MARMARA
BELEDİYELER BİRLİĞİ

Bilgi Teknolojileri
Platform Bülteni

Nisan 2018 | Sayı 2

Editörden...

Bilgi Teknolojileri Platformu'nun çıkardığı bültenin 2. sayısı ile karşınızdayız. Olabildiğince güncel kalmaya çalıştığımız sayılarımızda gündemi çokça meşgul eden ve uzun bir süre gündemdeki yerini koruyacak olan "kişisel veriler ve sosyal medya" konusuna geniş bir yer ayırdık. Bunların yanı sıra yeni teknolojileri de takipte kalarak bu sayımızı derledik.

3 aylık periyotlarla çıkarmaya başladığımız bültenimizin bu 2. sayısında ilk konumuz belediyeleri yakından ilgilendiren "Belbis" oldu. Akıllı güvenlik sistemlerinin barındırdığı risklere de ayrı bir parantez açtık. Bir önceki sayımızda "Bitcoin'e" giriş yapmıştık devamı niteliğinde bir yazıya yer verdik. Birkaç satır önce değindiğim kişisel verilerin sosyal medya aracılığıyla nasıl manipüle edildiği, bizi bekleyen tehlikeyi ve ortaya çıkan tepkilerin kaleme alındığı ve mutlaka okumanızı tavsiye ettiğimiz iki yazıya da sayfalarımızda yer açtık. Bültenimizin son sayfaları ise teknolojinin görünmeyen kahramanları ile dolu.

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

İyi okumalar dileriz,

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

Bilal Eren

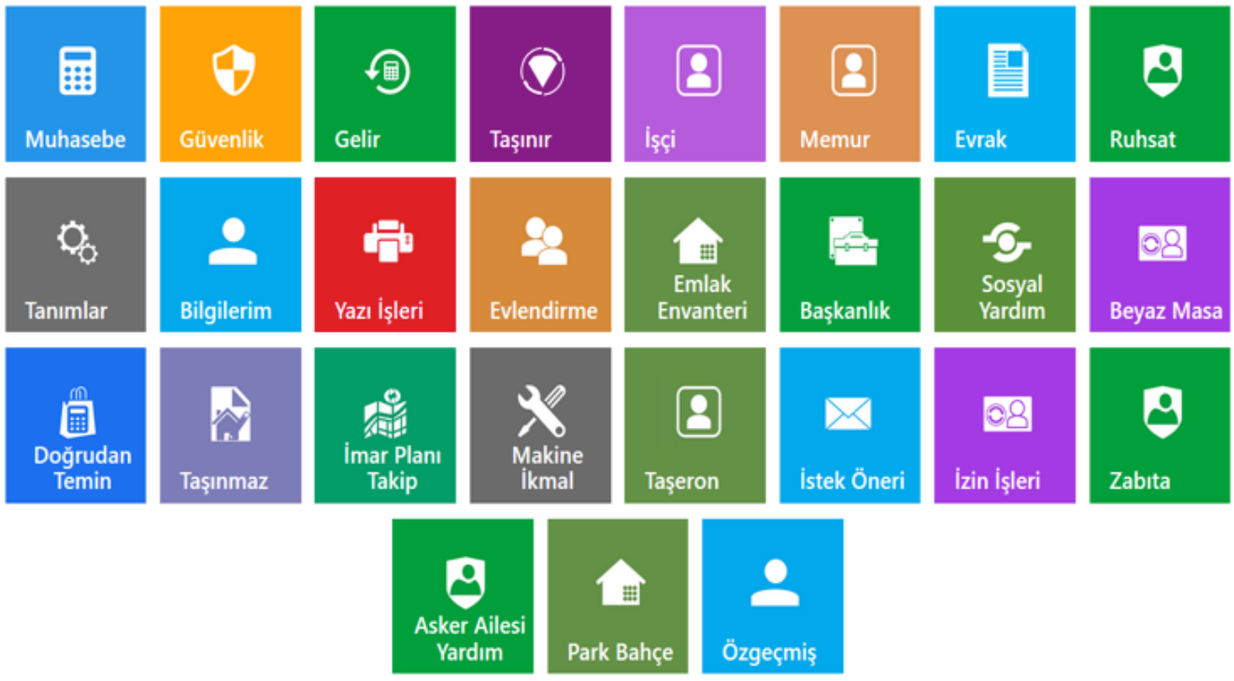
İsmail Hakkı Polat

Bilgin Metin

Nisan 2018, **Sayı 2**

BELBİS

"Türkiye Belediyeler Birliği Belediye Yönetim Bilgi Sistemi Projesi" (BELBİS) bir otomasyon sistemidir.



Belediyelerimizin talepleri doğrultusunda; belde sınırları içerisinde yaşayan vatandaşlara götürülecek hizmet kalitesini yükseltmek amacıyla başta idari ve mali işlemler ile taşınmaz ve mükellef bilgilerinin takip edilebileceği "e-belediye" uygulaması olarak 2011 yılında başlatılan "Türkiye Belediyeler Birliği Belediye Yönetim Bilgi Sistemi Projesi" (BELBİS) bugün itibariyle birçok modülünden oluşan bir otomasyon sistemidir.

BELBİS Projesi, Türkiye Belediyeler Birliği (TBB) tarafından 5355 Sayılı Mahalli İdare Birlikleri Kanunu'nun 20'nci maddesi ve Birlik Tüzüğünün 7'nci maddesinde yer alan "Belediyelerde bilişim teknolojilerinin kullanımı ve yaygınlaştırılması ile e-belediyeciliğin gelişmesine destek olmak." görevleri çerçevesinde yürütülmektedir.

AMACI

Belediyelerimize ücretsiz olarak sunulan BELBİS projesinde temel amaç;

- Tüm kullanıcılara her belediyede kullanabilecekleri standart bir uygulama sunmak,
- Belediye yöneticileri ihtiyaç duyduğu sabit ve değişken raporların hazırlanması ile sistemde bulunan bilgilerin etkili bir şekilde değerlendirilmesini sağlamak,
- Personele Uygulamaya ilişkin kullanım eğitimler ile birlikte konuya ilişkin hukuksal eğitimlerin verilmesi,
- Vatandaşa yönelik hizmetlerin web sayfası, e-devlet gibi elektronik ortamlara sağlanan servislerle hızlı sunulmasına yardımcı olmaktır.

Belediyelerimizin talepleri doğrultusunda; belde sınırları içerisinde yaşayan vatandaşlara götürülecek hizmet kalitesini yükseltmek amacıyla başta idari ve mali işlemler ile taşınmaz ve mükellef bilgilerinin takip edilebileceği "e-belediye" uygulaması olarak 2011 yılında başlatılan "Türkiye Belediyeler Birliği Belediye Yönetim Bilgi Sistemi Projesi" (BELBİS) bugün itibariyle birçok modülünden oluşan bir otomasyon sistemidir.

BELBİS Projesi, Türkiye Belediyeler Birliği (TBB) tarafından 5355 Sayılı Mahalli İdare Birlikleri Kanunu'nun 20'nci maddesi ve Birlik Tüzüğünün 7'nci maddesinde yer alan "Belediyelerde bilişim teknolojilerinin kullanımı ve yaygınlaştırılması ile e-belediyeciliğin gelişmesine destek olmak." görevleri çerçevesinde yürütülmektedir.

AMACI

Belediyelerimize ücretsiz olarak sunulan BELBİS projesinde temel amaç;

• Tüm kullanıcılara her belediyede kullanabilecekleri standart bir uygulama sunmak,

• Belediye yöneticileri ihtiyaç duyduğu sabit ve değişken raporların hazırlanması ile sistemde bulunan bilgilerin etkili bir şekilde değerlendirilmesini sağlamak,

• Personele Uygulamaya ilişkin kullanım eğitimler ile birlikte konuya ilişkin hukuksal eğitimlerin verilmesi,

• Vatandaşa yönelik hizmetlerin web sayfası, e-devlet gibi elektronik ortamlara sağlanan servislerle hızlı sunulmasına yardımcı olmaktır.

BELBİS'İN TEMEL ÖZELLİKLERİ

Farklı organizasyon yapıları ve uygulamaları olsa da BELBİS' de uygulama geliştirme sürecinde belediyelerde yürütülen iş ve işlemler esas alınmaktadır. Bu sayede belediyelerin birimlerinde kullanılabilen standart modüller tasarlanabilmektedir. Tüm belediyeler için ortak bir veri tabanı kullanmaktadır. Ancak kullanıcılara rollerine uygun yetkiler verilmesi nedeniyle tanımlanan görevler dışında hiçbir alana erişememektedir.

Belediye gelirlerinin izlenebilmesi amacıyla sistemde mükellef ve taşınmazlara ait işlemler "Tek Sicil" esasına göre yerine getirilmekte ve "emlak e nvanteri" gelir modülünün ana unsurunu oluşturmaktadır.

SAĞLADIĞI FAYDALAR

BELBİS, belediyelerin güvenli ve hızlı işlem yapabileceği, modüler yapıda ve web tabanlı yapısı sayesinde belediyelere aşağıdaki faydaları sağlamaktadır.

• "bulut mimari" altyapısıyla belediyelerin donanım ve yazılım maliyetler ortadan kalkmıştır. Bu yatırımlar TBB tarafından yapılmaktadır.

• TBB tarafından Merkezi Kurumlar ile yapılan protokoller ile entegrasyon sağlanmaktadır. Verinin toplanmasında ve doğruluğu konusunda belediyeye büyük yararlar sağlamaktadır. HİTAP ile oluşan entegrasyon ile memur personelin bilgi takibi için sisteme veril girilmemektedir.

• e-devlet altında belediyenin durumuna bağlı olarak 8 adet hizmeti sunma imkanı sağlanmıştır. Vatandaşın belediye gelmeden hizmet almasını ve personelin iş yükünün azalmasını sağlamaktadır.

• Tüm vergilerin taşınmaz tabanlı (emlak envanter) takip edilmesi nedeniyle vergi tahakkuk ve tahsilatlarında kaçak ve kayıplarını önlemektedir.

• Uygulama içerisinde mümkün olduğu kadar süreç tanımlanmaya çalışılmış ve modüller arası entegrasyon oluşturularak maddi ve hukuksal kullanıcı hataları en aza indirgenmeye çalışılmıştır. Doğrudan temin modülünde başlayan bir satın alma süreci taşınır modülü ve muhasebe modülüne kayıtları için ek bilgi girilmesine ihtiyaç olmadan tamamlanmaktadır.

• BELBİS kullanan belediyelere tek bir uygulama açılması nedeniyle amaçlanan standardizasyon sağlanmıştır.

TAMAMLANAN MODÜLLER

Toplam 28 modül tamamlanmıştır. Her bir modül altında ilişkili fonksiyonların birleştirilmesi nedeniyle tahakkuk, tahsilat, ÇTV, İlan Reklam Vergisi gibi modüller tek uygulama olarak sayılmıştır. Bu kapsamda BELBİS de bulunan modüller özel firmaların belediyelerimize sundukları modüllerin 42 sine karşılık gelmektedir.

A-SOSYAL MODÜLLLER

BEYAZ MASA

Vatandaşlardan telefon, SMS, internet, e-posta, faks ve yüz yüze görüşmelerden alınan görüş, düşünce, şikâyet ve tavsiyeleri kayıt altına alıp, belediye organizasyonu içinde gerekli bilgiyle, faaliyetle istenilen hizmeti sonuçlandırmak için hazırlanmıştır.

Sosyal Yardım

Vatandaşlara sunulan sosyal yardım hizmetini ulaştırılabilmesi ve bu hizmetlerin hakkaniyet ile yürütebilmesi amacını sağlayan kayıt ve takip modüldür.

İstek Öneri

Projeyi kullanan belediye personeli modüller hakkında istek ve önerilerde bulunmakta, geri dönüşler hem sistem üzerinden hem de SMS yoluyla yapılmaktadır.

Evlendirme

Evlenme başvurusunda bulunan bireylerin kayıtlarının oluşturulması, randevu işlemlerinin alınması ve Evlendirme Yönetmeliğinin eki olan formların hazırlanması için kullanılanmaktadır.

Başkanlık

Belediye Başkanları personel bilgileri ve raporları ile mali raporları izleyebilmektedir.

İzin İşleri

Belediyedeki tüm personellerin izin işlemlerinin talep ve onaylarının yapıldığı modüldür.

Bilgilerim

Personel kendi kişisel bilgilerine ulaşabilmektedir.

Güvenlik

Yönetici yetkisi olan kullanıcının yetki ve kullanıcı tanımlayabildiği bölümdür.

B-GELİR MODÜLLLERİ

Gelir

Su, ilan, ÇTV, eğlence, işgaliye, tahakkuk ve tahsilâtlar, gayrimenkul, emlak, işyeri kayıt ve mükellef işlemleri ile ilgili belediye gelirlerinin takibi yapılmaktadır.

Emlak Envanter

Belediye sınırları içerisinde bulunan bütün parsel kayıtlarının Tapu Kadastro Genel Müdürlüğünden, cadde sokak ve numara verilerinin NVİ'den alınarak sisteme girilmesinden sonra, bu parseller üzerinde bulunan emlakların (Arazi, Arsa, Bina) sisteme kayıtlarının yapılması ve takibini sağlamaktadır.

Tanımlar

BELBİS'te yer alan modüllerde kullanılan bazı sabit değerlerin (Gelir Ücret Tarifesi, ÇTV Grup Derece, Bina İnşaat Maliyetleri, vb.)tanımlanmaktadır.

İmar Planı Takip

Emlak Envanter Modülü ile entegre çalışan, belediye sınırları içindeki parsellerin imar işlemleri takip edildiği modüldür.

Dış Paydaş

Rayiç belgesi verilmesi amacıyla diğer kurumlara (Maliye, Tapu, vb.) verilen modüldür.

Taşınmaz

Belediye taşınmazlarının kayıt ve takibinin yapılmaktadır.

Ruhsat

Belediyelerin sınırları içerisinde yer alan işyerlerinin işyeri açma ve çalışma ruhsatlarının verilmesinde uygulanacak esas ve usulleri temel alarak, sıhhi ve gayrisıhhi işyerleri ile umuma açık istirahat ve eğlence yerlerinin ruhsatlandırılması ve bu ruhsatların denetlenmesini ilişkin bilgiler kayıt ve takip edilmektedir.

C-MALİ MODÜLLER

Muhasebe ve Bütçe

Mevzuata uygun yapısı ile muhasebe kullanıcılarının hata riskini ortadan kaldıran, Gelir, Personel ve Taşınır modülleri ile entegre çalışabilen bir modüldür. Sayıştay ve Maliye formatlarına uygun dosya formatları ve ay sonu işlemleri olan Muhtasar-Damga Vergisi-KDV Beyannameleri modülden alınabilmektedir.

Memur

SGK HİTAP Uygulaması ile entegre olarak Belediyede çalışan memur, sözleşmeli memur, başkan, başkan yardımcısı ve geçici görevli personellerin sicil bilgilerinin tutulması ve maaşlarının hesaplanmasını sağlar.

İşçi

Sendikalar ile yapılan toplu iş sözleşme bilgileri esas alınarak ücretin hesaplanması, bordro hazırlanmasını, özlük bilgilerinin tutulmasını sağlamaktadır.

Taşınır

Temin edilen mal alımlarının taşınır giriş ve çıkışlarının, amortisman işlemlerinin yapıldığı ve doğrudan temin ve muhasebe modülü ile entegre çalışan bir modüldür.

Yazı İşleri

Belediyenin encümen, meclis, komisyon toplantı kayıtlarının ve Başkan Vekâlet işlemlerinin oluşturulmasını sağlar.

Makine İkmal

Belediye araçlarının bakım, onarım, sigorta vb. takibini sağlar.

Doğrudan Temin

Mal ve Hizmet alımlarının Doğrudan Temin işlemleri Onay, Piyasa Fiyat Araştırması ve Muayene Kabul aşamaları iş akışları ile sistemimiz üzerinden sağlanabilmektedir.

Taşeron

Belediyede çalışan taşeron işçilerin özlük bilgilerinin, izin bilgilerinin, takip edildiği modüldür.

GEÇİŞ SÜRECİ

Belediyelerimizde mevcut bilişim sistemlerini değiştirme kararı oldukça geniş bir katılım ile alınması gerekli bir karardır. "Değişime karşı direnç" yalnızca belediye personelinde yaşanan bir durum olmayıp tüm insanlar için geçerli bir kavramdır. BELBİS' e geçiş de belediye personeline başlangıçta emlak envanteri oluşturma yükü getirmektedir. Bu yükü minimize etmek amacıyla Tapu Kadastro Genel Müdürlüğünden ve NVİ'den veriler alınarak belediyelerimize bir altlık verilmektedir. Sistem değişikliğinin en zor kısmı olan mevcut verilerin aktarımını % 100 e yakın gerçekleştirebilmek için aşağıdaki aşamalar uygulanarak bir belediye BELBİS ortamına alınmaktadır. Geçiş sürecinde belediyenin veri kaybı olmamasına büyük önem gösterilmektedir.

- Tanıtım
- Giriş Eğitimi
- Test Kullanımı
- Protokol
- Veri Çalışması Ve Envanter Oluşumu
- Kullanıcı Eğitimi
- Veri Aktarımı
- Canlı Sisteme Geçiş

Belediyenin Birliğimize yazılı başvurusu ile başlayan BELBİS geçiş süreci, yukarıdaki aşamalarının tamamlanmasıyla 3 ile 6 aylık bir sürebilmektedir.

AKILLI GÜVENLİK SİSTEMLERİ VE BARINDIRDIĞI RİSKLER

Evimizde kullandığımız pek çok cihaz yeni teknolojik özelliklerle donatılmış durumda. Ev güvenlik sistemleri de bunlardan biri. Kameralar, kilitler, hareketli dedektörler gibi akıllı telefonlardan veya internet üzerinden erişilebilen cihazlarla ev güvenliğimizi sağlamaya çalışıyoruz.

Ancak hayatımızın vazgeçilmez birer unsuru olmaya başlayan bu cihazlar, ailemiz ve evimiz için tahmin edildiği kadar güvenli olmayabilir. Hewlett Packard (HP) uygulama güvenlik test ekibi Fortify'daki araştırmacılar IoT ile bağlantılı en iyi 10 ev güvenlik sistemini test etmiş ve hepsinde pek çok açık tespit etmiştir. Araştırma sonucu ortaya konan rapora göre, ev sahibi evi izleyen tek kişi olmayabilir.

Çünkü sistemler ya zayıf parola politikaları ile yönetiliyor ya da hiç parolaya sahip değil. Ayrıca sistemlerin çoğunda ikili kimlik doğrulama seçeneği bulunmuyor. Araştırma, bulut sistemlerinde toplanan verilerin de savunmasız olduğunu ortaya koyuyor. Bu da başta hesap kimlik bilgileriniz olmak üzere pek çok verinizin siber saldırganlarca ele geçirilebileceği anlamına geliyor. Örneğin, bir hacker evde olup olmadığınızı öğrenebilir ya da evdeyseniz uzaktan evinizin en mahrem alanını bile gözetleyebilir.

Wi-Fi üzerinden çalışan kablosuz güvenlik kameraları açısından uygun önlemler alınmazsa bunlar da kullanıcılar için ek riskler oluşturabilir. Wi-Fi ile iletişimin doğası gereği bir hacker evinizdeki bir kameraya bağlanabilir ve pek çok verinize erişebilir.

Güvenliğimizi sağladığını düşündüğümüz akıllı ev sistemler karşısında hackerların yaratabileceği tehditleri anlayabilmek için şu soruları yakından incelemek gerekiyor

1. Güvenlik sistemimizde hangi kritik verileri bulunduruyoruz

2. Güvenlik sistemimiz hangi işlemleri gerçekleştiriyor

Özellikle video kayıtlarıyla olayların ve eylemlerin tarihsel günlüğünü tutmaya yarayan veriler, kritik verile-

Daha fazla bilgi için **http://quq.la/SWNd4** adresini ziyaret edebilirsiniz.

rimizi oluşturur. Bu verilerin başkalarının eline geçmesi durumunda önemli sorunlar oluşacağı aşikârdır. Örneğin, kötü amaçlı kişiler hırsızlık için kapı kilit sistemlerinin kontrolünü ele geçirebilirler, bina içine fark edilmeden girmek için video kayıtlarını kapatabilirler ya da suça delil oluşturabilecek kayıtları silebilirler.

Özellikle işletim sistemlerinin ve yazılımların güncel olmaması da güvenlik bakımından risk oluşturan bir hususdur. Eski yazılımlar hackerlar tarafından kolayca istismar edilebilir. Bu saldırılar bakımından veri sorumlusunun(-şirketin) veri güvenliğine ilişkin birtakım kanuni yükümlülükleri vardır. KVKK md.12'ye göre, veri sorumlusu, kişisel verilere hukuka aykırı olarak erişilmesini ve işlenmesini önleme ve kişisel verilerin muhafazasını sağlama amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

Akıllı sistemler hakkında değinilmesi gereken diğer bir konu da, tutulan kayıtların nerede saklandığı ve bunun güvenliğinin nasıl sağlandığıdır. Evinizin içinde, garajınızda veya aracınızdaki akıllı sistemlerden elde edilen verilerinizin güvenlik şirketlerince başka yerlere aktarılmadığından da emin olmak isteriz. Akıllı sistemlerce kaydedilen kişisel verilerinizin güvenliği için bunların başka amaçlarla kullanılmaması da gerekir. Bu yüzden, güvenlik amaçlı bu verileri işleyen bir şirket, faaliyetlerini de bu doğrultuda belirlemelidir. KVKK md.10'a bakıldığında, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi konusunda veri sorumlusunun kişilere bilgi verme yükümlülüğü vardır. Yine md.11 de bu konuda kişilerin haklarından bahseder. Herkes, veri sorumlusuna (burada verileri işleyen şirket) başvurarak kendisiyle ilgili;

- Kişisel veri işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerin eksik veya yanlış olması halinde bunların düzeltilmesini isteme ve
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğranması halinde zararın giderilmesini talep etme hakkına sahiptir.

Bununla birlikte barındırdığı riskler konusunda kullanıcılarda farkındalık oluşturmaya çalışan teknoloji şirketleri de mevcut. Bosch, Genetec ve SecureXperts siber saldırılara karşı dayanıklı video sistemleri tasarlamak ve geliştirmek için bir iş birliği geliştirdi. Ancak bu farkındalığın gerçekten yaratılabilmesi için sektördeki pek çok üretici, kişisel verilerin işlenmesi ve siber güvenlik konularında ilerleme kat etmelidir. Daha da önemlisi, tüketiciler bu hususları talep eder hale gelmelidir. Bunun sonucunda sektör açısından beklenen güvenlik seviyesine çıkılması, daha iyi hizmet sunulmasının da önünü açacaktır.

Tuna Taktak
Arbor Networks Türkiye

SİBER GÜVENLİKTE CDN AĞLARININ YERİ

CDN'ler, en sık rastlanan siber saldırılardan olan DDoS saldırılarından korunmanıza nasıl yardımcı oluyor?

İlk olarak, güvenlik bir CDN sağlayıcısının birincil odak noktası değildir. Onun temel işi içerik ve uygulama teslimidir. Saldırı araştırması, karşı önlemlerin geliştirilmesi ve tehdit istihbaratı en iyi olasılıkla ikinci planda kalan konulardır. Ayrıca, CDN sağlayıcıları saldırıların niteliğini araştırma, analiz etme ve anlamanın yanı sıra güvenliği destekleyecek bilinçli önerilerde bulunmak için yerleşik bir uzmanlığa sahip olmayabilir.

Bir CDN'nin ilk koruma önceliğinin kendi barındırdığı hizmetler olması anlaşılabilir bir durumdur. Son günlerde giderek daha fazla görülen kuvvetli ve çok büyük bir saldırı durumunda CDN, müşterilerinin tüm varlıklarını koruma kapasitesine sahip olmayabilir ve bazılarını savunmasız halde bırakmak zorunda kalır. Otomatik CDN karşı önlemlerinin de zaman zaman güvenli trafiği engellediği bilinmektedir. Ayrıca, CDN etki azaltma stratejileri, statik filtrelerden ve web uygulaması güvenlik duvarlarından (WAF) sıklıkla yararlandığı için, bulut tabanlı hizmetleri koruma esnekliğine ve istihbaratına sahip olmayabilir.

İlk olarak, güvenlik bir CDN sağlayıcısının birincil odak noktası değildir. Onun temel işi içerik ve uygulama teslimidir. Saldırı araştırması, karşı önlemlerin geliştirilmesi ve tehdit istihbaratı en iyi olasılıkla ikinci planda kalan konulardır. Ayrıca, CDN sağlayıcıları saldırıların niteliğini araştırma, analiz etme ve anlamanın yanı sıra güvenliği destekleyecek bilinçli önerilerde bulunmak için yerleşik bir uzmanlığa sahip olmayabilir.

Bir CDN'nin ilk koruma önceliğinin kendi barındırdığı hizmetler olması anlaşılabilir bir durumdur. Son günlerde giderek daha fazla görülen kuvvetli ve çok büyük bir saldırı durumunda CDN, müşterilerinin tüm varlıklarını koruma kapasitesine sahip olmayabilir ve bazılarını savunmasız halde bırakmak zorunda kalır. Otomatik CDN karşı önlemlerinin de zaman zaman güvenli trafiği engellediği bilinmektedir. Ayrıca, CDN etki azaltma stratejileri, statik filtrelerden ve web uygulaması güvenlik duvarlarından (WAF) sıklıkla yararlandığı için, bulut tabanlı hizmetleri koruma esnekliğine ve istihbaratına sahip olmayabilir.

İlk olarak, güvenlik bir CDN sağlayıcısının birincil odak noktası değildir. Onun temel işi içerik ve uygulama teslimidir. Saldırı araştırması, karşı önlemlerin geliştirilmesi ve tehdit istihbaratı en iyi olasılıkla ikinci planda kalan konulardır. Ayrıca, CDN sağlayıcıları saldırıların niteliğini araştırma, analiz etme ve anlamanın yanı sıra güvenliği destekleyecek bilinçli önerilerde bulunmak için yerleşik bir uzmanlığa sahip olmayabilir.

Bir CDN'nin ilk koruma önceliğinin kendi barındırdığı hizmetler olması anlaşılabilir bir durumdur. Son günlerde giderek daha fazla görülen kuvvetli ve çok büyük bir saldırı durumunda CDN, müşterilerinin tüm varlıklarını koruma kapasitesine sahip olmayabilir ve bazılarını savunmasız halde bırakmak zorunda kalır. Otomatik CDN karşı önlemlerinin de zaman zaman güvenli trafiği engellediği bilinmektedir. Ayrıca, CDN etki azaltma stratejileri, statik filtrelerden ve web uygulaması güvenlik duvarlarından (WAF) sıklıkla yararlandığı için, bulut tabanlı hizmetleri koruma esnekliğine ve istihbaratına sahip olmayabilir.

"HER ZAMAN AÇIK", HER ZAMAN İYİ DEĞİLDİR

CDN'ler "her zaman açık" koruma sağlar; bu özellik kulağa hoş gelse de yakından incelendiğinde bazı sorunlar oluşturur. "Her zaman açık" iki anlama gelebilir: Trafiğin

Daha fazla bilgi için **https://www.chip.com.tr/haber/siber-guvenlikte-cdn-aglarinin-yeri_73442.html** adresini ziyaret edebilirsiniz.

tıkanıklığı etkin bir şekilde araştıran ve otomatik olarak tetikleyen azaltma sistemlerinden sürekli olarak geçtiği ("her zaman azaltılan") veya olası saldırıları tespit etmek ve talep üzerine azaltma eylemlerini etkinleştirmek amacıyla trafiğin yalnızca izlenip pasif bir şekilde incelendiği ("her zaman izlenen"). Bu ikisi arasındaki farkın ve sağlayıcının hangisini sunduğunun anlaşılması önemlidir.

"Her zaman azaltılan" özellikteyse, maksimum saldırı azaltma ile güvenli trafiğe minimum etki arasındaki dengeyi değerlendirmeniz gerekir. Her zaman açık azaltmanın tek olası tamamlayıcı zararı hatalı pozitifler değildir. Hizmetler, gereksiz trafik incelemesi nedeniyle gecikebilir. "Her zaman izlenen" özellikteyse, saldırı algılama ilkeleri ve tepki süreleri karşısında görünürlüğü kaybetme riskiyle karşılaşırsınız. Gereksiz azaltmaları önleyebilirsiniz, ancak diğer yandan önemli saldırı göstergelerini kaçırabilirsiniz. Ayrıca, hacimsel saldırıları algılamak için tasarlanmış her zaman açık bir çözümün, ölçeği daha küçük olan uygulama katmanı saldırılarını kaçırma olasılığı yüksektir.

"Her zaman açık" koruma modelleri, tüm müşteriler için normal işlemleri korurken DDoS saldırılarını azaltmak için karmaşık trafik dengelemesi gerektirir. Son zamanlarda gözlemlenen büyük ölçekli saldırılar düşünüldüğünde bu önemlidir ve saldırıya uğramayan müşterilerde azaltma etkisine neden olabilir ya da saldırıya uğrayan müşterilerin toplam CDN kapasitesinin alt kümelerine ayrılması ile sonuçlanabilir. Müşteriler, her zaman açık sağlayıcının bazı müşterilere yönelik saldırıları, diğer müşterileri etkilemeden azaltmaya yönelik ölçeklenebilir mimariye sahip olup olmadığını dikkatlice değerlendirmelidir.

KARMA ÇÖZÜM

En iyi DDoS koruma uygulaması olarak karma güvenlik çözümlerini işaret eden sektör analist ve uzmanlarının sayısı giderek artmaktadır. Karma bir strateji; her zaman açık bir yerinde algılama ve azaltma sistemini, talep üzerine bulut tabanlı etki azaltma özellikleri ile bir araya getirir. Çoğu saldırı hala yerel olarak algılanamayacak ve azaltılamayacak kadar küçüktür. Ayrıca, yerel bir cihaz, uygulama trafiğini bir CDN çözümünden daha iyi tanır ve bu nedenle trafik modellerindeki anormallikleri daha iyi algılayabilir. Bulut tabanlı azaltma, yalnızca bir saldırı yerinde birimin kapasitesini belirgin biçimde aştığında otomatik olarak tetiklenir. Buna uygun olarak, bulut bileşeninin gerçek saldırılarla mücadele etmek için "her zaman açık" olması, maliyet tasarrufu yapması ve kapasiteyi koruması için bir neden yoktur.

Maliyet, CDN DDoS sağlayıcıları için temel faktörlerden biri olabilir. Ancak, karma bir çözüm şaşırtıcı oranda ekonomik olabilir. Sanallaştırma teknolojisi, pahalı donanımların yerini alabilir. Karma bir çözüm, tam yönetilen bir hizmet olarak dağıtılıp DDoS uzmanları tarafından desteklendiğinde ise maliyetler şirket içi BT ayak izinin ve güvenlik personeli gereksinimlerinin azalmasıyla dengelenebilir.

Son olarak, CDN çözümü tipik olarak büyük oranda otomasyondan yararlanır. Günümüzde saldırganlar kurnaz ve yaratıcıdır. Otomatik algılama ve etki azaltma özellikleri mutlaka gerekli olsa da, saldırıların engellenmesi için aynı zamanda kötü amaçlı saldırganlardan daha iyi ve akıllıca düşünebilmeyi sağlayan deneyim ve eğitime sahip bir ekip gerekir. Güçlü bir tehdit istihbaratı ağı ve kapsamlı bir araştırma programı, karma teknoloji çözümünün etkinliğini birkaç kat artırır; güvenliğin ikincil öneme sahip olduğu tipik bir CDN sağlayıcısına göre özel bir DDoS güvenlik uzmanında bulunma olasılığının daha yüksek olduğu güçlü yönler artar.

Wİ-Fİ PAROLASINI KOMUT SATIRINDAN ÖĞRENİN

Wi-Fi parolanızı unuttuysanız, onu PC'nizdeki kayıtlardan ortaya çıkarmanın bir yolu var.

Bilgisayarınızla Wi-Fi ağlarına bağlanıyorsanız, işletim sisteminiz genellikle bağlandığınız ağların parolasını kaydeder. Böylece aynı parolayı her defasında tekrar girmekten kurtulmuş olursunuz. Peki, parolayı unuttuysanız ve kayıtlı parolayı öğrenmek istiyorsanız, bunun bir yolu var mı?

Cevap evet. Daha önce oturum açtığınız bir Wi-Fi ağının parolasını Windows'ta öğrenmek için, önce yönetici haklarına sahip bir komut satırı çalıştırın. Ardından aşağıdaki komutu girin. ("AĞ ADI" yazan yere bağlı olduğunuz Wi-Fi ağının ismini yazmayı unutmayın)

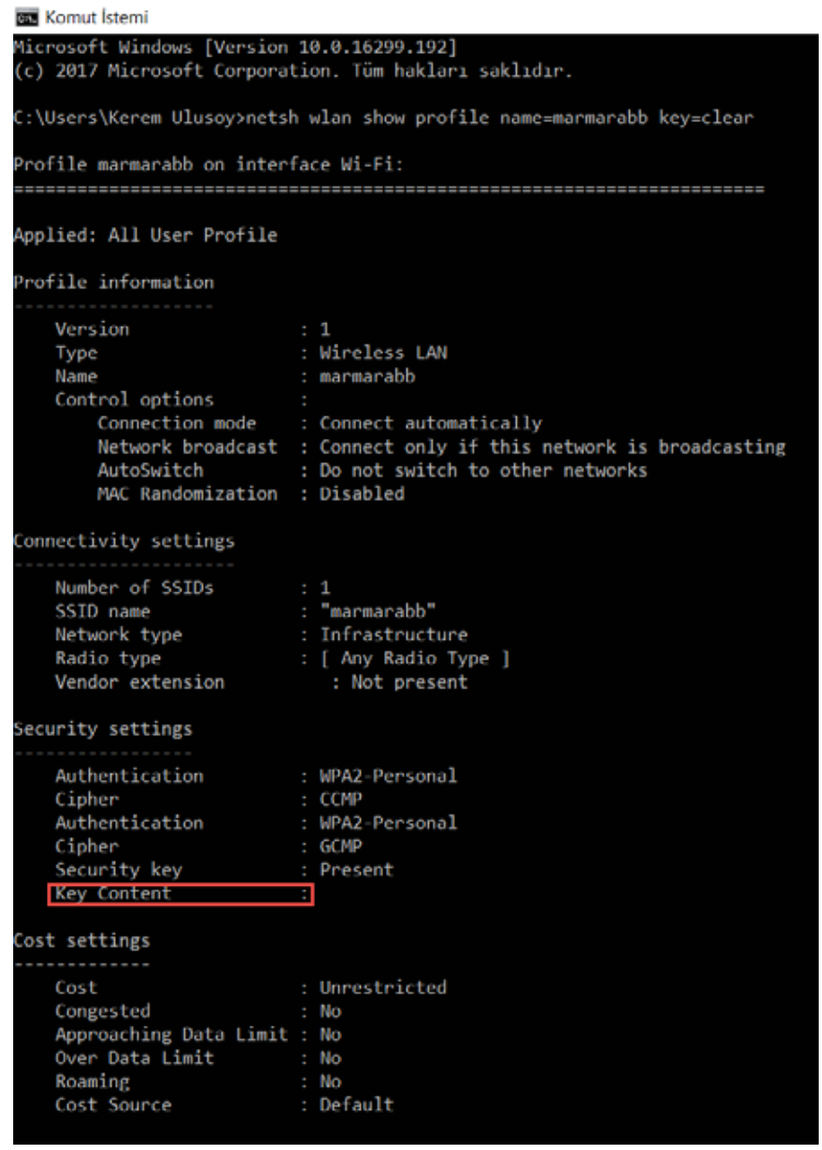
netsh wlan show profile name=AĞ ADI key=clear

Ekrana bir dizi metin gelecek. Parolayı Security bölümü altında, "Key Content"in karşısında görebilirsiniz.

MacOSX'te ise Terminal'i açmanız ve aşağıdaki komutu girmeniz gerekiyor. ("AĞ ADI" yazan yere bağlı olduğunuz Wi-Fi ağının ismini yazmayı unutmayın)

security find-generic-password -ga AĞ ADI " grep password

Hepsi bu kadar, artık bağlı olduğunuz ağın parolasını biliyorsunuz.



Daha fazla bilgi için **Kaynak: http://quq.la/8OnLY** adresini ziyaret edebilirsiniz.

BOSCH IOT KAMPÜSÜ AÇTI

Bosch IoT çalışmalarına hız kesmeden devam ediyor. Berlin'de açılan Bosch IoT kampüsü ile dijital dönüşüme yönelik yeni projeler geliştirilecek, iş birlikleri kurulacak.

BOSCH IOT ÇALIŞMALARI

Bosch, nesnelerin internetine yönelik girişimlerini destekleyecek bir adımla Berlin'de yeni bir merkez açtı. Şirket Berlin'deki merkezini, yazılım ve donanım sağlayıcıları, teknoloji ortakları ve yeni girişimlerle ilgili çözümler üzerinde çalışmak için kullanacak. Bosch, yeni IoT kampüsünde bu alanda çalışan birçok şirketle ortak çalışmalar yürütmeyi amaçlıyor.

Bosch CEO'su Dr. Volkmar Denner "Yeni tesislerimizde, kendi IoT uzmanlarımızla Berlin'in dijital sahnelerindeki köprüleri inşa ediyoruz. IoT kampüsünün açılışı, Berlin'in dijital bir başkent olması için bir diğer önemli yapı taşıdır. Açık hava ekosistemleri, açık iş birliği ve ortaklık ile nesnelerin interneti özgürlüğüne inanıyoruz. Bu fikir, kampüs kavramına da yansıyor" dedi.

Yeni kampüste 250'den fazla Bosch iştirakçisi çalışıyor. Önümüzdeki birkaç yıl içinde, çalışan sayısının yaklaşık 400'e çıkması bekleniyor. Bosch yeni kampüsü ile IoT alanında örnek bir girişime imza attı.

Daha fazla bilgi için **Kaynak: http://quq.la/8OnLY** adresini ziyaret edebilirsiniz.

İsmail Hakkı Polat
Kadir Has Üniversitesi

BİTCOİN'E NEDEN İHTİYAÇ DUYDUK

Başta BitCoin olmak üzere kendini finans sisteminden ve hatta diğer dijital paralardan da ayrıştıran KriptoPara kavramı neden bu kadar çok ilgi görüyor

İstanbul'un sonbahar trafiğinin keşmekeşinde her zamanki gibi sağa sola bakarak ağır ağır ilerlediğim geçtiğimiz günlerin birinde, arabanın radyosundan "BitCoin" kelimesini duyunca dikkatimi radyoya verdim; BloombergHT kanalının radyosunda kanalın yayın yönetmeni Cüneyt Başaran ile programın sunucusu Açıl Sezen Bitcoin üzerine hararetli bir tartışmaya girmişlerdi. Programa telefonla bağlanan dinleyicilerin de sorularıyla konu birçok boyutuyla dile getirildi, doğru-yanlış birçok kavram tartışıldı ve finalde Cüneyt Başaran, beni o günden bugüne düşündüren şu soruyla konuyu kapattı; "Bunların hepsini tartışabiliriz ama hepsinden önce BitCoin, finans dünyasının hangi eksikler yüzünden ortaya çıktı ve bunlara getirdiği hangi çözümlerden dolayı talep görmekte" Bu sorular üzerine kafa yormamız ve yanıtlarını bulmamız gerekli!"

Sayın Başaran'a işin daha bu sürecin en başından sorulması gereken soruları nihayet sorduğu ve geniş kitlelerle paylaştığı için müteşekkir olmamız lazım. Hem bir dinleyicisi hem de KriptoPara konularında kalem oynatan biri olarak soruyu "Türkiye ve dünyada bankacılık ve finans sektörünün hangi eksik ve yanlışları, BitCoin'i 100 milyar dolar değerinde bir finansal araç haline getirdi şeklinde düzenleyerek kendi penceremden maddeler halinde yanıtlamaya çalışayım;

1. Bankaların her türlü işlemden aldığı hizmet ücretleri ve komisyonlar çok pahalı. (Aslında Türkiye bu konuda en iyi ülkelerden ve biz de ücretsiz olan pek çok hizmet için dünyanın her yerinde müşterilere faturalanmakta.)

2. Bankalar arası para transferleri (özellikle ülkeler arası olanlar) bürokratik, çalışma saatleriyle sınırlı ve yavaş.

3. Finans kurumlarının müşterileriyle yaptıkları sözleşmeler, fazlasıyla kendi çıkarlarını gözeten maddelerle dolu. Buna karşılık müşterinin değer saklama ya da yükseltme amaçlı emanet ettiği varlıkları muhafaza etmek konusunda rahat, başına buyruk hareket eden hatta kimi istisnai kriz durumlarında da riske edebilen bir doğası var. 90larda Türkiye ile Arjantin, 2008'de ABD ve 2015'te de Yunanistan gibi ülkeler üzerinden örnekleyebileceğimiz pek çok örneği var bunun.

Oysa KriptoPara sistemlerinde bu ücretler çoğu durumda sistemin KriptoPara üretimiyle (madencilik) ilişkilendirilerek bünyeden karşılanmakta ve kullanıcıya yansıtılmamakta. Son dönem Bitcoin transferlerinde istenen ücretler bile bankalarınkinin yanında devede kulak; Sadece hızlı hizmet talep edilen kimi durumlarda ise çok cüzi (en fazla birkaç dolar) önceliklendirme ücretleri alınabildiğini de ekleyelim.

Ayrıca, KriptoParalarda banka gibi bir kurum olmadığından bir kişinin KriptoCüzdanından diğerininkine aracısız, 724 ve bankalara göre çok daha hızlı çalışmakta. Birkaç hafta önce bir cumartesi akşamı Finlandiya'da bir start-up ekibine verdiğim eğitim sırasında demo amaçlı gönderdiğim 1 dolar karşılığı BitCoin, karşıdaki ekibin yeni açtırdığım cüzdanına 6 dakikada transfer olunca o kadar hoşlarına gitti ki, eğitim ücretini BitCoin olarak ödemeyi bile teklif ettiler)

Bunun da ötesinde, Finansal Kurumların geliştirdiği dijital para hizmetlerinin, kullanıcıların varlıklarını kriptolu şifrelemeyle güvence altına alıp gözlerden uzak saklayabilen ve dünyanın her yerinde hemen her ülkenin para birimine çevrilip harcanabilen KriptoParalar karşısında rekabet etme şansları da az.

Kuşkusuz, başta BitCoin olmak üzere diğer tüm KriptoParaların da mevcut bankacılık ve finans sektörüne karşı eksikleri, yanlışları ve çok da fazla riskleri var. Ancak insan doğası hep mevcudu diğeriyle karşılaştırarak değerlendirme ve yargılama yapar. Bu da mevcut finansal kurumlar açısından büyük bir dezavantaj. Ancak finans ve bankacılık dünyasının dönüşüme öncelikle kendi öz eleştirisini yaparak girişmesi, her halükarda en sağlıklı başlangıç olur.

Daha fazla bilgi için **http://quq.la/dCc3R** adresini ziyaret edebilirsiniz.

LIGHTNING NETWORK (YILDIRIM AĞI) NEDİR, NASIL ÇALIŞIR?

"Lightning Network Nedir"in kısa cevabı, kendi sitelerinde söyledikleri gibi tanımlanabilir: Ölçeklenebilir, Anlık Bitcoin/Blockchain İşlemleri…

Lightning Network Türkçe adıyla Yıldırım Ağı, Bitcoin'in transfer yavaşlığı ve ölçeklenebilirliğinin anahtarı olacak sistemin kendisidir. Bitcoin'i bir cüzdandan bir cüzdana veya bir borsaya göndermek istediğinizde dakikalarca hatta bazı durumlarda saatlerce bekleyebiliyoruz. İşte Lightning Network bu işlemi saniyelere indirmeyi vadediyor ve binlerce transferi miktar önemli olmadan saniyeler içinde gerçekleştireceğini söylüyor.

Lightning Network'ü teknik anlamda anlatmak istersek, çift yönlü ödeme kanallarının bir Mesh Network aracılığıyla Bitcoin, Litecoin, Vertcoin gibi para birimlerinin mikro boyuttaki ödemelerini yapmak için kullanılan P2P sistemidir. Lightning Network'e kısaca LN denilir ve LN'de fonlarınızı (paranızı) kimseye emanet etmeden (borsa, 3. kişi veya kurum) işlem yapabilirsiniz.

BİTCOİN ÖLÇEKLENDİRME SORUNU NEDİR?

Bitcoin ağı her 10 dakikada 1 MB'lik bloklar oluşturur ve saniyede maksimum 7 transfer gerçekleştirebilir. Bu rakam size oldukça iyi gelmiş olabilir ama Visa'nın saniyede 2.000 transfer yapabildiğini bilirseniz, 7 transferin ne kadar küçük bir rakam olduğunu anlarsınız.

Özellikle Bitcoin'e karşı artan taleple birlikte işlemler fazlalaştı. Böylece yoğunluk ve yapılabilen transfer adedine bakıldığında yoğun anlarda transferler aşırı gecikebiliyor ve mining (madenci) ücretleri artabiliyor. Bunun dışında blok boyutları artırıldığında toplam Bitcoin blok zincirinin boyutu da artacağı için (şu an yaklaşık 125GB'lik bir boyutu vardır) uzun vadede blok zincirin hızlıca büyümesine ve ağdaki senkronizasyon süresinin uzayacağından korkuluyor.

1 Ağustos 2017 tarihinde oluşan fork (çatallaşma) sonucu ortaya çıkan Bitcoin Cash, blok boyutunun artırılması fikrinden ortaya çıkıp asıl Bitcoin zincirinden ayrılmıştır.

LİGHTNİNG NETWORK NASIL ÇALIŞIR?

Lightning Network, kişiler arasındaki transferlerin ana blok zincirinde (blockchain) yayınlanmadan yapılmasını sağlar. Böylece madencilere ücret ödemeye gerek kalmadan Bitcoin, Litecoin ve Vertcoin gibi fonları transfer eder.

Lightning Network, blok zincirin temel teknolojisine bağımlıdır. Gerek Bitcoin blok zincir işlemlerini kullanarak, gerekse Ethereum'dakine benzer akıllı sözleşmeli sistemler aracılığıyla, yüksek hacim ve yüksek hızda işlem yapabilen güvenli bir katılımcı ağı oluşturur.

Lightning Network'de, iki katılımcı, blok zincirinde her iki katılımcının da herhangi bir fon harcamasını imzalamasını gerektiren bir defter kütüğü girişi oluşturur. Buna "Multi Signature Address" denir. Bu adresin iki ayrı özel anahtarı (private key) vardır. Birinci katılımcı diğerinin özel anahtarını asla bilmez. Her iki taraf da yaptıkları işleme göre bu sisteme bir işlem girdisi oluştururlar. Böylece iki katılımcı arasında "Bi-Directional Channel" kurulmuş olur. Fonlama dışında hiçbir transfer ana blok zincirinde yayınlanmaz. Bu kanalın ne kadar uzun süre açık olacağı bu iki katılımcıya bağlıdır.

Bunu bir örnekle anlatalım. Ahmet ve Ayşe, 1 BTC'lik bir para transferi yapmak istiyor. Yani Ahmet, Ayşe'ye 1 BTC gönderecek. İlk önce LN yardımıyla blok zinciri üzerinde bir defter kütüğü girişi (Multi Signature Address) oluştururlar. Bu kütük içinde Ahmet, Ayşe'ye 1 BTC'yi şu tarihte göndereceğim der ve kendi özel anahtarıyla bunu imzalar, Ayşe'de Ahmet bana 1 BTC'yi şu tarihte gönderecek diyerek o da kendi özel anahtarıyla işlemi imzalar. Eğer belirtilen tarihe kadar taraflardan biri işleminden vazgeçmezse işlem gerçekleşir. Böylece aktarım blok zinciri dışındaki bir kanal içinde gerçekleşir.

Bu kanal içinde yapılan her işlemden sonra eski özel anahtarlar geçersiz olur ve değiştirilir.

"İki Yönlü Ödeme Kanalı" denilen bu sistemde iki katılımcı, blok zincirinde her iki katılımcının da herhangi bir fon harcamasını imzalamasını gerektiren bir defter kütüğü girişi oluşturur. Her iki taraf, yaptıkları ödeme ve para alma işlemini oluşturur ama bunu blok zincirinde yayınlamaz.

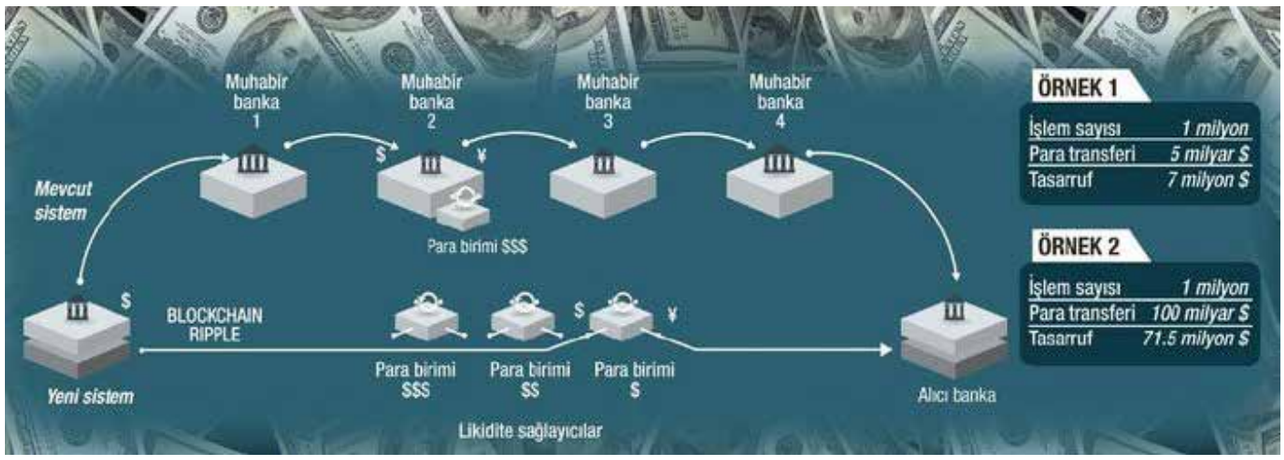
Bu iki katılımcı arasındaki bütün işlemler bittiğinde veya kanalı kapatmak istediklerinde karşılıklı olarak son transferler yapılır ama bu kez bu işlemler özel anahtarlar olmadan yapılır ve son hesaplar blok zincirinde yayınlanır.

Bu kanalların sanki bir sosyal ağ gibi binlerce kişi arasında açık olduğunu ve devamlı işlemler yapıldığını düşünün… Bu işlemlerin hızı, blok zincire yapacağı yarar, Bitcoin'i günlük hayatta kullanılabilecek bir yapıya dönüştürmesi gibi artıları Lightning Network'ü merakla beklememize neden oluyor.

Daha fazla bilgi için **http://quq.la/RZEKL** adresini ziyaret edebilirsiniz.

SWİFT'E ALTERNATİF SİSTEM RİPPLE'DEN (KRİPTO PARA) GELDİ

Blockchain sistemi para transferi ağına dönüştü. Akbank'ın da olduğu 100'ü aşkın banka, ripple firmasının altyapısı ile yurtdışına para göndermeyi 3 günden 10 dakikaya düşürecek. 100 milyarlarca $'lık transferden milyonlarca $ tasarruf sağlanacak.



Bankacılık sektörü, bitcoin'in altyapısını oluşturan blockchain sistemini para transferi ağına dönüştürüyor. Akbank'ın da içinde olduğu 100'ü aşkın banka, ripple firmasının altyapısı ile yurtdışına para göndermeyi 3 günden 10 dakikaya düşürecek. Bu sistem sonrası bankalar hem zaman hem de maliyet avantajı sağlayacak. Akbank Direkt Bankacılıktan Sorumlu Genel Müdür Yardımcısı Tolga Ulutaş, blockchain sisteminin bankaların kârlarına olumlu yansıyacağını belirtti. Ulutaş, maliyetin azalmasını müşterilerine de yansıtacaklarını söyledi. 100 banka arasında UBS, Unicredit, BBVA, Credit Agricole ve Mizuho gibi küresel ölçekte bankalar var.

MİLYONLARCA $ TASARRUF

Ripple ile yapılan işlemlerde bankaların sağlayacağı maliyet avantajı ise milyonlarca doları buluyor. Örneğin yılda 1 milyon işlem yapan ve toplamda 5 milyar doları yurtdışına yollayan üç banka bu işlemlerden işlem başına 6.86 dolarlık tasarruf sağlayacak. Yıllık toplam tasarruf miktarı ise 7 milyon doları bulacak.

Aynı işlem sayısında rakam büyüdükçe bankanın maliyet avantajı da artıyor. Örneğin yine 1 milyon işlem ile 100 milyar dolar yollayan bankalar 71.5 milyon dolarlık tasarruf sağlıyor. Tüm bunlara ilave olarak bir de zamanın azalması nedeniyle kur riski de ortadan kalkıyor. Kurdaki yukarı ya da aşağı yönlü üçdört günlük fark yansımıyor. Tolga Ulutaş, "Şu anda fiyatlamayı önceden yapamıyoruz. 'İşlem bittikten sonra şu kadarlık bir fatura çıktı' diyoruz. Bu ortadan kalkacak" dedi.

BİTCOİN KULAK İSE BLOCKCHAİN UZAYAN BOYNUZDUR

BItcoin'in çıkışındaki amacın para transferi olduğunu belirten Ulutaş, "Eğer siz Bitcoin'i para transferi için kullanmak isterseniz, Bitcoin'in bir tanesinin değerinin bir lira mı yoksa 1 milyon lira mı olduğu sizin için çok önemsiz bir şey. Ama bunu yatırım aracı gibi alıp da üzerine çökerseniz başka bir şey yapmış olursunuz. Şu anda ki süreç kafa karışıklığından kaynaklandı. Ondan sonra birçok kripto para birimi çıktı. Bitcoin'in kendisi önemli değil, Blockchain önemli. Blockchain dünyada birçok işletmenin iş yapış şeklinde inanılmaz tasarruf ve hız sağlayacak bir şeydir. Bitcoin kulak ise Blockchain uzamakta olan bir boynuzdur" dedi.

İHRACATÇI İÇİN ÖZEL BLOK

Blockchain teknolojisinin içinde barındıran ve birçok şirketi bir araya getirmeye yarayan 'dağıtık defter' teknolojisini de kullanmaya başlayacaklarını belirten Tolga Ulutaş, "Şu anda bir ihracat için önce üretim, sonra karşıdaki firma ile görüşmeler, ardından bankalar ile görüşme ve sigorta ile lojistik firmaları ile görüşmeler yapılıyor. Bu firmaların tamamı birbiriyle onlarca işlem yapıyor. İhracat üç dört hafta sonra yapılabiliyor. Üzerinde çalıştığımız yeni sistem ile tüm bu paydaşların tek seferde ve aynı anda tüm detayları onaylayabileceği bir hale getireceğiz. Böylece bir günde tüm işlemler bitecek. Bu sistem ile ilgili olarak da Türkiye'nin ağırlıklı olarak ihracat yaptığı ülkelerdeki bankalarla görüşmelerimiz sürüyor" şeklinde konuştu.

Daha fazla bilgi için **http://www.teknokulis.com/haberler/guncel/2017/12/21/swifte-alternatif-sistem-1513883478** adresini ziyaret edebilirsiniz.

CLOUDFLARE'DEN 1.1.1.1 DNS HİZMETİ

1 Nisan şakası gibi dursa da Cloudflare'in gizlilik ve hız odaklı yeni DNS hizmeti, tamamen gerçek.

Cloudflare'in DNS hizmetinin tanıtılmasının hemen ardından ülkemizde engellendiği ortaya çıktı. Engelleme sadece standart DNS hizmetini kapsamıyor - DNS üzerinden TLS gizlilik işlevi de engellenmiş görünüyor.

ABD merkezli internet altyapısı firması Cloudflare, tüketiciye yönelik ilk ürününü, 1.1.1.1 DNS hizmetini ortaya çıkardı. Başından söyleyelim, bu bir 1 Nisan şakası değil, gerçek.

Gizlilik ve hıza odaklanan DNS hizmeti 1.1.1.1, Cloudflare'in dünya çapında yayılmış olan altyapısının gücünden yararlanıyor. DNSPerf'e göre 1.1.1.1 şimdiye kadar sunulmuş olan en hızlı DNS hizmeti.

Cloudflare'in iş modeli kullanıcı verilerini toplamaya dayanmıyor. Firma bu yüzden bir adım ileri atarak DNS sorgularının geldiği IP adresini diske hiç yazmıyor ve tüm günlüklerini 24 saat içerisinde siliyor. Bu ise 1.1.1.1 kullanıcılarının detaylı bir profilinin oluşturulmasını imkansız kılıyor.

ŞİFRELİ DNS'İ DE DESTEKLİYOR

Standart DNS hizmetleri şifresiz olduğu için, internet trafiğinizi izleyen biri hangi alan adlarını sorguladığınızı rahatça görebiliyor. Buna karşın Cloudflare'in DNS hizmeti, hem DNS-over-TLS'i, hem de DNS-over-HTTPS'i destekliyor.

TÜRKİYE'Yİ ÖRNEK VERDİ

Cloudflare, duyurusunda DNS gizliliğinden bahsederken ilginç bir detay göze çarptı. Firma, Mart 2014'te Türkiye'de Twitter'ın engellenmesini örnek gösterdi ve duvarlara yazılan Google DNS'inin IP'lerini hatırlattı.

GERÇEKTEN GÜVENİLİR Mİ?

Teknoloji firmalarına eskisinden çok daha fazla şüpheyle yaklaştığımız şu sıralarda Cloudflare, böyle bir hizmeti para kazanmadan neden sunuyor olabilir? Matthew Prince, firmanın görevinin "daha iyi bir internet sunmak" olduğunu, performans ve gizlilik sorunlarını çözmenin bunun için doğru yaklaşım olduğunu söylüyor.

Verilerimizin, gizliliğimizin ve bu yolla beynimizin dev firmalara oyuncak olduğu şu günlerde birilerinin iyilik yapmanın iyilik getireceğine inandığını görmek, güzel bir şey olsa gerek.

Daha fazla bilgi için **http://quq.la/ZUnVj** adresini ziyaret edebilirsiniz.

REKABETİ ÜÇ BOYUTLU YAZICILAR BELİRLEYECEK

General Electric (GE) tarafından gerçekleştirilen ve iş dünyasının inovasyon konusundaki yaklaşımını küresel bazda ve Türkiye özelinde mercek altına alan 6. GE Küresel İnovasyon Barometresi'nin sonuçları açıklandı. Türkiye'nin de dahil olduğu 20 ülkeyi kapsayan 2 binin üzerinde inovasyon yöneticisinin katıldığı araştırma; üç boyutlu yazıcının potansiyeli, inovasyonun finansal sonuçlara etkisi, inovasyonda öne çıkan ülkeler, inovasyonda çok uluslu şirketlerin öncülüğü, korumacı politikalara olan yerli ve küresel yaklaşım, popüler olan kavramlar ve inovasyonda yeteneğe duyulan ihtiyaç konusunda önemli sonuçlar ortaya koyuyor. Araştırmaya göre, Amerika ve Almanya gibi inovasyona liderlik eden ülkeler hız keserken Japonya ve Çin liderliğindeki Asya ülkeleri ise inovasyonun alternatif merkezleri haline geliyor. Bu yıl altıncısı gerçekleştirilen araştırmanın sonuçlarını açıklayan GE Türkiye Yönetim Kurulu Başkanı ve Genel Müdürü Canan M. Özsoy, inovasyonda başarılı olan şirketlerin veriyi etkin bir şekilde kullandığını ve dijital becerileri iş modelinin merkezine yerleştirdiğini, bunun da Türk şirketleri açısından yol gösterici olduğuna dikkat çekti.

TÜRK CEO'LARIN DA GÜNDEMİNDE

Araştırma üç boyutlu yazıcının potansiyelinin yöneticileri oldukça heyecanlandırdığını gösterdi. Araştırmaya katılan küresel yöneticilerin yüzde 63'ü, Türk yöneticilerin ise yüzde 79'u üç boyutlu yazıcının pazara pozitif etkisinin olacağını belirtiyor.

Daha fazla bilgi için **http://quq.la/8mcZR** adresini ziyaret edebilirsiniz.

KAĞIT KADAR İNCE VE ESNEK LCD ÜRETİLDİ

LCD teknolojisi üzerinde çalışma gerçekleştiren araştırmacılar, kağıt kadar ince ve esnek fakat çok daha dayanıklı bir LCD türü üretmeyi başardılar.

Çin ve Hong Kong'dan optoelektronik mühendisleri, kağıt kadar ince, esnek ve hafif bir LCD üretmeyi başardılar. Amerikan Fizik Enstitüsü AIP'nin Applied Physics Letters adlı dergisinde yayınlanan rapora göre yeni üretilen LCD türü, optik olarak yeniden yazılabilme özelliğine de sahip.

Yeni LCD türü, standart LCD'lerde olduğu gibi sandviç bir yapıya sahip olmasına karşın, iki panel arasında sıvı kristal doldurulmasıyla elde ediliyor. Fark olarak ise standart LCD'lerde görüntüyü değiştirmek için paneller arasındaki pikseller yanıp sönerken, optik olarak yeniden yazılabilir LCD'lerde görüntüyü değiştirmek için polarize ışık varlığında hizalanan özel moleküller kullanılıyor.

Yeni teknoloji, görüntü oluşturmak için geleneksel elektrotlara olan ihtiyacı yok ederken yeniden yazılabilir olmasına karşın daha ince LCD'ler üretilmesini mümkün kılıyor. Bu yeni teknoloji LCD'ler yarım milimetreden daha ince olabiliyorlar, esnek plastikten oluşuyorlar ve yalnızca birkaç gramlık ağırlığa sahipler.

Donghua Üniversitesi'nden çalışmanın yardımcı yazarı Jiatong Sun, kağıttan yalnızca biraz daha kalın olan yeni LCD'nin basit yapısı nedeni ile maliyetinin son derece düşük olduğunu, buna rağmen son derece sağlam bir yapıya sahip olduğunu söyledi. Ayrıca yeni LCD'ler görüntüler değiştirilmediği sürece herhangi bir enerji harcamıyor.

İkinci inovasyon ise plastik veya cam tabakaları ayırmak için ara parça kullanılmasıydı. "Cam tabakalar arasına ara parça koyarak, sıvı kristali tek parça halinde tutabiliyoruz." diyen Sun, her ne kadar bugün LCD tabakalar arasına ara parça konulsa da, sıvı kristalin kalınlığını belirlemek ve sabit kalınlık sağlamak gerektiğini belirtti.

Sıvı kristalin kalınlığını sabit tutmak kontrast, tepki süresi ve görüş açısının bozulmamasını sağlıyor. Yine de plakalar büküldüğünde sıvı kristaller, çarpışma bölgesinden uzaklaşıyor, alanı boş bırakıyordu. Fakat plakaların esnek yapısı, bu sorunun de üstesinden gelinmesini sağladı.

Araştırmacılar, LCD büküldüğünde dahi görüntünün bozulmaması için üç farklı ara yapıcı denediler ve ızgara benzeri tasarımın LCD bükülse bile sıvı kristali akmaktan alıkoyduğunu keşfettiler. Bu keşif, ilk optik olarak yeniden yazılabilir LCD'nin üretilebilmesini sağladı. Üstelik yeni LCD teknolojisinin 5 inçi yalnızca 5 dolara mal ediliyor.

Daha fazla bilgi için **http://quq.la/cMpJK** adresini ziyaret edebilirsiniz.

PEŞİNDEKİ SOSYAL MEDYA CANAVARI: FACEBOOK

ISWA; hem ulusal hem de yerel düzeyde politika yapıcıları, planlamacıları ve yöneticileri, 21-26 Mayıs 2018 tarihlerinde İtalya'nın Bologna şehrinde düzenlenecek "Katı Atık Yönetimi için Tasarım Çözümleri - Düşük ve Orta Gelirli Ülkeler için Bir Yöntem ve Araç Seti" konulu Bahar Okuluna katılmaya davet ediyor.

Cambridge Skandalı ile sarsılan sosyal medya devi Facebook'un senin hakkında ne kadar bilgiye sahip olduğunu, bu sitedeki paylaşımlarını ucunun nereye vardığını hiç düşündün mü?

Yaptığın ve son anda yapmaktan vazgeçtiğiniz paylaşımları bile takip edip saklayan Facebook, sana ayakkabı satmaya çalışmaktan kiminle flört ettiğine veya kime karşı sempati duyduğunu bile anlayabilecek bir noktada. Sosyal medya devi, online kadar offline bilgilerinin de peşinde. Bunları da satın alıp algoritmanın içine eklemeye çalışıyor… Bunlar, Zeynep Tüfekçi'nin TED konuşmasından yansıyanlar. Konuşmanın ayrıntılı bir özetini ve konuşmanın kendisini aşağıda bulabilirsiniz:

İnsanlar yapay zekâyla ilgili korkularını dile getirdiğinde, genellikle kontrolden çıkmış insansı robotları hayal ederler. Terminatör gibi. Düşünmeye değer olsa da uzak bir tehdit bu… Yakın gelecekteki bağımsızlığımızı ve itibarımızı tehdit eden teknolojinin büyük kısmı veri ve dikkatimizi toplayıp reklamcı ve benzerlerine satan şirketler tarafından geliştiriliyor: Facebook, Google, Amazon, Alibaba, Tencent.

Gelin, dijital hayatımızdaki temel bir gerçeğe bakalım… İnternet reklamları. Bir örnek verelim. Diyelim ki Las Vegas'a uçak bileti satmak istiyorsunuz. Eski düzende, de-

neyim ve öngörülerinize dayanarak hedef bir demografik kesim belirlersiniz. Reklam yapmayı da deneyebilirsiniz, 25 – 35 yaş aralığındaki erkekler veya kredi kartı limiti yüksek olan insanlar veya emekli çiftler, değil mi? Geçmişte böyle yapardınız. Şimdi büyük veri ve makine öğrenimi ile işler artık böyle yürümüyor.

Bunu anlamak için, Facebook'un sizinle ilgili sahip olduğu tüm verileri düşünün: Yazdığınız her durum bildirisi, her bir Messenger sohbeti, oturum açtığınız her konum, yüklediğiniz tüm fotoğraflar. Bir şey yazmaya başlayıp sonra vazgeçip silerseniz, Facebook bu silinenleri de saklayıp analiz ediyor. Çevrimdışı verilerinizle sizi gitgide eşleştirmeye çalışıyor. Ayrıca veri acentalarından da çok fazla veri satın alıyor. Finansal kayıtlarınızdan tarama geçmişinize kadar her şey bu veri setinde olabilir. ABD'de bu tür veriler rutin olarak toplanıyor, karşılaştırılıyor ve satılıyor. Avrupa'da daha sıkı kurallar var.

Yani aslında olan şey, tüm bu veriler harmanlanarak, bu makine öğrenimli algoritmalar daha önce Las Vegas'a gitmek için uçak bileti alan insanların özelliklerini nasıl ayrıştıracaklarını öğreniyorlar. Var olan verilerden bunu öğrendiklerinde, bunu yeni insanlara uygulamayı da öğreniyorlar. Böylece, yeni bir bireyle karşılaştıklarında onun Las Vegas'a bilet alıp almayacağını sınıflandırabiliyorlar. Olsun, diye düşünüyorsunuz, alt tarafı Vegas'a uçak bileti teklifi. Görmezden gelebilirim. Ancak asıl sorun bu değil. Asıl sorun şu ki biz bu karmaşık algoritmaların nasıl çalıştığını artık anlamıyoruz.

Bu sınıflandırmayı nasıl yaptıklarını artık anlamıyoruz. Dev matematik matrisleri, binlerce sıra ve sütun, belki de milyonlarcası… Ve tüm verilere sahip olsalar bile, ne programcılar, ne bunları inceleyen herhangi biri bunun tam olarak nasıl işlediğini anlayabiliyor. Tıpkı size beynimden bir kesit göstersem ne düşündüğümü anlayamayacağınız gibi. Sanki artık programlama yapmıyoruz, tam olarak anlayamadığımız bir bilinç geliştiriyoruz. Ve bu mekanizmalar yalnızca müthiş miktarda veri varsa çalışıyor, dolayısı ile hepimizin üzerinde kapsamlı bir gözetleme de teşvik ediliyor ki makine öğrenimli algoritmalar işini yapabilsin. Bu yüzden Facebook, hakkınızda toplayabildiği tüm veriyi istiyor. Algoritmalar daha iyi çalışıyor…

Deneyler gösteriyor ki algoritmanın sizin için seçtikleri duygularınızı etkileyebilir. Bununla da bitmiyor. Siyasi davranışınızı da etkiliyor. 2010 yılı orta dönem seçimlerinde, Facebook, ABD'deki 61 milyon insan üstünde daha sonra açıklanan bir deney yaptı.

Bir grup insana "Bugün seçim günü" yazısı gösterildi, bu daha basit olandı, diğer bir gruba ise aynı şey, küçük bir farkla gösterildi: "Oy verdim" butonuna tıklayan arkadaşlarının küçük fotoğraflarının bulunduğu versiyon. Bu kadar basit bir nüans. Değişen tek şey fotoğraflardı ve seçmen kütüğünce de onaylandığı üzere, bu araştırmaya istinaden yalnızca bir kez gösterilen bu paylaşım o seçimde 340.000 ek seçmen olarak sonuçlandı. Şans eseri mi? Hayır. Çünkü 2012'de aynı deneyi tekrarladılar. O zaman, yalnızca bir kez gösterilen sivil mesaj 270.000 ek seçmen olarak geri döndü.

Hatırlatayım, 2016 ABD başkanlık seçimleri yaklaşık 100.000 oy farkıyla belirlendi. Yani Facebook kolaylıkla politikanız hakkında çıkarım yapabiliyor, siz bunu sitede hiç açıklamamış olsanız bile. Bu algoritmalar bunu oldukça kolay başarabiliyorlar. Peki ya bu güce sahip bir platform bunu adaylardan birinin destekçilerini arttırmak için kullanırsa? Bundan haberimiz olur mu?

Masum gibi görünen bir yerden başladık: Bizi takip eden reklamlardan… şimdiyse çok farklı bir yerdeyiz. Hem halk hem de vatandaş olarak, artık aynı bilgileri görüp görmediğimizi ve başkalarının ne gördüğünü bilmiyoruz ve ortak bir bilgi tabanı olmadan, adım adım, toplumsal tartışma imkânsız hale geliyor, biz bunun sadece başlangıç aşamasındayız.

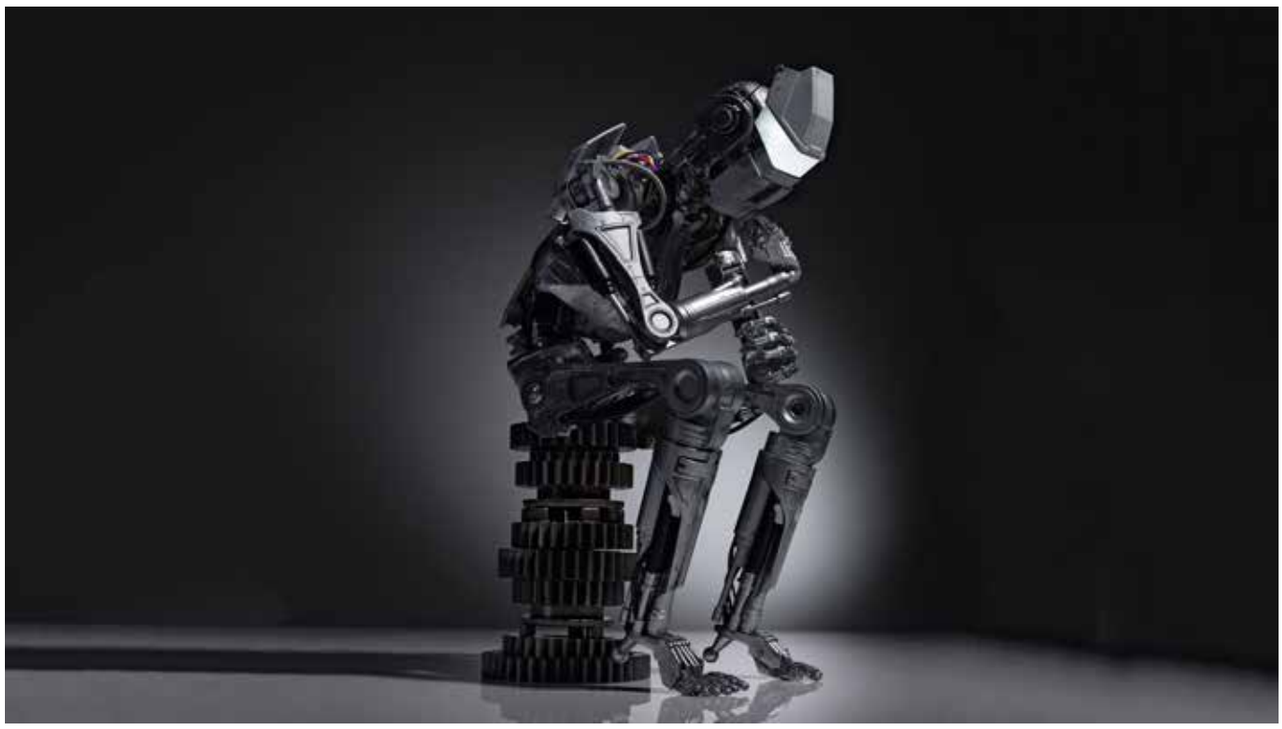
Bu algoritmalar kolaylıkla insanların etnik özelliklerini, dini ve siyasi görüşlerini, kişilik özelliklerini, zekâsını, mutluluğunu, madde kullanıp kullanmadığını, ailesinin durumunu, yaş ve cinsiyetini sadece Facebook beğenilerinden tahmin edebilir. Bu algoritmalar, yüzleri kısmen gizlenmiş olsa da protestocuların kimliğini belirleyebilir. Bu algoritmalar insanların cinsel yönelimini, flört uygulamalarında kullandığı profil fotoğraflarından anlayabilir.

Facebook'un piyasa değeri yarım trilyon dolara yaklaşıyor. Bunun sebebi ikna mimarisi olarak harika çalışıyor olması. Ancak bu mimari yapı ayakkabı satıyor olsanız da aynı siyaset satıyor olsanız da… Algoritmalar farkı anlamıyor. Reklamlara karşı bizi sabırlı kılmak için üzerimize salınan bu algoritmalar, aynı zamanda siyasi, kişisel ve sosyal bilgi akışımızı da düzenliyor ve bu değişmek zorunda.

Daha fazla bilgi için **http://quq.la/E9Vtk** adresini ziyaret edebilirsiniz.

YAPAY ZEKÂ, VERİ GÜVENLİĞİ VE GDPR

Günümüzde pek çok sektörde kullanılmaya başlanana yapay zekâ ve makine öğreniminin öne çıkan özellikleri arasında, verileri programatik araçlardan ve insandan çok daha hızlı analiz edebilmesi ve verilerin nasıl işleneceğini kendi kendine öğrenebiliyor olması bulunuyor.



Özellikle son yıllarda hem kamu hem de özel sektörde sıklıkla kullanılan profilleme ve otomatik karar verme sistemleri, artan verimlilik ve kaynakların korunması bakımından bireylere ve kurumlara çeşitli faydalar sunarken aynı zamanda riskleri de beraberinde getiriyor. Bu sistemlerin aldığı kararlar bireyleri etkileyebiliyor ve karmaşık yapısı dolayısıyla kararlarının gerekçesini izlemek mümkün olamayabiliyor. Örneğin, yapay zekâ, bir kullanıcıyı belirli bir kategoriye kilitleyip, önerilen tercihlere göre kısıtlayabiliyor. Bu, dolayısıyla onların kitap, müzik veya haber yazısı gibi belirli ürün ve hizmetleri seçme özgürlüklerini de daraltabiliyor. (Article 29 Data Protection Working Party, WP251, sf.5)

Mayıs ayında Avrupa'da yürürlüğe girecek olan GDPR, profilleme ve otomatik karar vermenin bireylerin hakları üzerinde olumsuz bir etki doğuracak şekilde kullanılmaması için çeşitli hükümler barındırıyor. GDPR, profillemeyi madde 4'te şöyle tanımlıyor: "Profilleme, belirli bir şahısla ilgili onun kişisel yönlerini değerlendirmek için kişisel verilerinin kullanılması; özellikle bu kişinin işteki performansı, ekonomik durumu, sağlık bilgileri, ilgi alanları, güvenilirlik, davranış, konum veya hareketlerinin analiz edilmesi veya tahmin edilmesidir." (WP251, sf.6) Profilleme, çeşitli kaynaklardan bireylerle ilgili elde edilen verilerin kullanılarak, kişilerle ilgili tahminlerde bulunmada kullanılır. Bu açıdan, yaş, cinsiyet, kilo gibi özelliklere dayanarak bireylerin değerlendirilmesi ya da sınıflandırılması olarak da düşünülebilir.

Otomatik karar verme ise insan müdahalesi olmaksızın teknolojik araçlarla (yapay zekâ gibi) karar verme özelliğidir. Otomatik karar verme herhangi bir veri türüne dayanabilir. Örneğin, kişiler tarafından doğrudan sağlanan veriler (ankete verilen cevaplar); kişilerden sağlanan veriler (uygulama aracılığıyla konum verisinin toplanması); önceden oluşturulmuş, türetme ya da sonuç çıkarmaya dayalı bireyin profili.

Potansiyel bir profilleme için ise üç yol vardır:

1. Genel profilleme,

2. Karar verme temelli profilleme,

3. Yalnızca otomatik karar verme içeren profilleme (madde 22)

2 ve 3 arasındaki fark, 2'de tamamen otomatik araçlarla üretilen bir profile dayalı insan kararı vardır. 3'te ise kararı algoritma verir ve karar anlamlı insan girdisi olmaksızın bireye otomatik olarak teslim edilir. (WP251, sf.8)

Burada karşılaşılacak önemli sorular ise şunlardır:

• Algoritma bu verilere nasıl erişiyor?

• Verinin kaynağı doğru mu?

• Algoritmanın verdiği karar, kişi üzerinde yasal etkiler doğuruyor mu?

• Bireyler otomatik işlemeye dayalı verilen karar karşısında birtakım haklara sahip olabilir mi?

• Veri sorumluları bu durumda ne gibi önlemler almak zorunda?

Günümüzde çoğu şirket müşterilerinin davranışlarını onlardan topladıkları verilerle analiz edebiliyor. Örneğin, bir sigorta şirketi, sürücünün sürüş davranışlarını izleyerek sigorta primlerini otomatik karar verme yoluyla belirleyebilir. Bunun yanında özellikle reklam ve pazarlama uygulamalarında farklı kişilerin verilerinden yola çıkarak yapılan profilleme ve otomatik karar verme sistemleri, diğer bireyler üzerinde de etkili sonuçlar doğurabiliyor. Varsayımsal olarak, bir kredi kartı şirketi, bir müşterinin kart limitini, kendi ödeme geçmişine dayanmadan aynı bölgede yaşayan ve aynı mağazadan alışveriş yapan diğer müşterileri analiz ederek azaltabilir. Dolayısıyla bu, başkalarının eylemlerine dayalı olarak, bir fırsattan mahrum kalma anlamına gelir.

HATALARIN HESABI VERİ SORUMLUSUNDAN SORULACAK

Bu nokta dikkat edilmesi gereken husus, toplanan veya paylaşılan verilerdeki hatalar ya da önyargılar otomatik karar verme sürecinde yanlış sınıflandırmalara ve kesin olmayan sonuçlara dayalı değerlendirmelere neden olup bireyler açısından olumsuz etkiler doğurabilmesidir. Kararlar güncel olmayan verilere dayanabilir ya da dışarıdan alınan veriler sistem tarafından yanlış yorumlanabilir. Yani otomatik karar vermede kullanılan veri doğru değilse bu durumda sonuçtaki karar ya da profilleme de doğru olmayacaktır.

Yapay zekâ ve makine öğrenmesinin kullanıldığı bu gibi sistemlerde oluşabilecek benzeri muhtemel hatalar karşısında "veri sorumlusunun" birtakım yükümlülükleri doğacaktır. Veri sorumlusu, kullanılan ya da dolaylı olarak elde edilen verilerin doğru ve güncel olması için yeterli önlemleri almalıdır. Ayrıca verilerin saklanma süreleri de doğruluk ve güncelliğin sağlanması için sakıncalar yaratabileceği gibi, orantılılık ilkesi ile de çelişeceğinden uzun süreli veri saklanması konusunda da veri sorumlusu gerekli adımları atmalıdır.

Diğer önemli husus ise özel nitelikli kişisel verilerin bu sistemlerce işlenip kullanılmasıdır. GDPR, özel nitelikli kişisel verilerin işlenmesinde ilgili kişinin açık rızasını aramaktadır. Ancak, bu durumda veri sorumlusunun unutmaması gereken şey, profillemenin özel nitelikli kişisel veri olmayan verilerin birleşimi ile özel nitelikli kişisel veri oluşturabilir olmasıdır. Örneğin, bir kişinin sağlık durumu, gıda alışverişi kayıtlarından, gıdaların kalite ve enerji içeriği ile ilgili verilerinden elde edilmesi ile mümkün olabilir. (WP251, sf.22)

GDPR, verileri kullanılarak otomatik karar verme işlemlerinden etkilenen kişilerin bu durum karşısında bazı hakları olduğundan da bahseder. GDPR'ın temelini oluşturan şeffaflık ilkesi göz önüne alındığında, madde 13 ve 14'e göre, veri sorumlusu bireylere açık bir şekilde profilleme veya otomatik karar verme sürecinin nasıl işlediğini açıklamalıdır.

Profilleme, hata riskini artıran bir tahmin unsuru içerebilir. Girdi verileri yanlış veya alakasız olabilir ya da bağlam dışı kalabilir. Bireyler kullanılan verilerin ve gruplandırmanın doğruluğunu sorgulamak isteyebilir. Bu noktada, madde 16'ya göre, ilgili kişinin düzeltme hakkı da söz konusu olacaktır.

Benzer şekilde, madde 17'de belirtilen silme hakkı da bu çerçevede ilgili kişi tarafından talep edilebilir. Profillemenin temeli için rıza gösterilirse ve bu rıza sonradan geri çekilirse veri sorumlusu profilleme için başka yasal dayanak olmadığı sürece ilgili kişinin kişisel verilerini silmek zorundadır.

ÇOCUKLARIN KİŞİSEL VERİLERİNİN ÖNEMİ

Profilleme ve otomatik karar vermede dikkat edilmesi gereken bir başka nokta ise çocukların kişisel verilerinin kullanılmasıdır. Çocuklar özellikle çevrimiçi ortamlarda daha duyarlı olabilir ve daha kolay etkilenebilir. Örneğin, çevrimiçi oyunlarda profilleme, algoritmanın daha fazla kişiselleştirilmiş reklam sunmasının yanı sıra, oyunda para harcamasının daha olası olduğunu düşündüğü oyuncuları hedeflemesi için de kullanılabilir. GDPR madde 22'de işlemenin çocuklar ve yetişkinler ile ilgili olup olmadığı konusunda ayrım yapmıyor. Ancak yine de çocuklar bu tür pazarlama çalışmalarından kolayca etkilenebileceği için, veri sorumlusu, çocuklar için uygun önlemleri almalı ve bu önemlerin çocukların haklarını, özgürlüklerini ve meşru çıkarlarını korumada etkili olduğundan emin olmalıdır.

Sonuç olarak, yapay zekâ ve makine öğrenimi gibi sistemlere dayanarak yapılan profilleme ve otomatik karar verme, birey hakkında önemli sonuçlar doğurabilir. Bu teknolojiyle bağlantılı olarak toplanan verilerin, kişilerin rızası alınarak toplanması ya da yasal bir zemine oturtulması gerekir. Akabinde kullanılacak olan bu verilerin toplandıkları amaçla bağlantılı olarak kullanılması da önemlidir. Sistemin aniden alışılmadık kararlar almaya başlaması halinde ne gibi yol haritaları izleneceği de dâhil olmak üzere, veri sorumlusu gereken önlemleri almalı ve ilgili kişilerin hak ve özgürlüklerini de gözetmelidir.

Daha fazla bilgi için **http://quq.la/bqc7j** adresini ziyaret edebilirsiniz.

Bilal Eren
Marmara Üniversitesi

FACEBOOK KRİZİ ANALİZİ

Sadece 68 defa "Beğen" butonuna basmış herhangi bir Facebook kullanıcısının hangi partiye oy vereceğini %85 doğrulukla bulabiliriz.

Modern sosyal mühendislik "Cambridge Analytica" skandalını, çıkan sonuçlarını ve bizlerin yapabileceklerini Twitter üzerinde bir zincir ile paylaşmıştım. Bu paylaşımlar yaklaşık 45 milyon Facebook kullanıcısının olduğu ülkemizde toplumun her katmanından ve kesiminden büyük ilgi gördü. Şimdi bu zinciri yazı şekline getirmek, eksikleri gidermek ve derli toplu sizlere sunmak istedim.

Skandala konu olan Cambridge Analytica; tüketici, takipçi, seçmen davranışlarını değiştirmek isteyen iş dünyası ve siyasi partilere hizmet sunmayı amaçladığını ilan ederek 2013 yılında Londra'da kurulmuş. Şirket, verilerimizi davranış bilimlerini kullanarak analiz edip kurumların (şirket, parti, devlet, STK vb.) hedef kişi ve kitlelerini belirlemeye/bulmaya yardımcı olacağını ilan etmiş. Şirketin ilan etmediği ancak bir gizli kamera kaydında açıkladığı çalışma şeklinde ise,

"Bilgiyi internetin dolaşım sistemine bırakıp, arasıra küçük müdahalelerle olayın büyüyüp yayılmasını izleriz. Kimsenin propaganda olduğunu düşünmemesi önemli. Çünkü propaganda diye düşündüğünüz anda bir sonraki soru; arkasında kim var?"

YAVAŞ YAVAŞ KAHRAMANLARIMIZI TANIYALIM.

Cambridge Analytica şirketinin kurucusu Alexander Nix, bir finansal analist uzmanı. 25 yıldır hükümetler ve askeri kurumlar için bilgi, analiz ve strateji elde eden bir şirket olarak kendini tanıtan SCL Group bünyesindeki SCL Elections (SCL grubunun seçimler ile ilgili şirketi) isimli şirkette 2003 yılında CEO olarak çalışmaya başlıyor. Önemli bilgi, SCL Group şirketinin Türkiye ofisi de var.

Skandala konu olan Cambridge Analytica ise 2014 yılında SCL Group bünyesinde kuruluyor. Alexander Nix o yılları şöyle anlatıyor:

"ABD'de Demokratlar teknoloji devrimine öncülük ediyorlardı. Veri analizi ve dijital dünya Cumhuriyetçilerin rekabette zayıf oldukları alanlardı. Biz de bunu fırsat olarak gördük."

Şirket, bu fırsatları sadece müdahale ettikleri ifşa ile kesinleşen 2016 yılı haziran ayındaki ABD'de Trump'ın başkan olduğu başkanlık seçimi ve aynı yılın kasım ayındaki İngiltere'nin AB'den ayrıldığı Brexit referandumu kampanyalarında mı gördü, bilinmez! İddialar hatta soruşturmalar Nijerya, Kenya, Çekya, Hindistan ve Arjantin'a kadar uzanıyor.

Ayrıca hem o yıllarda da hem de günümüzde bu alanda çalışan birçok şirket olduğunu biliyoruz.

Ve Cambrigde Analytica, vadettiği plana göre hedeflenen kişiler ve kitleler için özel içerik üretmeye başlar. Hedef kitleler ve kişiler yani "kime seslendiğin" her alanda insanlık için hep önemli olmuştur/olmalıdır. İnternet ve üstündeki teknolojiler ise sesleneceğin doğru kişiyi bulmak için şimdiye kadar insanoğlunun bulduğu en iyi araç.

PEKİ, NEYİ/NASIL YAPMIŞLAR?

İki çalışma önlerini açmış.

Birincisi; 2008 yılında Cambridge Üniversitesi Psikometri Merkezi'nden davranışbilimci iki doktora öğrencisi (Kosinski ve Stillwell) "Büyük Beşli"adlı seksenli yıllardan kalma davranış teorisi üzerinde çalışmaya başlamış. Nedir bu teori:

Bireylerin her davranışının kişiliklerindeki 5 yapıtaşı (yeniliklere açıklık, mükemmeliyetçilik, sosyallik, uzlaşmacılık ve kırılganlık) üzerinden çözümlenebileceğini savunuyor.

Teoriyi test etmek ve sonuçlar bulmak için kendi geliştirdikleri "MyPersonality" adlı bir Facebook uygulaması yapmışlar. Facebook kullanıcılarına kişisel basit sorular soran bu kişilik testi uygulaması üzerinden gönüllü denekler ile çalışmaya başlamışlar.Bu noktada aklımıza "Nasıl oluyor da Facebook, bu test ve uygulamalara izin veriyor?" sorusu gelebilir; 2010 yılında Facebook daha fazla kullanıcıya ulaşmak, para kazanmak vb. için "bizi" uygulama geliştiricilerine (STK, akademisyen, analiz şirketleri, yazılımcılar vb.) satıyor; "Dükkan sizin, Facebook daha çok kullanılsın, daha çok çevrimiçi olunsun. Bir şeyler yapın gibi."

Facebook hesaplarımızda bulunan her türlü bilgimizin bu uygulama geliştiricilere sonuna kadar açık olduğu yıllarda iki bine yakın proje için bilgilerimiz kullanılıyor. Hatta; diyelim ki siz bu uygulamalardan kullanmadınız, izin vermediniz ama Facebook arkadaşınız kullandı, izin verdi. Geçmiş olsun.

VE ABD BAŞKANLIK SEÇİMİ: HAZİRAN 2016

Cambridge Analytica ekibi Trump'ın seçim ekibi ile çalışıp kendi ifadeleriyle; "Milyonlarca veriyi analiz ettik. En çok ikna edilebilecek seçmeni tespit edip, ilgilendikleri meseleleri belirledik ve 'kişiyi hedef alan' mesajlarla harekete geçirdik."

ÖRNEKLERLE ANLAYALIM

Trump'ı tüm konuşma ve mesajlarını ellerindeki veri setleriyle insanların kişilik, davranış ve ihtiyaçlarına göre hazırladılar.

Politik mesajları test ettiler. "İslam'ın bu ülkede yeri yok" gibi radikal bir söylemi haberleştirip, profil tepkilerine baktılar.

Etkili yalanlar üretip, yaydılar. "Göçmenlerin ülkemize maliyeti askeri harcamalarımızın üstünde.." gibi.

17 eyalette her gün Facebook üzerinde ellerindeki profillerin kişiliğine göre şekillendirilerek sadece o kişiye gösterilen Trump yanlısı paylaşımlar ve anketler yaptılar. Bazen anketleri dolduranlara para bile verdiler.

Trump'a asla oy vermeyecek Miami'deki siyahlara, onları sandığa gitmekten alıkoyacak haberleri (örneğin: Clinton aleyhinde) gösterdiler. Bu sayede seçime katılımı bölgede %7–8 etkilediler.

Trump'ın konuşmalarından parçaları tarafların beklentilerine uyacak şekilde bir kısmını sağcılara bir kısmını liberallere vb. gösterdiler.

Ellerindeki verilere göre iki parti arasında kalan kararsızları tespit edip, onlara yoğunlaşan reklamlar yaptılar.

Aynı mahalledeki az eğitimli, fakir, aktif insanları belirlediler. Sonra bunlara hoşlanmayacakları haberleri verip, karşıt statüdeki insanlarla kavga ettirdiler vb.

Burada korkunç olan "bizim kim olduğumuzu" profillerimizden bilmeleri idi. Böylece haber ve reklamları doğru zamanda doğru seçmene göstererek, 2016 seçimlerinde Trump'ın önü açılmış oldu. (Kaynaklara göre 220 milyon ABD'liye ulaşmıştı bu operasyon)

Ve zafer. Trump'ın seçim kampanyasının dijital kısmını yöneten Theresa Hong: "85 milyon dolar harcadık. Facebook olmasaydı, seçimi kazanamazdık." dedi.

Tüm bu olup bitenler konuşuluyor, haber yapılıyordu. Ancak, Cambridge Analytica'dan Christopher Wylie'ın pişmanlık ifşası! ve İngiliz The Guardian gazetesinin haberiyle olay kesinleşti bir anlamda. Ne oldu da ifşa zamanı geldi şu an için bilinmiyor. Bir "propaganda makinesi" ürettiklerini söylüyor ve kendi ifadesiyle ne yaptıklarını basitçe anlatıyor;

PEKİ, TÜM BUNLAR OLURKEN FACEBOOK NE YAPTI?

Kogan'a profiller üzerinden araştırma yapmasına 2015 yılından beri izin verdiklerini söyleyen Facebook, "Bu çalışma ticari olmadığı için izin verdik. Sonuçta insanlar bilerek bilgilerini paylaştılar, herhangi bir sisteme girilmedi, şifreler ve hassas bilgiler çalınmadı veya hacklenmedi. Bu araştırma sonuçlarının Cambridge Analytica'ya verildiğini bilmiyorduk." şeklinde resmi bir açıklama yaptı.

Cambridge Analytica CEO'su Nix ise bir gizli kamera kaydında; "internette yaydıkları bilginin illa doğru olmak zorunda olmadığını duyguları harekete geçirmesinin yeterli olduğunu" söylemiş. Yani hem suçlu hem güçlü.

Facebook - Cambridge Analytica ilişkisi ise büyük boyutta duygusal!. Başka nedenler de var. Bu nedenleri başka bir yazıda değerlendirmek isterim.

Sonuçta "sosyal medya şirketleri" bize verdikleri hizmet ve servisleri bu yüzden bedava yapıyorlar. Yani Cambridge Analytica gibi onlarca firmaya satıyorlar. Birşey ücretsiz ise "ürün" biziz.

Diğerleri (Örneğin: Google) bunu, belki de daha fazlasını yapıyor. Hatta dünya üzerinde internetleri olmadıkları için "birşey arayamayan/beğenemeyen" insanlar için bile çözümleri var.

SKANDALIN SONUÇLARI NELER OLDU?

İngiltere/ABD'de soruşturma başlatıldı.

Şirket faaliyetleri şimdilik askıya alındı, CEO Nix görevden alındı.

Facebook şimdilik kaçamak açıklamalar yapıyor. Şirket içinde görevden almalar oldu, borsada ciddi değer kaybediyor.

Zuckerberg, "hatalar yaptık" dedi ve ekledi "şu ana kadar çok ciddi kullanıcı kaybetmedik"

Avrupa Parlamentosu Başkanı A. Tajani; ''Mark Zuckerberg'i Avrupa Parlamentosu'na davet ettik. Facebook'un, kişisel verilerin demokrasiyi manipüle etmek için kullanılmadığına, 500 milyon Avrupalının temsilcileri karşısında açıklık getirmesi gerekiyor." dedi.

AB Dijital Komisyonu: "Hedeflenmiş kitlelere yapılan seçim kampanyası seçmen manipülasyonudur, geçersizdir. Çünkü seçim kampanyasında vaat edilenler tüm kamuoyunu ilgilendirir." dedi. Brexit konusu ilginç olacak!

Özellikle ABD kamuoyu çok büyük tepkiler (haklı olarak) vermeye başladı. "Facebook'u silin, Facebook'a düzenleme" etiketleriyle paylaşımlar yapılıyor ve hesaplar siliniyor. Büyük bir sivil harekete dönüşebilir.

BU SKANDAL NEDEN BUGÜN ÇIKTI, BU NEYİN KAVGASI?

Trump/ABD/Rusya/İngiltere'nin Facebook üzerinden hesaplaşması olabilir mi?

İnternet teknolojisi ve özellikle Facebook yüzünden gelir kaybı yaşayan geleneksel medya devlerinin (Murdoch gibi) intikamı mı?

TRUMP KARŞITLARININ ABARTMASI MI?

Zamanla ortaya çıkar. Çok önemli değil bence. Bizleri ilgilendiren komplolar üzerine konuşmak veya "ne büyüksün big brother!" demek yerine "Bize etkileri ne? Şimdi ne yapmalıyız? Nasıl önlemler almalıyız?" olmalı. Birey/Toplum/Devlet olarak yapılması gerekenler var.

Doç. Dr. Bilgin Metin
Boğaziçi Üniversitesi

BOĞAZİÇİ ÜNİVERSİTESİ BÜSİBER'DE KİŞİSEL VERİLER PLATFORMU ÇALIŞMALARINA BAŞLADI

BÜSİBER (Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi) ve sektörün önde gelen hukuk bürolarından Özbek, Gün, Hergüner, Cerrahoğlu ve Turunç öncülüğünde Kişisel Veriler Platformu çalışmalarına devam ediyor.

BÜSİBER Yöneticisi Doç. Dr. Bilgin Metin ve Özbek Avukatlık Ortaklık'tan Av. Selin Özbek platform kuruluş amacını şu şekilde açıkladılar."Tüm Ülkemizi etkileyecek genişlikte bir kanun olan Kişisel Verilerin Korunması (KVK) Kanunu ve ikincil mevzuatının, uyum projeleri yürüten ve bu alanda fiilen çalışan avukat, akademisyen ve teknik kişilerin de dahil olduğu daha geniş katılımlı bir zeminde tartışılmasını sağlamak gerekmektedir. Bunun için herkesin tecrübe, bilgi ve fikrini paylaşabileceği aylık buluşmalar düzenliyoruz. Mart özellikli hukuki meseleleri konuşmak ve çözümler üretmek gerektiğini düşünüyoruz. Şu ana kadar 18 Ocak, 23 Şubat,16 Mart,29 Mart tarihlerinde toplandık. Bu toplantılarda tartışılanlar konuları ve varılan sonuçları, düzenli şekilde hem kamuoyu hem de Kişisel Verilerin Koruma Kurulu ile paylaşmayı ve mevzuatın hazırlanması ve uygulamanın daha sağlıklı gelişmesi için katkıda bulunmayı amaçlayan toplantılar için Boğaziçi Üniversitesi BSUYGAR Bünyesinde BÜSİBER altında bu platform kurulmuş faaliyetlere başlamıştır.

BÜSİBER BÜNYESİNDEKİ KVKK HİZMETLERİ

KVKK hukuk boyutu ve teknik boyutu eğitimleri

KVKK uyum süreci çalışmları

Sızma testleri(penetration test)

Yerli ve milli ürünler ile veri güvenliğinin sağlanması

KİŞİSEL VERİLERİN KORUNMASI KANUNU'NDA VERİ GÜVENLİĞİ

ZEYNEP BURCU DEVECEL-BUSİBER

TÜİK'in Hane halkı Bilişim Teknolojileri Kullanım Araştırması'na göre internet kullanımı oranının 2017 yılı itibariyle % 66,8 ye yükseldiği, Türkiye'de 10 haneden 8'inin internet erişim imkanına sahip olduğu belirlenmiştir.[1] Bilginin elektronik ortamda bu kadar çabuk yayıldığı ve işlendiği günümüzde kişisel verilerin korunması adına adımlar atılması kaçınılmaz olmuştur. Ülkemizde 4 Nisan 2016'da Resmi Gazete'de yayımlanan, 7 Ekim 2016 ile önemli bir çok hükmü yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu ile amaç, kişisel verilerin çağdaş standartlarda işlenmesi ve korunmasıdır. Kanun kapsamında kişisel verilerin korunmasına ilişkin genel hususlar, önem arz eden kavramlar, kişisel verilerin işlenme şartları , veri sahibinin hakları, kişisel verilerin silinmesi, yok edilmesi, anonimleştirilmesi, aktarılması ve veri sorumlusu gibi konular hakkında Kişisel Verileri Koruma Kurulu duyurular yapmakta, rehberler yayımlamaktadır.[2]

Kanuna uyumlu hale gelmek isteyen şirketlerin kanunun 12. maddesi birinci fırkasınca kişisel verilerin kanuna aykırı işlenmesi, bu verilere hukuka aykırı erişilmesini önlemek ve verilerin muhafazasını sağlamak amacıyla idari ve teknik olarak çeşitli tedbirler alınması gerekmektedir. Bu konuda veri sorumlusunun kişisel verileri belirlemesi, şirketin varlıkları olan kişisel verilere ilişkin ortaya çıkabilecek risklerin ve bu risklerin gerçekleşmesi durumunda verebileceği zararların belirlenmesi, buna bağlı olarak çeşitli tedbirler alınması çok önemlidir. Bilgi güvenliği yönetim sistemini doğru şekilde organizasyon kültürüne işlemiş bir kurumun bu konuda zorlanmayacağını söyleyebiliriz. Bir Bilgi Güvenliği Standardı olan ISO 27001'de uygulanması gereken bazı kontrollerin Kişisel Verileri Koruma Kurulu tarafından yayınlanan Kişisel Veri Güvenliği Rehberi'nde belirlenen kıstaslarla uyuştuğunu görüyoruz.[3]

ISO 27001'e göre bilgi güvenliği yönetim sistemi kapsamı dahilindeki bilginin gizlilik, bütünlük, erişilebilirlik kayıpları ile ilgili risklerin tespit edilebilmesi için bilgi güvenliği risk değerlendirme prosesinin uygulanması ve risk sahiplerinin belirlenmesi gerekmektedir. Risklerin gerçekçi bir analiz ve değerlendirme sürecinde geçmesi ve buna bağlı olarak bir bilgi güvenliği risk işleme sürecinin tanımlanması ve uygulanması beklenir. Kişisel verilerin de şirketin bir varlığı kabul edildiği bilgi güvenliği yönetim sistemini benimsemiş bir kuruluşun KVKK' da belirlenen bu süreci yaşadığını görüyoruz. KVKK Veri Güvenliği Rehberi'nde vurgulanan bir diğer husus çalışanlara bilgi güvenliği farkındalığı kazandırılmasıdır. Kişilere ait rol ve sorumlulukların tanımlanması, işe alınması süreçlerinde gizlilik anlaşmalarının imzalanması, çalışanların güvenlik politika ve prosedürlerine uymaması halinde uygulanacak bir disiplin sürecinin oluşturulması beklenmektedir. Bu politika ve prosedürlerin çalışanlara duyurulması ve değişiklik olması halinde güncel halinin çalışanlara bildirilmesi ayrıca beklenmektedir. Bu süreçlerin hepsini ISO 27001 kontrollerinde görüyoruz.[4]

Şu ana kadar bahsettiklerimiz işin idari boyutu ile alakalıydı. Teknik boyutta istenenlere bakacak olursak siber güvenliğin sağlanması adına güvenlik duvarı, ağ geçidi, antivirüs, antispam uygulamaları kuruluş için bir temel önlem olarak görülüyor. Kurumda kullanılan yazılımlarla alakalı olarak da yazılımların güncel ve güvenli olması, yama yönetiminin uygulanması, düzenli aralıklarla güvenlik açıklarının kontrol edilerek kapatılması gibi beklenmektedir. Şifre ve parolalarla alakalı bir politikanın belirlenmesi, erişim yetki ve kontrol matrisi ve erişim politikalarının oluşturulması ise bir diğer beklentiler arasındadır. Bilgi güvenliği yönetim sisteminde biliyoruz ki yazılanın yapılması, yapılanın yazılması çok önemlidir. Veri güvenliğinin sadece hukuki bir zorunluluk olarak görülmemesi, kurum kültürüne yerleşmesi gerek kurumun değerini koruyabilmesi, gerek veri sahiplerinin haklarının korunabilmesi adına büyük önem arz etmektedir.

Referanslar

[1] TUIK(2017) Türkiye İstatistik Kurumu. "Hanehalkı Bilişim Teknolojileri Kullanım Araştırması." http://www.tuik.gov.tr/PreTablo.do?alt_id=1028 1 Nisan 2018 tarihinde erişilmiştir.

[2] KVKK. (2016). "Kişisel Verilerin Korunması Kanunu". http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf 1 Nisan 2018 tarihinde erişilmiştir

[3] KVKK(2018). "Kişisel Veri Güvenliği Rehberi(Teknik ve İdari Tedbirler)", http://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf 1 Nisan 2018 tarihinde erişilmiştir

[4] International Organization for Standardization ISO. "ISO 27001Information Technology, Security Techniques, Information Security Management Systems", Requirements. Geneve, 2013.

İSMİNİ DUYMADIĞIMIZ TEKNOLOJİ KAHRAMANLARI

Teknoloji dünyası sadece Jobs, Gates veya Zuckerberg'den ibaret değil. İşte ismi pek bilinmese de çok önemli işlere imza atan 7 kahraman.

Facebook'un yaratıcısı Mark Zuckerberg tüm dikkatleri üzerine çekse de teknoloji dünyasında ismini pek duymadığımız başka sayısız kahraman var.

İnternet'ten alışveriş yapabilmeniz veya müzik satın alabilmemiz için saatlerce çalışıp pek az uyuyan bu teknoloji kahramanlarının adı, Steve Jobs'ın adının yanında pek az geçiyor. İşte adını duymadığımız ancak DNS'den kameralı telefonlara önemli teknolojik geliştirmelere imza atan isimler:

JORDON RİTTER, (NAPSTER'IN KURUCULARINDAN)

Medyanın ilgisini Sean Parker çok daha fazla çekse de dünyaca ünlü müzik paylaşım aracı Napster'ın ilk beş yayımındaki programlamayı Jordon Ritter yapmıştı. Oluşturduğu arka uç sistemi ve yük dengeleme özelliği, hizmeti veritabanına entegre etmesi, güvenliği ele alışı ve yöntemi, Napster'ın gelişmesinde anahtar rol oynamıştı. Napster en parlak döneminde 60 milyon kullanıcıya ve aynı anda çevrimiçi olan 2 milyon kullanıcıya sahipti.

TAHER ELGAMAL, (SSL'NİN MUCİDİ)

Taher Elgamal, 1995'de Netscape'deki takımına karmaşık bir hedefte liderlik ediyordu: e-ticaret'i güvenilir bir hale getirmek. Takımı bugün her tarayıcıda kullanılan SSL şifreleme standardını meydana getirdiler. Temel şifreleme standartlarını geliştiren takım, şifrelemeyi daha güçlü bir hale getirerek para aktarımlarında kullanılabilmesini sağladı. İşte bugün güvenle internetten alışveriş yapıp, para gönderebiliyorsak bu adam sayesinde...

Ancak Elgemal, en büyük katkısının SSL olduğunu düşünmüyor. 80'lerde Stanford'da öğrenci olduğu dönemlerde herkese açık-anahtar şifreleme algoritmalarını ortaya çıkaran Elgemal'ın algoritmaları, bugün hala kullanılıyor.

DAVİD BOHNETT, (GEOCİTİES'İN MUCİDİ)

Facebook ve MySpace ortaya çıkmadan önce, kullanıcıları belirli konularda birbirine bağlayan GeoCities adındaki hizmet vardı. Bohnett; GeoCities'i kişisel bir web sitesine sahip olmak, içerik oluşturma ve yönetme, ortak reklam gelirleri gibi bugün interneti meydana getiren fikirler ile kurmuştu. Konsept zamanla fotoğraf, müzik ve resimleri de içerecek şekilde gelişti, ancak GeoCities'in 'kullanıcı tarafından oluşturulan içerik modeli, o zaman için yepyeni bir şeydi ve henüz onu besleyecek yeterli altyapı mevcut değildi. Bugün ise sıkça rastlanan bir hal aldı.

PHİLİPPE KAHN (CEP KAMERASININ MUCİDİ)

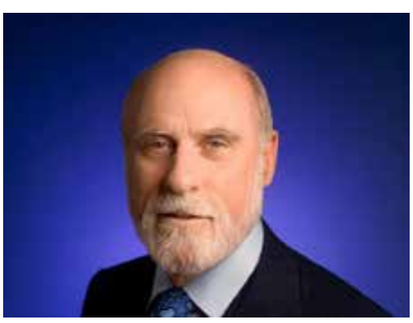
Kahn, 1997'de bir Motorola telefon, Casio kamera ve laptop'unu kullanarak ilk kameralı telefonu ortaya çıkarmıştı ve o gün tarihe şöyle not düşmüştü: "Evimde kamera telefonu yazılımının çekilen resimleri kablosuz olarak gönderdiği ve firewall'umun dışından erişim için URL'ler oluşturan bir web sunucusu kurdum." Diğer şirketler de kameralı telefon prototipleri oluşturduklarını söylüyorlar, ancak Kahn, ilk belgeli resmin kendisine ait olduğunu söylüyor. Kahn şu an GPS yazılımı ve cep telefonları için GPS uygulaması geliştiren FullPower'ın CEO'su.

PAUL MOCKAPETRİS, (DNS'İN MUCİDİ)

DNS'leri her gün, hemen hemen her internete girdiğinizde kullanıyorsunuz. DNS (Domain Name System), web tarayıcınızın internet adresleri için başvurduğu bir adres defteri gibidir. Paul Mockapetris 1983'de Güney Kaliforniya Üniversitesi Bilgi Bilimleri Enstitüsü'nde (ISI) DNS için birkaç teklifi değerlendiriyordu. Ve zamanla bugün kullandığımız teknolojiyi geliştirdi. İlk başlarda DNS hakkında yapılan eleştiriler, onun çok karmaşık olmasıydı. Ancak Mockapetris, beş yıl sonra aynı uzmanların DNS'de eksik olanlardan şikâyet etmeye başladıklarını söylüyor ve ekliyor: "İşte bu benim başarı tanımım."

Şimdi de sıra geldi 2 bonusa... Tüm bunların temelini oluşturan asıl iki mucide. Onlar olmasaydı belki şu an bugünkü icatların hiçbirini konuşmuyor olacaktık. Günümüzün dijital dünyasını borçlu olduğumuz yegâne iki insan, daha doğrusu üç insan...

VİNTON CERF (İNTERNETİN MUCİDİ)



Amerikan Savunma Bakanlığı ve bazı Amerikan Üniversiteleri tarafından başlatılan bir proje, günümüz sanal âleminin temelini oluşturuyor. Altmışlı yıllarda savunma bakanlığının isteği üzerine olası felaket senaryolarının (doğal afet, nükleer saldırı) ardından dahi işlevselliğini koruyabilecek bir iletişim sistemi yaratmak amacı ile başlatılan askeri bir projeydi ARPANET. 1960'larda başlayan bu proje 1970 yılında hayata geçti. ARPANET, başlangıçta sadece 15 bilgisayarın birbirine bağlı olduğu bir ağdan ibaretti ve özel kullanıcılara kapalıydı. 1970'li yıllar internet fikrinin hızla geliştiği yıllar oldu. Elektronik posta ortaya çıktı ve İngiltere Kraliçesi'nin 1976 yılında ilk e-postasını göndermesiyle internet fikri popüler hale gelmeye başladı.

Vinton Cerf, 1970'li yıllarda üniversiteyi yeni bitirmiş, yirmili yaşlarının sonunda bir matematik mühendisiydi. İnternet, o zamanlar askeri amaçla kullanılan bir sistemdi. Sivillerin kullanamadığı internet, kısa sürede 200 ayrı sivil kuruma yayıldı. Cerf interneti geliştiren bilim adamları arasındaydı. Ancak o daha önemli bir şey yaptı ve interneti karısının da kullanabileceği bugünkü haline getirdi. Eğer bunu yapmamış olsaydı internet denilen uçsuz bucaksız dünyada kimse istediği bilgiye ulaşamazdı. Cerf bugün, "Karım artık üniversitede okuyan oğlumuzla bile internet yoluyla konuşabiliyor. Kimbilir belki de interneti karımı mutlu edebilmek için icat etmişimdir" diye konuşuyor.

JOHN PRESPER ECKERT VE JOHN MAUCHLY

Esasen bilgisayarın mucidi konusu epey karmaşık bir mevzu olmakla birlikte net bir cevabı da yoktur. Tarihsel gelişimi icabı temeli abaküse kadar dayandırılır. Fakat burada günümüz modern bilgisayarlarının atası sayılabilecek dijital bilgisayarları temel alacağız.

İlk dijital bilgisayar konusu da biraz karışıktır. İlk dijital bilgisayar konusunda hemen hemen aynı dönemlerde farklı iki ekip piyasaya ürü sunmuştur. İlki Prof. John Vincent Atanasoff ve Cliff Berry tarafından 1942 yılında sunulan ABC (Atanasoff-Berry Computer) idi. İkincisi ise John Presper Eckert ve John Mauchly tarafından 1946 yılında sunulan ENIAC (Electronic Numerical Integrator And Computer) idi.

19 Ekim 1973'te ABD'li Federal Yargıçlar Earl R. Larson, John Presper Eckert ve John Mauchly'nin yaptıkları ENIAC'ın patentinin geçersiz olduğuna ve ilk dijital bilgisayarın mucidinin Atanasoff olduğuna hükmettiler. Fakat ABC'nin ilk dijital bilgisayar olduğu kararı olmasına rağmen günümüzde birçok uzman ENIAC'ın tamamen işlevsel olması nedeniyle ilk dijital bilgisayar olduğu düşünmektedir.

ENIAC'a kısaca değinmek gerekirse; 1941 yılında savaş sırasında yapım emri verilen, 1945'de şekillenen ve 1946 yılında basına tanıtılan ilk elektronik bilgisayar ENIAC, günümüzdeki bilgisayarların atasıdır.

ENIAC, ilk elektronik veri işleme kapasiteli ve elektrikle çalışan bilgisayardır. II. Dünya savaşı sırasında John Presper Eckert ve John Mauchly tarafından icat edilmiştir. 167 m2'lik bir alana ancak sığabilen ENIAC'ın ağırlığı da 30 tondu.