabi kripto paralar dışında çeşitli kullanım alanlarına sahip olan blockchain'in genellikle kripto paralarla anılması bu kavram üzerinde kafa karışıklığına neden olabiliyor.

Araştırma çözümleri sunan Twentify tarafından yürütülen bir çalışma toplumumuzda da blockchain konusunda büyük yanılgılar olduğunu ortaya koyuyor. Twentify'ın Bounty mobil araştırma paneli üzerinden gerçekleştirilen çalışmada Türk halkının kripto para birimlerine karşı tutum ve kullanımının araştırılırken 28 Ağustos ile 4 Eylül tarihleri arasında 965 kişiye kripto paralar ve blockchain hakkında çeşitli sorular soruldu. Çalışmayla ilgili ilgi çeken rakamlar ise şunlar:

Z JENERASYONU, BLOCKCHAİN TEKNOLOJİSİNE HAKİM

Çalışmaya katılanların %37'si blockchain teknolojisini bildiğini söylerken, %58.3'ü blockchain'i bir kripto para birimi sanıyor. Araştırmaya katılanların büyük bir kısmı Bitcoin ile blockchain teknolojisini bir tutarken Z jenarasyonu (1996 ile 2011 yılları arasında doğanlar) blockchain teknolojisine en hakim jenarasyon olarak dikkat çekiyor.

Katılımcıların %53.2'si Bitcoin hakkında bilgi sahibi olduğunu belirtmiş durumda. Çalışmaya katılanların %19.8'i daha önce Bitcoin alıp sattığını söylerken, bunların %73'ü halen elinde Bitcoin tuttuğunu belirtiyor. Ayrıca Bitcoin alanların %44.4'ü yatırım amaçlı aldığını dile getiriyor. Bitcoin satın alırken en çok Btc Turk ve Paribu'yu tercih ettiklerini belirten kullanıcıların %31.7'si Bitcoin satın aldıktan sonra ellerindeki Bitcoin'i en az 3 ay tutuyor.

PARASI OLAN BİTCOİN DEĞİL ALTIN ALMAYI TERCİH EDİYOR

Bitcoin'lerini satmayıp tutmaya devam eden kişilerin %58.6'sı, Bitcoin'in ileride değer kazanacağını düşündüğü için Bitcoin'lerini satmadıklarını belirtiyor. Bugüne kadar Bitcoin satın almayanların ise %35.3'ü önümüzdeki 5 yıl içinde Bitcoin satın almayı düşünüyor. Çalışmadaki ilginç bir detaya göre eğitim seviyesi arttıkça insanlar Bitcoin satın almaya daha olumlu yaklaşıyor.

Tıpkı internet dünyasında olduğu gibi toplumumuzda da Bitcoin'in geleceği konusunda iki farklı düşüncenin yer edindiğini söylemek mümkün. Çalışmaya katılanların %45.8'i Bitcoin'in önümüzdeki 5 yıl içerisinde daha da değer kazanacağını düşünüyor. Yani Bitcoin'in balon olduğu ve patlayacağı yönündeki düşüncenin toplumun büyük bir kısmı tarafından benimsenmiyor.

Bununla birlikte bir yatırım aracı olarak Bitcoin, geleneksel yatırım araçlarının gerisinde kalıyor. "Elinizde 1000 TL olsa neye yatırım yapardınız?" sorusuna katılımcıların büyük bir kısmı ilk olarak altın cevabını verirken Bitcoin ancak son sıralarda kendisine yer bulabiliyor.

Kaynak: **http://quq.la/fMmMr**

STARBUCKS KRİPTO PARA PİYASASINA GİRİYOR

Starbucks, kripto para piyasasına girmek için yeni bir platform kuruyor. Bu platformda ICE ve Microsoft da yer alacak. Bu platformla birlikte, Starbucks mağazalarında kripto para ile alışveriş yapılabilecek.

Kahve şirketi olmanın ötesine geçen Starbucks, teknoloji odaklı yatırımlarına devam ediyor. Geçtiğimiz günlerde sanal mağaza ile kahve alışverişi ve teslimatı için Alibaba ile ortaklık kuran şirket, bu kez kripto para girişimiyle gündeme geldi.

Starbucks, Microsoft, ICE iş birliği ile oluşturulan, Bakkt isimli yeni kripto para girişimi duyuruldu. Bu yıl Kasım ayında kullanıma sunulacak olan platform ile kullanıcılar kripto para kazanabilecek, saklayabilecek ve harcayabilecek.

Bu platform ile kullanıcılar Starbucks alışverişlerinde kripto para kullanabilecek. Günlük alışverişe odaklanılan Bakkt girişimiyle kripto para kartı çıkarılması da bekleniyor. Ancak kripto para kabul eden işletme sayısının az olması, böyle bir kartın ne kadar kullanışlı olacağı sorusunu beraberinde getiriyor.

Platform, özellikle bireysel kullanıcılara önemli yenilikler getirecek.

Kaynak: **http://quq.la/AWT4Q**

ROBOTLARI KANDIRMANIN CEZASI VAR MI?

Akıllı teknolojiler hayatımızı her anlamda kolaylaştırmaya ve pratikleştirmeye devam ediyor. Sesli asistanlardan, giyilebilir teknolojilere, sürücüsüz araçlara ve internette karşılaştığımız botlara kadar onlarla artık sürekli etkileşim halindeyiz. Vazgeçilmez hale gelen bu teknolojiler teknik anlamda farklı yöntemler kullanılarak oluşturuluyor. Bunlardan biri de makine öğrenmesi ya da diğer bir deyişle yapay öğrenme(YÖ).

YÖ kısaca veriler üzerinden tahminlerde bulunup, karmaşık örüntüleri algılama ve akılcı karar verebilme üzerine odaklı bir bilim dalıdır. YÖ'nün geçmişine baktığımızda, modern yapay öğreniminin matematiksel temellerinin birçoğunun, bilgisayarlardan önce geldiğini görüyoruz. Bu konudaki büyük atılımlar, 18. yüzyılda Pierre-Simon Laplace'ın Bayes Teoremi'ni tanımlamasını sağlayan Thomas Bayes'in çalışmalarını içeriyor (1812).

Bu dönemlerde yapılan çalışmalar, günümüzdeki yapay öğrenmenin ataları sayılıyor. 1940'lı yıllara gelindiğinde ise başta Manchester, Cambridge ve Pennsylvania Üniversitelerdeki çalışmalar dikkat çekmeye başlıyor. 1950 yılında Alan Turing'in bir makinenin düşünüp düşünmeyeceğine yönelik olan "Computing Machinery and Intelligence" makalesi büyük yankı uyandırıyor.

Bunu takip eden önemli gelişime 1951 yılında Marvin Minsky ve Dean Edmonds'in, organik beyinlerin çalışma şeklinin bilgisayar tabanlı bir simülasyonu olarak ilk yapay sinir ağını tasarlaması oluyor. Oluşan büyük beklentinin hayal kırıklığına sebep olması ve yaşanan yavaşlama dönemi sonrasında, yakın geçmişimizden başlayarak bu çalışmalar tekrar büyük bir hız kazanmış durumda.

YÖ'de temelde üç yaklaşım bulunmaktadır: gözetimli, gözetimsiz ve pekiştirmeli öğrenme.

Gözetimli öğrenmede, girdi değişkenlerini (X), çıktı değişkenlerine (Y) eşleme işlevini öğrenmek için etiketli eğitim verileri kullanılıyor. Daha anlaşılır bir dil ile diyelim ki siz bir emlakçısınız. İşleriniz büyüyor ve size yardım etmesi için birçok stajyer işe aldınız. Ama bir problem var—siz bir eve baktığınızda evin değeri hakkında iyi bir tahminde bulunabiliyorsunuz ama stajyerlerinizin tecrübesi olmadığından nasıl değer biçmeleri gerektiğini bilmiyorlar.

Stajyerlere yardım etmek amacıyla (ve kendinizi tatil için boşa çıkarmak maksadıyla), sizin bölgenizdeki ev fiyatlarını genişlik, muhit ve benzer evlerin kaça satıldığı vb. gibi özelliklere göre hesaplayan basit bir uygulama yazmaya karar verdiniz. Bu yüzden son üç ayda şehirde satılan tüm evlerin fiyatlarını kaydettiniz. Satılan her evin oda sayısı, genişliği, muhiti vb. gibi detaylı özelliklerini not aldınız. Ama en önemlisi nihai satış fiyatını da kaydettiniz. Bu eğitim verisini kullanarak, bizim bölgemizdeki diğer tüm evlerin satış fiyatlarını tahmin eden bir program yazmak istiyoruz. İşte bu yöntem gözetimli öğrenmedir. Her bir evin kaça satıldığını biliyorsunuz, yani problemin cevabını biliyorsunuz ve oradan yola çıkarak geriye doğru bir mantık oluşturmaya çalışıyorsunuz.

Gözetimsiz öğrenmede ise sistem yalnızca girdi değişkenlerine (X) sahip, buna karşılık çıktı değişkenleri bulunmuyor. Verilerin altında yatan yapıyı modellemek için etiketsiz eğitim verileri kullanılıyor. Yine baştaki emlakçı örneğine geri dönelim.

Her evin satış fiyatını bilmeseydiniz ne olurdu? Tüm bildiğiniz evin genişliği, yeri vb. gibi bilgiler olsa bile, görünen o ki hala işe yarar hesaplamalar yapabilirsiniz. Buna da gözetimsiz öğrenme deniyor. Bu yöntem şuna benziyor: Birisi size bir kâğıtta sayı listesi veriyor ve şunu diyor: "Bu sayıların ne ifade ettiğini bilmiyorum ama belki sen burada bir düzen veya grup gibi bir şey bulabilirsin—iyi şanslar!". Pekiştirmeli öğrenmede ise yazılımlar, genellikle deneme yanılma yoluyla en iyi eylemleri öğrenirler. Bu yöntem genel olarak robotikte kullanılır. Burada bir robot, engele çarptıktan sonra negatif geri bildirim alarak çarpışmalardan kaçmayı öğrenebilir. Ayrıca video oyunlarında da yine deneme yanılma yöntemiyle bir oyuncunun ödülleri alabileceği belirli hareketleri saptayabilir ve bir sonraki hareketini buna göre komutlar.

Günümüzde oldukça ilerleyen bu teknikler pek çok alanda da kullanılmaya başlandı. Nesne ve ses tanıma, görüntü işleme, arttırılmış gerçeklik bu konuda ilerleme kat edilen önemli konulardan bazılarını oluşturuyor. Bunlar hayatımızı kolaylaştırmakla birlikte bazı hukuksal sorunları da beraberinde getiriyor. 2018 WeRobot konferansında Washington Üniversitesi'nden Ryan Calo ve ekibinin sunduğu "Is tricking a robot hacking?" yani "Bir robotu kandırmak hacklemek midir?" adlı makalesinde harika bir hususa değiniyor.

Calo'ya göre, hasmane YÖ (adversarial ML) hukuksal açıdan da incelenmesi gereken bir konu. Hasmane YÖ, yapay öğrenme ile bilgisayar güvenliğinin ortak çalışma alanını oluşturuyor. Burada öğrenme algoritmalarının güvenlik açıklarından faydalanılarak, giriş verileri sistem güvenliğini tehlikeye atmak için manipule ediliyor. Hasmane YÖ'ye karşı savunma yapmak da oldukça güç; çünkü hasmane örnek hazırlayıp sürecin kuramsal modelini oluşturmak zor-

ludur. Araştırmalar, YÖ algoritmalarının kırılabileceğini ortaya koymakta ve YÖ'deki bu başarısızlık, basit algoritmaların bile tasarımcılarının düşündüğünden oldukça farklı davranabileceğini göstermektedir.

Örneğin, hasmane YÖ kullanılarak, televizyondaki bir reklamda gömülü olan ve hiç kimsenin anlamlı bir şekilde farkına varamayacağı olumsuz bir ses girdisi yoluyla sesi işiten kişisel asistan sosyal medyada konum verisi paylaşabilir. Ya da sürücüsüz bir araç, dur işaretini bir hız limiti olarak algılayıp durmak yerine hızlanarak trafik kazasına yol açabilir.[1]

Görüldüğü gibi, aslında sisteme doğrudan bir müdahale yapılmayıp, sistem "kandırılarak" belli bazı sorunlara sebebiyet veriliyor. Calo'nun da dediği gibi asıl soru şu: "Bir robotu kandırmak hacklemek midir?" Ve bunun hukuktaki yansımaları nasıl olur?

Türk Ceza Kanunu (TCK) bilişim suçlarını birden fazla maddede düzenlemiştir. Bilişim Alanında Suçlar başlıklı bölümünde, madde 243'te hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçunu düzenlemektedir. Buna göre, "Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir." Veriler ele geçirilsin veya geçirilmesin bilişim sistemine hukuka aykırı olarak girilmesi ve orada kalınması bu suçun eylemini oluşturmaktadır. Burada failin eylemi neticesinden bir zarar veya tehlike oluşması aranmamakta, sisteme girilmesi ve orada kalınması yeterli görülmektedir.

Bilişim sistemlerinin işleyişinin engellenmesi veye bozulması suçu ile verilerin yok edilmesi veya değiştirilmesi suçunu düzenleyen madde 244/1-2'ye göre ise, "Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır."

Bu düzenleme ile bilişim sisteminin her nasıl olursa olsun çalışmasının engellenmesi, sistemin bozulması ve verilere zarar verilmesi ya da erişilmez hale getirilmesi cezalandırılmaktadır. Maddenin gerekçesinde de, bu maddeyle bilişim sistemlerine yöneltilen ızrar (mala zarar verme) eylemlerinin ayrı bir suç haline getirildiği belirtilmektedir. Ayrıca yine maddenin gerekçesinde, yapılan düzenleme ile "aracın fizik varlığı ve işlenmesini sağlayan bütün diğer unsurları, söz konusu suçun konusu oluşturmaktadır" denilerek bilişim sisteminin somut ve soyut bütün unsurlarının bu suçun konusunu oluşturacağı ifade edilmektedir.[2]

TCK devamında madde 245'te banka ve kredi kartlarının kötüye kullanılması suçlarını düzenlemiştir. Kısacası bu madde ile söz konusu kartların haksız, hukuka aykırı olarak kullanılması yoluyla bankaların ve kart sahiplerinin zarara sokulması ve bu suretle hukuka aykırı yarar sağlanması istenmektedir.[3]

Bilişim alanında suçlar başlıklı bölüm dışında, TCK, Malvarlığına Karşı Suçlar başlıklı bölümünde madde 142'de hırsızlık suçunun nitelikli hali olarak fıkra 2, e bendinde "bilişim sistemlerinin kullanılması suretiyle" ifadesine yer verilmiştir. Bunun dışında, madde 135 vd. kişisel verilerin korunmasına ilişkin suçlarından; madde 124 haberleşmenin engellenmesi suçundan; madde 132 haberleşmenin gizliliğini ihlal suçundan bahsetmekte ve Kanun bilişim sistemleri aracılığıyla işlenebilecek diğer suç tiplerine de ilgili maddelerde yer vermektedir.

Sonuç olarak, TCK'nın bilişim suçları ile ilgili düzenlemelerine baktığımızda, genel itibariyle bilişim sistemlerine girip belli birtakım değişiklikler, tahribatlar, kopyalamalar vs. yapılması üzerine kurgulanmıştır. Ancak, gelişen teknoloji ile birlikte kötü niyetli kişiler yukarıda da anlatıldığı üzerine doğrudan sisteme bir müdahale etmeden de zararların oluşmasına sebep olabiliyor.

Sürücüsüz aracın hasmane YÖ ile durma işaretini hızlan olarak algılayıp bir insanın ölümüne sebep olduğunu ve kötü niyetli kişilerin bu kasten yaptığını düşünelim. TCK, bilişim alanında suçlar başlığı altında bilişim sistemlerine yapılan müdahalelere yönelik düzenlemelere yer verdiğinden, burada farklı bir yol izlenmesi gerecek. Çünkü örnekte olduğu gibi, bu teknolojinin getirdiği kolaylıktan faydalanılarak suçun işleyişi kolaylaşmaktadır.

Kasten öldürme, kasten yaralama, özel hayatın gizliliğini ihlal, trafik güvenliğini tehlikeye sokma gibi suçları da oluşturacak şekilde hasmane YÖ gibi teknolojiler kullanılabilmektedir. Dolayısıyla bunlar gözetilerek, nitelikli hal olarak bu teknolojileri kullanmanın getirdiği kolaylıkla suçun işlenmesi durumu TCK'ya eklenmelidir.

Prof. Dr. Cem Say, Richard Kelley ve Av. Gökhan Ahi'ye değerli görüşleri için teşekkürler…

Kaynak: **http://quq.la/UaSxb**

[1] Is Tricking a Robot Hacking?; Ryan Calo; sf. 13

[2] Bilişim Suçları ve İnternet İletişim Hukuku; M. Volkan Dülger; sf. 406

[3] Dülger; sf. 447

AYIN KİTABI: "50 SORUDA YAPAY ZEKÂ"

Boğaziçi Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyesi Prof. Cem Say'ın "50 Soruda Yapay Zekâ" adlı kitabı bu ay okurları ile buluştu. Pek çok farklı alandan insanın ilgi ile karşıladığı kitap, oldukça zengin bir içeriğe sahip.

Leibniz'in rüyasını gerçekleştirmek için cebir ve mantığı evlendiren Boole'den, kariyerini mantıkla matematiğin birleştirilmesi ülküsüne adayan Frege'ye kadar yapay zekaya uzanan serüvenin tarihsel akışını okurlara sunuyor.

Hoca'ya göre, sıradan bir insan, bilgisayarların her şeyi yapabilecekleri fikrine kapılmakta haklı sayılabilir. Çünkü bilgisayarlar, okul notlarımızdan, iş yerindeki maaşlarımıza, sigorta yaptırmaya niyetlenirsek kalan ömrümüze kadar her şeyimizi biliyorlar.

Kitapta ilginç bulduğum sorulardan biri "Beyin nasıl bir bilgisayardır?" sorusu. Hoca, sorunun içinde beyni bir bilgisayar olarak kabul ettiğini de ortaya koyarak kısaca şöyle açıklıyor: Beyin denilen organ bir ağ bellek işlevi görmekte ve duyu organlarınca uyarılan hücreler bu ağa girdi, kaslar gibi hareket vs. yollarla dış dünyada etki yaratabilecek olanlara sinyal taşıyanlar da çıktı olarak görülebilir. Yani beyin bir bilgi işlem makinesidir.

Kitapta bilgisayarların çeşitli kullanımlarına dair sorular sorarken, arada kendi anılarından da bahsederek okuyucuyu bağlayan bir dil kullanıyor. Hikâyeleştirilmiş anlatımı ile teknik sayılan bilgileri her kesimden okuyucunun anlayabileceği bir seviyeye indirmeyi başarıyor.

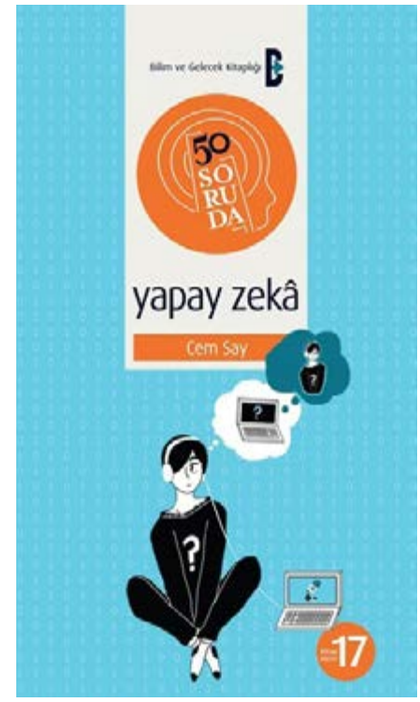
Keyifli bulduğum kısımlardan biri de herkesin tanımlamasını yaparken zorlandığı "yapay zekâ"nın hoca tarafından yıllarca önce yapılan tanımlamasına dair anlatım. Kendisi 20. yüzyılda yaptığı tanımlamayı eksik buluyor; çünkü o dönemlerde yapay zekâyı, birçok kombinasyondan doğru olanını bulmayı gerektiren bulmacaları hızlı çözebilmeyi bilgisayarlara yaptırmaktan ibaret olarak gördüklerini söylüyor. Dolayısıyla hocaya göre bu, yapay zekâ tanımlamasının sakat doğmasına sebep olmuştu. Yaptığı yeni tanımlama da mevcut. Meraklıları kitapta bunu bulabilir.

Bir hukukçu olarak, sabırsızlanıp ilk olarak okuduğum kısım ise "Bilgisayarlar avukatlık yapabilir mi?" sorusu idi. Kendisi bu sistemlerin dokümantasyon, içtihat arama ve karar tahmin etme gibi konularda avukatlardan daha başarılı olduğunu söylüyor ve bana göre bu konuda oldukça haklı. Avukatların saatlerini alan angarya pek çok iş bu sayede kolaylaşabilir.

Son soru ise bize sınırlarımızı hatırlatan cinsten: "İnsan zekâsının bir geleceği var mı?" Oldukça olumlu bir tablo çizerek bu "ek beyinlerin" geleceğimiz için faydalı olacağını söylerken, baskıcı yönetimlerce kötüye kullanımının ise insanlığı köreltebileceğinin vurgusunu yapıyor.

Kitapta yukarıdakilere ek olarak pek çok güncel ve sosyal alanlarla bağlantılı sorular da mevcut. "Robotlar aşık olabilir mi?" "Bilgisayarlar buluş yapabilir mi?" ya da "Robotlar askere alınsın mı?" gibi…

Okuması keyifli ve akıcı… Daha fazla ayrıntı vermek istemem ama kitabın son cümlesi çok umut verici: "Başarabiliriz."



Kaynak: **http://quq.la/WSkhD**