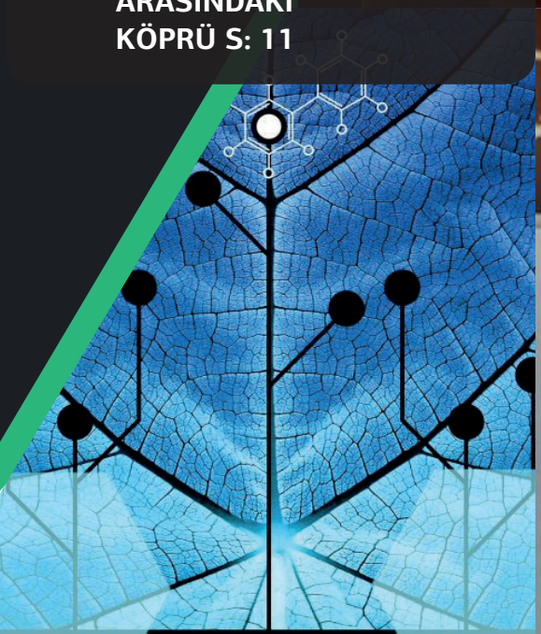
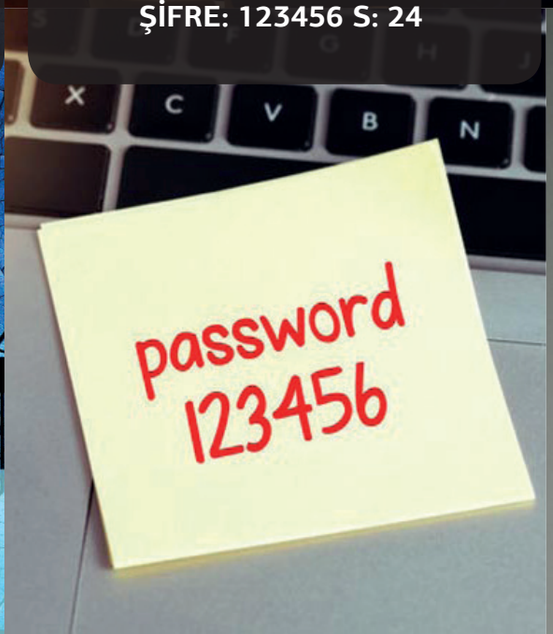
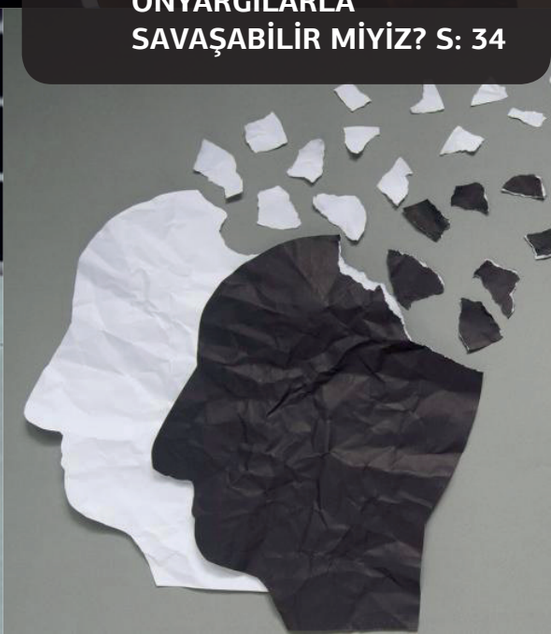
MARMARA
BELEDİYELER BİRLİĞİ

Bilgi Teknolojileri
Platform Bülteni

Ocak-Mart 2019 | Sayı 5







Editörden...

Öncelikle hepimize umut dolu, güzelliklerle dolu, mutlu, sağlıklı, keyifli ve bunun yanında sistemlerimizin saldırıya uğramadığı (hacklenmediği) tertemiz bir yıl dilerim 2019, hepimiz için iyilikler biriktirdiğimiz bir yıl olur umarım.

Dolu dolu bir bülten ile tekrar sizlerleyiz. Bilişim dünyasının gündemini aktarmaya çalıştığımız bu bültenlerde; günceli yansıtmanın yanında mümkün mertebe gelecek projeksiyonunu da çizerek sektörün yöneldiği yolu da okumaya çalışıyoruz.

Akıllı Şehir konsepti ilk konuşulmaya başladığı yıllarda, büyük oranda, teknoloji ile özdeşleşmişti. Sokaklara sensörler (Türk Dil Kurumu'nun önerisiyle, almaçlar) koymak, şehircilik işlerini olabildiğince otomatize etmek, her alana teknoloji sıkıştırmak vb... girişimler, akıllı şehir konseptinin baş aktörleriydi. Günümüzde ise bunun böyle olmadığı ve hatta tek bir "Akıllı Şehir" tanımının olamayacağı kabul görmüş durumda. Artık bu kavram belediyenin tüm birimlerini, paydaşlarını içine alan; şehir yönetiminin temel politikasını oluşturacak en önemli üst başlıklardan biri olarak tanımlanmakta. Hemen hemen atacağınız her adım, akıllı şehir politikanızdan referans almak durumda kalacak. Esasen ilerleyen yıllarda "Akıllı Şehir" söyleminin yok olacağını, her şehrin zaten akıllı olmak zorunda olduğunu, "akıllı" ifadesinin telaffuz edilmesi gerekmeyen doğal bir kavram olacağını da söylemek zor değil. Tıpkı 1990'ların sonuna doğru çıkan Multimedia PC kavramının şimdilerde yol olması gibi...

Kaçınılmaz bir öngörüyle, akıllı şehir kavramını takip etmemek, zamanında düştüğümüz "matbaa" hatasıyla aynı olacaktır. Akıllı şehirin bilişim (teknoloji) ayağı, biz BT çalışanlarını fazlasıyla ilgilendirmekte. Akıllı Belediyecilik Zirvesi'nde, bu alandaki günceli takip ediyor ve bunu sizlere ulaştırmaya çalışıyor; düzenlediğimiz çalıştaylarla da görüşlerinizi alıp, aktörü olduğumuz konularda sizleri dinliyoruz. Bunları da bir rapor haline getirip hem sizlerle hem de ilgili kuruluşlarla paylaşacağız. Bu yıl beşincisini düzenlediğimiz Akıllı Belediyecilik Zirvesi'nde aşağıdaki konuları konuştuk:

OTURUMLAR

1. Dijital Dönüşüm Çağında Akıllı Şehir Kurmak
2. Şehir Yönetiminde Siber Güvenlik ve Güncel Yaklaşımlar
3. Kişisel Verilerin Yönetiminde Sorumluluklar ve Riskler
4. Şehir için Yerli ve Milli Çözümler

ÇALIŞTAYLAR

1. Belediyelerde Milli Yazılım, Milli Donanım Göç Stratejileri / Sorunlar ve Çözümler
2. Akıllı Şehirler Eylem Planları Nasıl Olmalı?
3. Belediyecilikte Blok Zincir Teknolojisinin Kullanımına Dair Stratejik Yaklaşımlar

Marmara Belediyeler Birliği olarak, bilgi teknolojileri alanında günceli takip eden, geleceğe yön veren bu gibi etkinlikleri gerçekleştirmeye ve sizlere aktarmaya devam edeceğiz.

2019'un 12'de 1'ini geride bırakırken, yeni yılda bizleri nelerin beklediğini de, otoritelerin gözünden, sizlere aktarmak istedik. Bu bağlamda Serdar Kuzuloğlu'nun ve Gökhan Ahi'nin yazıları bizlere ışık tutacaktır. Daha uzak bir projeksiyon için "2050 Öngörüsü" yazısını okuyabilirsiniz. Milenyum öncesi fazlasıyla bilim kurgu kalan fakat şimdilerde daha gerçekçi bulduğumuz bir gelecek senaryosu...

Genelde her bültende es geçmediğimiz iki temel konu var. Birincisi, tabiki de, siber güvenlik. Hemen

hemen her konu siber güvenliğe bir şekilde temas etse de, özellikle Ocak ayında fazlasıyla kişinin ilgisini çeken #10YearChallenge etiketini veri güvenliği penceresinden ele alarak neyle karşı karşıya olabileceğimizin dikkatini çekmeye çalıştık. Siber saldırganların da odak noktasının kullanıcı verisi olduğu düşünülürse, tekrar söylemek gerekir ki, sosyal mecralardaki mahremiyetinize çok fazla dikkat edilmesi gerektiği, su götürmez bir hakikat. 773 milyon e-posta hesabının kırılmasıyla, internetin güvensizliği tekrar sorgulanırken, (kara bir tablo çizelim) buralar en vahşi ormandan bile daha vahşi tehlikeler barındırıyor.

Biraz da kara mizah sayılabilir ya da "güleriz ağlanacak halimize" mi demek lazım bilemiyorum ama ESET'in yayınladığı "Şampiyonluğu Kaptırmayan Şifre: 123456" yazısını da okumadan geçmeyin derim.

Her bültende vazgeçmediğimiz ikinci konu ise, Blockchain... Birden fazla sahibi olan veritabanlarında güvenliği sağlamanın şu an tek yolu gibi görünen Blockchain teknolojisinin mantığını, felsefesini, avantajlarını, dezavantajlarını her bültende paylaşmaya çalışıyoruz. Bu sayıda da Blockchain'i, belediyecilik ve çevresel etkileri açısından ele alırken; blockchain değişiminin ne demek olduğunu Adnan Veysel Ertemel'in yazısıyla ele aldık.

Yapay zekâ, dijital ikiz, teknoloji bağımlılığı gibi konuları da ele aldığımız bu sayımızda bence es geçmemeniz gereken yegâne yazı ise "Algoritmaları Kullanarak Önyargılarla Savaşabilir Miyiz?" oldu. Rumman Chowdhury ve Narendra Mulani, yazılarında "yapay zekâ, bizi objektif ve ideal sonuçlara götüren bilinmezlik perdesini sağlayabilir mi?" sorusuna yanıt arıyorlar.

En başta da söylediğim gibi, dopdolu bir bülten sizleri bekliyor. Yine de "bu da olsaydı güzel olurdu" diyeceğiniz ne varsa ya da katkı sağlamak istediğiniz her konuda bize önerilerinizi ve eleştirilerinizi btk@mbb.gov.tr e-posta adresine gönderebilirsiniz.

Bir sonraki bültende görüşmek dileğiyle...

Yunus Demiryürek
Marmara Belediyeler Birliği
Bilgi Teknolojileri Koordinatörü
yunus.demiryurek@marmara.gov.tr

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

Katkı Sağlayanlar
Kerem Ulusoy
İsmail Hakkı Polat
Melike Öztürk
Yusuf Kara
Ahmet Cihat Kahraman
Emrehan Furkan Düzgiden

Ocak - Mart 2019

Sayı 5

Bu sayıda...

AKILLI BELEDİYECİLİK ZİRVESİ 2018

Bu yıl beşincisi düzenlenen Akıllı Belediyecilik Zirvesi'nin açılış konuşması Marmara Belediyeler Birliği ve İstanbul Büyükşehir Belediye Başkanı Mevlüt Uysal tarafından gerçekleştirildi. Şehir yönetiminde siber güvenlik ve kişisel verilerin korunması hususlarının altını çizen Mevlüt Uysal, ulaşım sistemlerinde kamera uygulamaları, sinyalizasyon sistemleri, İstanbul Kart uygulaması ve akıllı şehir teknolojileri ile bu sistemlerin sürdürülebilirliği üzerinde durdu. Başkan Uysal, "Türkiye'nin sanayileşme ve belediyecilik açısından en gelişmiş bölgesi Marmara'dır. Bu bölgedeki belediyelerin, akıllı belediyecilik noktasında ortaya koyacakları vizyon ve stratejiler, diğer bölgelerdeki belediyelere örnek olması açısından önemli." dedi.

Zirvenin keynote konuşmasını yapan Eczacıbaşı Holding Yönetim Kurulu Başkan Yardımcısı ve Türkiye Bilişim Vakfı Başkanı Faruk Eczacıbaşı, "İnternetin hayatımıza girmesinin üzerinden 30 yıl geçti ve Türkiye nüfusunun yarısı 30 yaşının altında. Yapay zekâ, kripto paralar ve blockchain gibi uygulamalardan bahsettiğimiz dönem içerisinde savrulmanın önüne geçmeliyiz. Dünyanın her yerinde bilgi var. Biz bilgiyi kendi içimizde aradığımız zaman bilgiye ulaşabiliriz. Alışkanlıklarımızı değiştiren bozguncu yenilikler var. Dünya haber alma ve bilgiye gitme alışkanlıklarını değiştirdi. Telefonlarımızın arama fonksiyonu 5. sıraya düştü. Masalarımızın üzerindeki her şey artık telefonlarımızın içinde. Bozguncu yenilikler hesap edilebilse zaten yenilik olmazdı. 5 yıl öncesini düşündüğümüzde bugün geldiğimiz yeri tahmin edemezdik. Dünya fütüristlerin tahminlerinin çok ötesine geçti. Kendi zenginliklerimizi bugünün koşullarıyla birleştirmek, ileriye gitmek yolunda önemli bir adım. Her teknoloji kendi yöneticisi kadar akıllı. Veri için yeni petrol deniyor. Bu petrol doğru şekilde kullanıldığında bilgi haline gelir. Teknoloji ancak yardım edebilir. Bilginin paylaştıkça yükseldiğine, doğru bilginin elimizin altında olduğuna ve ancak emin ellerde ehil hale geleceğine inanıyoruz." dedi.

"Belediyeler, Akıllı Şehir 2.0 Teknolojileri için Yeni Bir Döneme Giriyor"

Akıllı Şehir 2.0 teknolojileri hakkında güncel bilgileri ve yapılan çalışmaları aktaran Novusens İnovasyon ve Girişimcilik Enstitüsü Kurucusu Berrin Benli konuşmasında "Akıllı Şehir 1.0 modelinden Akıllı Şehir 2.0 modeline geçildi. Akıllı Şehir 2.0 modelinde yerel yönetimlerin sahiplendiği ve teknolojinin araç olarak hizmetlerde kullanıldığı yeni bir sürüme geçiliyor. Akıllı şehir 3.0 kapsamında yerel halk ile birlikte interaktif oluşumlardan bahsediyoruz. Bugünlerde Akıllı Şehir 4.0'dan bahsediyoruz. Gelecekte 2.0 ve 3.0'ın harmanlanmış halini göreceğiz. Ar-

tık dünyada ülkeler değil şehirler hatta destinasyonlar yarışıyor. Bu destinasyonları teknoloji ile nasıl daha çekici hale getirebileceğimiz üzerinde durulmalı. Bir şehrin akıllı şehir olabilmesi için tüm paydaşlarının bir araya gelmesi gerekir." dedi.

İnovasyon ve teknolojinin şehir hayatında kullanılabileceği alanlardan bahseden Samsung JDM İş Geliştirme ve İş Ortaklıkları Avrupa Sorumlusu Yankı Yalçın, "Önce nesneleri akıllandırmaya başladık, sonra onları internete bağladık ve veriler topladık. Fakat o veriyi anlamlandırmak ve bilgiye dönüştürmek önemli." şeklinde konuştu.

Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Öğretim Üyesi Ahmet Onur Durahim, yapay zekâ ve büyük veri kavramlarını anlattı. Ahmet Onur Durahim "Yapay zekayı anlamak için öncelikle zekayı anlamak lazım. Zekâ bir amaç ve hedef doğrultusunda o hedefi yerine getirme yeteneği. Bunu başarırken en önemli nokta adaptasyonun sağlanabilmesi. Yapay zekada en önemli nokta ise adapte edilen sistemlerin geliştirilmesi." diyerek yapay zekanın önemine değindi.

Zirvenin Şehir Yönetiminde Siber Güvenlik ve Güncel Yaklaşımlar başlıklı 2. oturumunun keynote konuşması Alibaba Cloud/TradeFive Yönetim Kurulu Üyesi & CEO'su Orkan Aytulun tarafından gerçekleştirildi. İstanbul Üniversitesi Bilgisayar Mühendisliği Öğretim Görevlisi Mehmet Demir'in moderatörlüğünde gerçekleştirilen 2. oturumda Boğaziçi Üniversitesi BUSİBER Yöneticisi Bilgin Metin, TÜBİTAK BİLGEM Siber Enstitü Müdürü Mustafa Dayıoğlu, Yönetim Sistemleri Danışmanı Zühtü Kayalı, BTK Bilişim Uzmanı Onur Aktaş, , Beyaz Net Genel Müdürü Mehmet Fatih Zeyveli ve Küçükçekmece Belediyesi Bilgi İşlem Müdürü Çağdaş Mersinlioğlu yer aldı.

Boğaziçi Üniversitesi İnovasyon ve Rekabet Odaklı Kalkınma Çalışmaları Uygulama ve Araştırma Merkezi Müdürü Aslı Deniz Helvacıoğlu moderatörlüğünde başlayan 3. oturumda ise kişisel verilerin yönetiminde sorumluluklar ve riskler konusu Bağcılar Belediyesi Bilgi İşlem Müdürü Cüneyt Yılmaz, Eralp Danışmanlık ve Başkent Üniversitesi Misafir Öğr. Gör. Özgür Eralp, Digisecure Genel Müdürü İbrahim Saruhan, Kişisel Verileri Koruma Kurulu Uzmanı Cennet Alas Şekerbay ve E-Yönetişim ve E-Devlet Kıdemli Uzmanı Mustafa Afyonluoğlu tarafından ele alındı.

Yerli ve Milli Çözümler Konuşuldu

Zirvenin Şehir için Yerli ve Milli Çözümler başlıklı son oturumunda ise keynote konuşması Türk Elektronik Para A.Ş Genel Müdürü Serkan Aziz Oral tarafından gerçekleştirildi. Marmara Belediyeler Birliği Çevre Yönetimi Koordinatörü A. Cihat Kahraman moderatörlüğünde gerçekleştirilen oturumda Esenyurt Belediye Başkanı Ali Murat Altepe, Pendik Belediyesi Bilgi İşlem Müdürü Üstün Murat Yıldız, Boğaziçi Üniversitesi İnovasyon ve Rekabet Odaklı Kalkınma Çalışmaları Uygulama ve Araştırma Merkezi Müdürü Aslı Deniz Helvacıoğlu, Yörenet Teknoloji Yönetim Kurulu Başkanı Hakan Kalyoncu ve Profelis Bilişim-GIBUX Projesi Yöneticisi Türker Gülüm yer aldı.

Geleceğin şehirlerinin nasıl olması gerektiğinden yapay zekaya, nesnelerin interneti ve bulut teknolojilerinden siber güvenliğe, yerli ve milli inovasyondan blok zincir teknolojisine akıllı şehirleri şekillendiren unsurları gündemine alarak katılımcılara gerçekçi bir gelecek senaryosu çizen ABZ'nin ikinci gününde yerel yönetimler, akademi, STK'lar ve özel sektörden konularında uzman kişilerin katıldığı "Belediyelerde Milli Yazılım, Milli Donanım Göç Stratejileri / Sorunlar ve Çözümler", "Akıllı Şehir Eylem Planları Nasıl Olmalı?" ve "Belediyecilikte Blok Zincir Teknolojisinin Kullanımına Dair Stratejik Yaklaşımlar" çalıştayları düzenlendi. Çalıştaylarda çıkan sonuçlar raporlaştırılmak üzere kayıt altına alındı.

2019 HEM UMUT BAHARI HEM DE UMUTSUZLUK KIŞI

Yazan: Serdar Kuzuloğlu

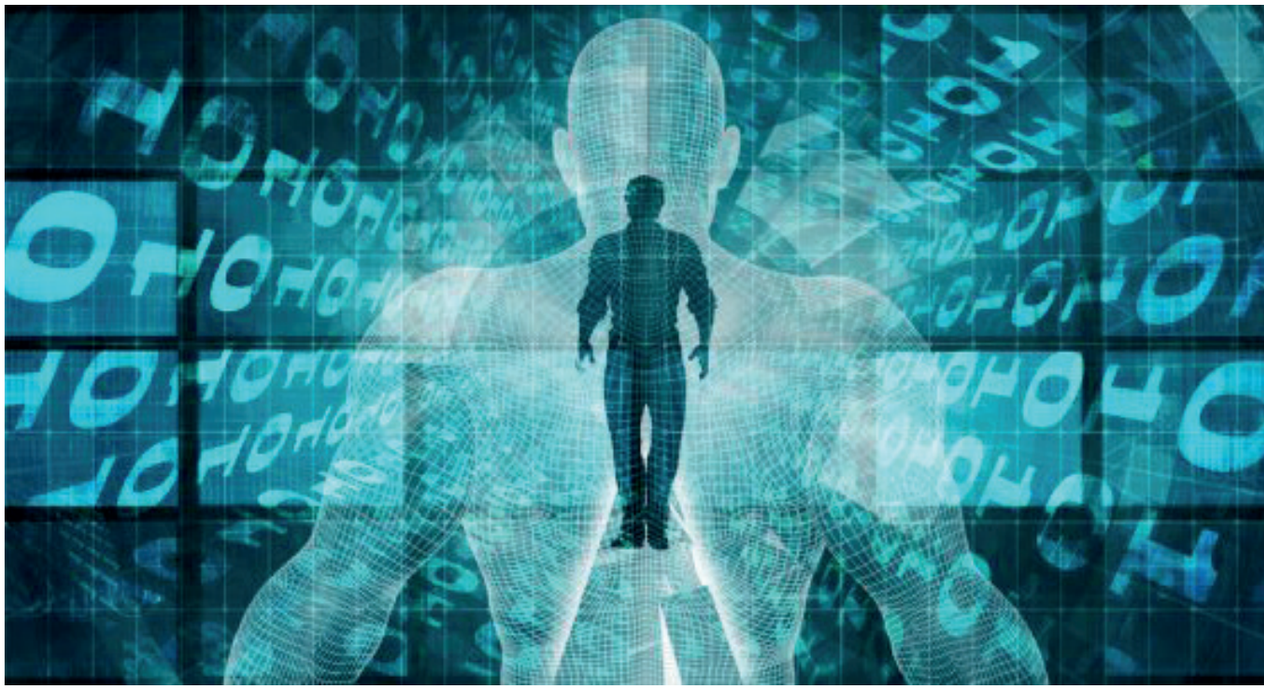
Müreffehlerin gündeminde Mars'ta kurulması planlanan koloni için Ay'ın öte yüzünde bir ara istasyon inşa etmek var. Biz ise -haklı olarak- yeni asgari ücretin zaten nefessiz kalan küçük işletmelerde tetikleyeceği işten çıkarma dalgasının endişesindeyiz. Ama öyle ya da böyle; işte bir yıl daha bitti. Hoşgeldin 2019. İnsanın çilesiyle yoğrulma sırası sende.

Zenginin malıyla yorulan çenelerin sadece bize has olduğunu sanmayın. Bu dünyanın en yaygın ortak paydalarından biri. Servet çetelesi tutan bu yüzden hayli fazla. Ama şüphesiz aralarında en çok ses getireni, bu işi -2018 itibarıyla- 32 yıldır sürdüren Forbes dergisi. Dünya genelinde devlet kayıtlarına geçen beyanlar doğrultusunda oluşturulan bu listenin zirvesi geçtiğimiz 24 yılın 18'inde Microsoft'un kurucusu Bill Gates'e aitti. Ancak Gates geçtiğimiz yıl Mart ayında tacını Amazon'un kurucusu Jeff Bezos'a devretti.

Bezos'un taç devralışı mütevazı bir tarzda da değildi üstelik. Zira hem kişisel serveti 100 milyar dolar sınırını aşan ilk işadamı oldu hem de bir yıl içinde servetine en çok servet katan kişi unvanını kazandı. Bu sizin için ne ifade eder bilemiyorum fakat hemen her ticaret erbabının rüyalarını süsleyecek bir tablo olduğuna kuşku yok.

10 Yıl Sonra Neyin Değişeceğine Değil; Neyin Değişmeyeceğine Odaklanmak

Patronların serveti beni çok heyecanlandırmıyor. Ancak onları rakipleri arasından sıyıran şeyler ile fena halde ilgiliyim. Amazon'un kurucusunun bir röportajında sarf ettiği bir cümle bu yüzden her zaman aklımın bir köşesinde: 'Ben 10 yıl sonra neyin değişeceğine değil; neyin değişmeyeceğine odaklanırım.'



Kulağa gayet makûl geliyor, değil mi? Binbir değişkenle, bilemediğimiz parametrelerle ve her an yeniden yazılan formüllerle ilerleyen hayat denkleminde değişimin izini sürmek kolay iş değil. Ancak nelerin değişmeyeceğini kestirmek -değişeceklere kıyasla- çok daha mümkün.

Örneğin hepimiz gayet iyi biliyoruz ki dün olduğu gibi yarın da müşteri, iş dünyasının her zaman en önemli besin kaynağı olmaya devam edecek. Ve tekrar etmekten içi boşalmış gibi duran "müşteri memnuniyeti" kavramı istisnasız her ürünün, hizmetin, ekibin ve şirketin kaderini belirleyen en temel unsur olarak kalacak.

Bugünün kapasitesini (arz potansiyelini) düşününce üretimi ihtiyaç ile denkleştirmenin imkansızlığı ortada. Yani bundan sonra da ihtiyacımızdan çok daha fazlasını üretmeye devam edeceğiz. Dolayısıyla onları ihtiyaç gibi gösterip satma çabası da son bulmayacak.

İsraf bu çağın en büyük gelir kalemi. Demek ki üretim, pazarlama ve satış sürecek. Peki şimdiye dek sürdüğü gibi mi? Asla!

Örneğin bugün milimetre ölçeğinde hata toleransıyla çalışmak zorunda olan tekstil sektörü imalatta optimizasyon (tasarruf diye de okuyabilirsiniz) adına neredeyse yeni bir bilim dalı yaratacak.

İnternet mecralarındaki pazarlama (reklam) altyapıları milisaniyeler içinde yüzlerce farklı kaynaktan veri çekerek, kişiye özel dinamik kampanyalar oluşturup ekrana yansıtıyor. Her bir reklam yine mikro zaman dilimleri içinde analiz edilip, alternatiflerle karşılaştırılıp yeniden iyileştirmeye tabi tutuluyor. Satış ise bugün geleneksel mecralarından taşıp 'omnichannel' kapsamında müşterinin var olduğu her an ve her yerde tezgâh açma derdinde. Üstelik her bir kanal (mecra) ayrı bir içerik, üslup; hatta bazen strateji istiyor.

Yine de Gözden Kaçan Bir Şeyler Var

Örneğin reklamcılık sürüyor ancak bütçe hemen her ülkede elektronik mecralara kayıyor. Doğası (ve vaadi) gereği her geçen gün şeffaflaşma ve verimlilik baskısı altındaki internet reklamı destekli satış ve pazarlama aktiviteleri ise insandan hızla soyutlanarak yerini algoritmalara bırakıyor.

Pazarlama ve reklamın ilgi ve yetki alanı Golan Tepeleri kadar ihtilaflı. Örneğin "fizikî" bir kitap dükkânının raflarında öncelikli yer almak için harcadığımız bütçeye "pazarlama", bir e-ticaret sitesinin sayfalarında öncelikli yer almak için harcadığımıza ise "reklam" diyoruz. Birinden birinde yanlışlık var. Ama hangisinde? Bir adım ötesinde akıllı hoparlörler ve chatbot'lar ile hayatımıza giren yapay zeka asistanları bizi giderek kendi tercihlerine (algoritmalarına) mecbur bırakıyor. Tüketimin kararında tüketici giderek daha az söz sahibi hale geliyor.

Geçen ayki yazımda değindiğim bir temayı da araya sıkıştırmak isterim: Şimdiye dek yazılım ağırlıklı ilerleyen dijital evren yüzünü donanıma döndükçe küreselliğini de kaybediyor.

Uber sadece Türkiye'de değil, birçok ülkede farklı sıkıntılarla boğuşuyor. ABD, Uzakdoğu ve Avrupa'nın şu dönemki en parlak furyası elektrikli scooter'ların Türkiye gündeminde yeri dahi yok. Amazon Batı'da, Alibaba Doğu'da perakende sektörünü zangır zangır sarsarak kuralları yeniden yazıyor ancak dünyanın geri kalan kısmına "endişeli modern" tavrı yeterli olabiliyor.

İbn-i Haldun'un meşhur "coğrafya kaderdir" tespitini internet ile yıkar gibi olmuştuk. Gel gelelim birçok devletin sınırına fiziki duvarlar ördüğü bu zamanda internet de ülkeler ve bölgeler bazında başkalaşmaya başladı. ABD Başkanı Donald Trump'ın popülist politikaları yüzünden hortlayan ticaret savaşlarının gölgesinde kalsa da Endüstri 4.0 çözümleri, fabrikaların Sanayi Devrimi'nden bu yana ilk defa Doğu'dan Batı'ya taşınmasını mümkün kıldı. Varlığını ucuz ve vasıfsız iş gücüyle fason imalata borçlu ülkeler için durum her geçen gün biraz daha zor, rekabet ise can yakar hale gelecek.

Şu Dönemin Ruhunu En İyi Anlatan Satırlar Charles Dickens'ın Kaleminden Çıkmış Gibi

Müreffehlerin gündeminde Mars'ta kurulması planlanan koloni için Ay'ın öte yüzünde bir ara istasyon inşa etmek var. Biz ise -haklı olarak- yeni asgari ücretin zaten nefessiz kalan küçük işletmelerde tetikleyeceği işten çıkarma dalgasının endişesindeyiz. Mart ayındaki yerel seçimler yüzünden baskılanan, ertelenen ekonomik kriz ihtimali herkesin korkulu rüyası.

İlginçtir ama şu dönemin ruhunu en iyi anlatan satırlar 1859'da İngiliz Yazar Charles Dickens'ın kaleminden çıkmış gibi. Fransız Devrimi'nin kaotik yıllarında geçen İki Şehrin Hikâyesi adlı eserinde Dickens şöyle diyor: "Zamanların en iyisiydi, zamanların en kötüsüydü. Hem akıl çağıydı hem aptallık. Hem inanç devriydi hem de kuşku, Aydınlık mevsimiydi. Karanlık mevsimiydi. Hem umut baharı hem de umutsuzluk kışıydı. Hem her şeyimiz vardı hem hiçbir şeyimiz yoktu. Hepimiz ya doğruca cennete gidecektik ya da tam öteki yana. Sözün kısası, şimdikine öylesine yakın bir dönemdi ki, kimi yaygaracı otoriteler bu dönemin iyi ya da kötü fark etmez; sadece 'daha' sözcüğü kullanılarak diğerleriyle karşılaştırılabileceğini iddia ederdi."

Araştırma şirketi Konda'nın Genel Müdürü Bekir Ağırdır, 'Bu yaşanan küresel kriz değil, çağ değişimidir' diyor. Sahiden de öyle galiba. Özetle, öyle ya da böyle; işte bir yıl daha bitti.

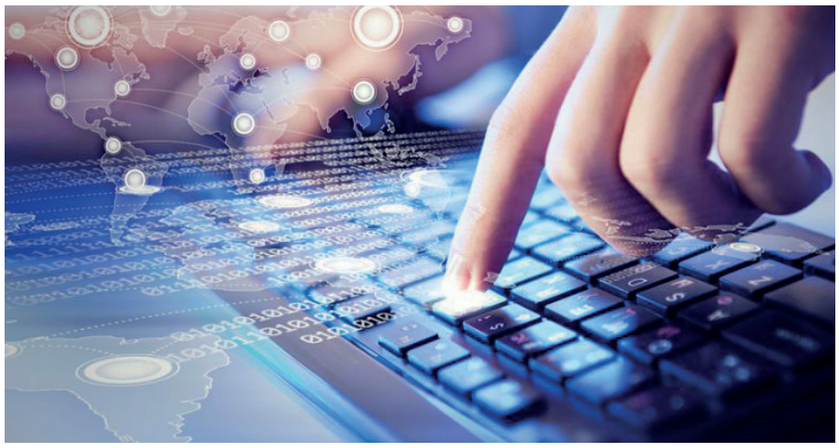
Hoşgeldin 2019. İnsanın çilesiyle yoğrulma sırası sende.

Kaynak: http://quq.la/b9i2x

TEKNOLOJİ VE İNTERNETİN EN PAHALI YILI

Yazan: Gökhan Ahi

2018'de özellikle teknoloji ile ilgili her şeyde döviz kaynaklı bir maliyet artışına şahit olduk. Görünen o ki 2019 teknoloji ve internet tüketicisi için pahalı bir yıl olacak.



2018, Türkiye ekonomisi için zor bir yıl oldu. Türk Lirası'nın yabancı paralar karşısında değer kaybetmesi, hammadde girişi ithalata dayalı olan sektörleri oldukça sarstı ve günün sonunda girdi maliyetlerinin artması, tüketici düzeyindeki fiyatların da artmasına sebep oldu. Teknoloji üretebilen bir ülke olmadığımızdan dolayı, özellikle teknoloji ile ilgili her şeyde döviz kaynaklı bir maliyet artışı kaçınılmaz oldu. Tüketici düzeyindeki fiyat artışları, sadece dövizin değer kazanmasından kaynaklanmadı, teknoloji temelli ürünlerde yapılan vergi artışları ve uygulama değişikliğinden de kaynaklandı.

Kullandığımız tüm yazılımlar ve platformların ücretleri güncellendi ve arttı. İşletim sistemi yazılımlarından ofis yazılımlarına, reklam yazılımlarından kaynak planlama yazılımlarına kadar tüm abonelik ve lisans bedelleri ciddi oranda arttı. Netflix, Google Drive, Apple iCloud, Spotify, Apple Music gibi tüm online platformlarda da fiyatlar yükseldi. Bilgisayar, akıllı telefon, çevre cihazları ve sarf malzemelerinden hiç bahsetmiyorum bile.

Tam E-Kitap İmdada Yetişecekti ki…

Her yerde ve her şekilde kullandığımız kâğıt dahi ithal edilen bir ürün, dolayısıyla basılı tüm gazeteler, kitaplar ve dergilerin fiyatı döviz kaynaklı arttı. Tam burada imdada e-kitap ve e-dergi yetişecekti, kâğıda, baskıya ve lojistiğe bağlı olmadan binlerce kopya çok düşük maliyetli olarak herkese ulaşabilecekti. Ancak burada da sevgili devletimiz, vergiyi artırmayı uygun gördü ve elektronik yayıncılık alanında KDV oranı yüzde 18'e geldi. 2016'dan beri internet erişiminde kademeli olarak kaldırılacağı bildirilen Adil Kullanım Noktası / Kotası, 1 Ocak'tan itibaren kaldırılmış olacak. Ancak, AKN olmadan verilecek bir internet aboneliği aslında gizli bir zam anlamına geliyor. 2019'da Turkcell'in yapmaya çalıştığı bir başka maliyetimiz daha olacak. Akıllı telefondan bilgisayarımıza veya tabletimize paylaştırdığımız internet (tethering) için de aylık 9 TL'lik bir fatura (şimdilik) bizi bekliyor olacak. Yılın son maliyet kalemi ise internet reklamlarından. Aralık ayında yapılan bir değişiklikle, vergi mükellefi olsun olmasın, internet ortamında reklam hizmeti veren veya aracılık eden tam veya dar mükellef gerçek kişiler ile dar mükellef kurumlara gerçekleştirilecek internet reklamı bedeli ödemelerinden yüzde 15 gelir vergisi stopajı yapılacak.

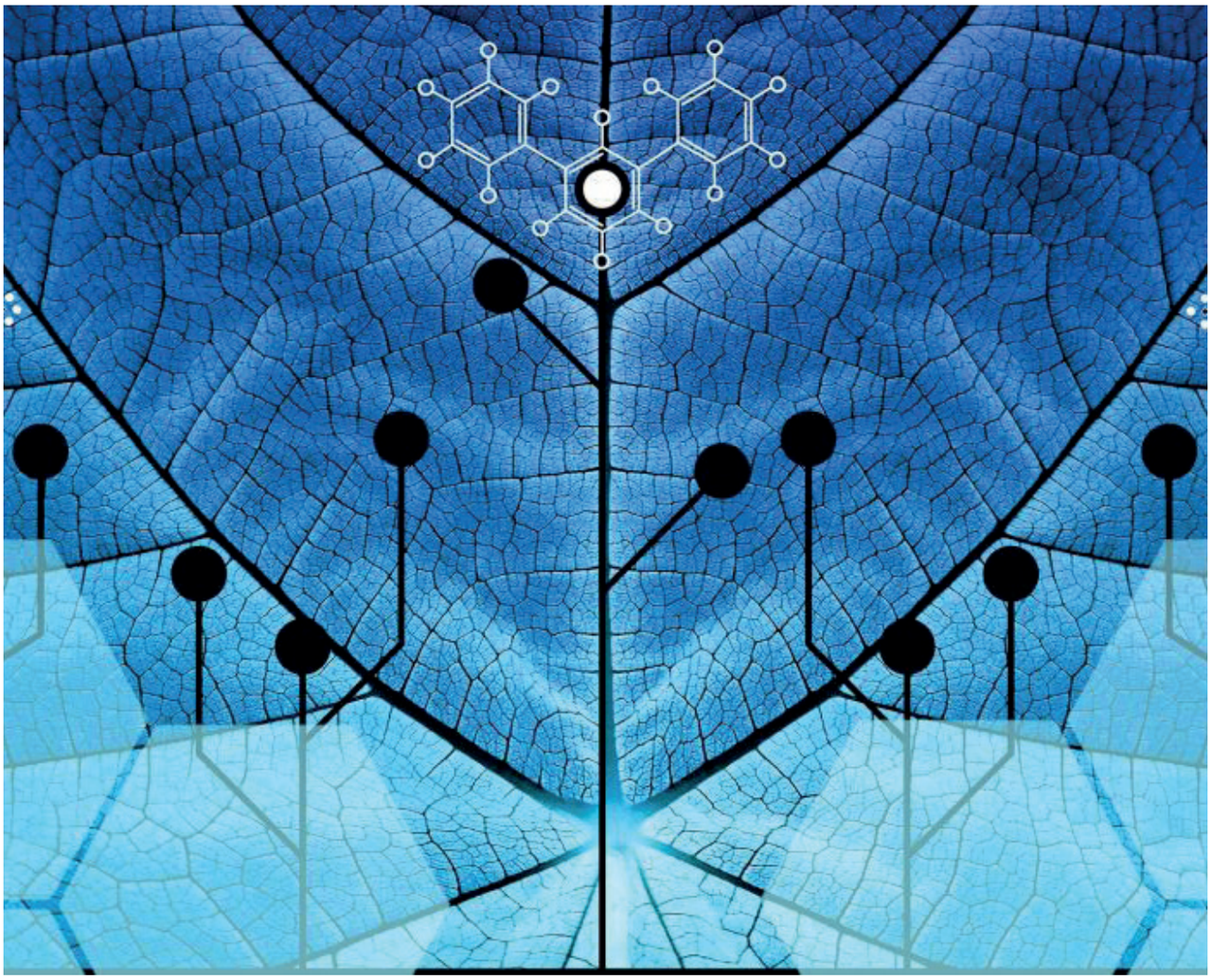
Teknoloji Tüketmeye Devam

Sonuç olarak, 2019 yılı teknoloji ve internet tüketicisi için pahalı bir yıl olacak. Her zaman söyleriz ya, Türkiye'nin teknoloji trenini kaçırma lüksü yok, bir şekilde teknoloji dünyasında üretim ile yer almamız gerekir diye. İnsanlar, okumak, öğrenmek, yazmak, paylaşmak, toplumu aydınlatmak, hayal kurmak, kendini geliştirmek, fikir geliştirmek, iş kurmak, üretim yapmak ve ilham almak istiyor. Bunlar için kullanılan cihazlar, yazılımlar ve internet bağlantısı artık lüks değil, zorunlu temel ihtiyaç. Ancak, daha ucuz erişilebilen, daha az vergi alınan, avantajlar yaratan, teşvikler sağlayan, adil rekabet ortamı yaratan bir sistem yerine, her adımda cebimizden para çıkan bir düzen inşa ediliyor. Ne diyelim, o halde teknoloji ve bilim üretmek yerine, tüketmeye ve vergi ödemeye devam!

Kaynak: http://quq.la/3jyrR

İNSAN VE YAPAY ZEKÂ ARASINDAKİ KÖPRÜ

Yazan: Gökhan Arıksoy



Günümüzün en popüler konularından biri olan yapay zekâ hakkında birçok kişi görüşlerini belirtiyor. Ben de bu kişilerden biriyim ve yapay zekâya pozitif yaklaşan tarafta yer alıyorum. Elbette yapay zekânın birçok şeyi temelden değiştireceği ve bildiğimiz konulara çok farklı şekillerde yaklaşmamızı gerektireceği artık su götürmez bir gerçek.

Yapay zekânın yaratacağı etkiler hakkında birçok şey yazmak mümkün. Fakat herkesin hemfikir olduğu bir nokta varsa o da yapay zekâ ile insanın birlikte çalışması gerektiği. İnsan ve makine arasında, birbiriyle mücadele eden değil, her iki tarafın da birbirinin varlığını desteklediği simbiyotik bir ilişkiden söz ediyoruz.

İnsanların ve makinelerin güçlü ve zayıf olduğu yönler de birbirinden farklı. Bilgisayarlar algoritmaları ve işlemleri bir insandan katbekat daha hızlı uygulayabiliyor. Hatta tüm bunları tekrar tekrar, yorulmadan ve hep aynı doğrulukta yapabiliyor. Gittikçe ileri bir seviyeye ulaşan mantık sistemleri, karmaşık meselelerin altından başarıyla kalkmalarını sağlıyor. Öte yandan biz insanlar da var olmayan bir şeyi gözümüzde canlandırabiliyor, yeni şeyler icat edebiliyor, şefkat ve

aşk gibi duyguları yaşayabiliyoruz. Sözün özü, insanlar ve makineler birbirinin rakibi değil, birbirini tamamlayan iki parça.

İnsan ve makine birlikteliğinin bir adı da var: Hibrit Zekâ. En basit şekilde hibrit zekâ, insana karşı makine değil, insan ile makine birlikteliği demek. Yani insan ve yapay zekânın birlikte çalıştığı hibrit zekâ, yaşam kalitemizin artmasını sağlayacak. Peki, bunu nasıl yapacak?

Bazı yükleri üstümüzden alarak. Yapay zekânın elimizden alacağı şey varsa o da el yoran ve düşünmeyi gerektirmeyen işler olacak. Bu sayede biz de yaratıcılık ve yorum yapmayı gerektiren işlerle uğraşarak çok daha yapıcı bir geleceğe yelken açmaya devam edeceğiz.

Fakat tüm ipleri bir anda yapay zekâya teslim etmek, herkesin hoşuna giden bir şey olmayabilir. Hibrit zekâ bu noktada yapay zekâyı benimseme sürecini en kolay hale getirecek köprü görevi de görüyor. Çünkü;

- Yapay zekâ ve insan zekâsının bir araya gelmesiyle ortada oluşan hibrit bir ortam var. Bu sayede yapay zekâyla kolay iletişim kurabiliyoruz,
- Risk az, kazanç fazla,
- Kontrol kullanıcının elinde,
- İnsan ile yapay zekâ arasındaki etkileşim ne kadar yoğun olursa, yapay zekâ beraber hareket ettiği insanın tercihlerini o kadar kolay tahmin edebiliyor. Başka bir deyişle daha faydalı bir yapı haline geliyor.

Aslında hibrit zekânın bize sağlayacağı faydaları görmek için çok beklememiz gerekmiyor. Örneğin Robotik Süreç Otomasyonu (RSO) alanındaki gelişmeler hem robot yazılımların tek başına çalıştığı hem de herkesin bilgisayarında bir robot yazılımın faaliyet gösterdiği iki yöntem üzerinden ilerliyor. Böylece bu yazılımlar, bir dosyadan başka bir dosyaya kopyalama ve yapıştırma gibi el yoran ve zaman kaybettiren işlerin yükünü kullanıcılarının omuzlarından alıyor.

Dünyanın çeşitli yerlerinde hibrit zekâ ile ilgili çalışmalar yapan firmalar mevcut. Bu şirketlerin çalışma modellerinin her aşamasında insan yer alıyor. Arka planda ise derin öğrenme ve doğal dil işleme teknolojileriyle daha zekileşen yapay zekâ yer alıyor.

2011'de kurulan Estimize ve 2015'te kurulan Cindicator, hibrit zekâ modelini kullanan şirketler arasında başarılı örnekler olarak yer alıyorlar. Estimize, profesyonel finans uzmanlarının öngörülerini yapay zekâ sisteminden geçirerek bir analiz ortaya çıkarıyor. Bu analizlerin başarı oranı, Wall Street'te bugün sıklıkla kullanılan tahmin sistemlerinden yüzde 74 daha başarılı. Cindicator ise bir seviye daha üste çıkarak tüm dünyadan rastgele isimler belirleyerek onların öngörüleri üzerinden analiz oluşturuyor.

Yapay zekâ hakkında uyarılarda bulunan Elon Musk, Temmuz 2016'da kurduğu Neuralink şirketiyle işlemsel cihazları insan zihnine bağlayacak teknolojiyi geliştiriyor. Bu şirketin amacı, ikili arasındaki ilişkinin konuşmadan çok daha hızlı olan düşünmeyle gerçekleşmesini sağlamak. Eğer bu teknoloji gerçek olursa zihinsel becerilerimiz eşi benzeri olmayan seviyelere ulaşabilir.

20 yıl önce IBM'in Deep Blue isimli robotuyla satranç tahtasında kozlarını paylaşan eski satranç dünya şampiyonu Garry Kasparov, "Yapay zekâ bizim daha insan olmamızı sağlayacak" diyor. Hibrit zekâ şu anki durumunda hala geliştirilmesi gereken bir teknoloji. Aynı zamanda biz insanlara muhteşem faydalar sunacak yapay zekayı hayatımıza en kolay entegre edecek yöntem.

Kaynak: http://quq.la/m4kbx

#10YEARCHALLENGE ÇILGINLIĞI VERİ TOPLUYOR

Sosyal medyayı kullanıyorsanız, Facebook, Instagram veya Twitter'da 10 Year Challenge isimli etikete denk gelmişsinizdir. İnsanlar 10 sene önceki ve sonraki fotoğraflarını, bu etiketle paylaşıyor. Tam bir çılgınlık yaşanıyor. Ancak Wired sitesinin editörlerinden Kate O'Neill bu duruma farklı bir açıdan yaklaştı ve ortada geniş ölçüde yüz tanımlama ve kişisel veri senaryosu olduğunu vurguladı.

İşte Kate O'Neill'ın dikkat çekici yazısı:

"İnsanlar eski ve yeni fotoğraflarını paylaşıyor. Bu konuda Tweet mesajı attım ve bu tweet etkileşim aldı. Ancak yüz tanıma senaryosunun geniş ölçüde mantıklı olduğunu ve insanların bilmesi gereken bir eğilim oluştuğunu da biliyordum. Paylaşılan kişisel verilerin derinliğini ve genişliğini dikkate almaya değer bir durum.

Teorimi eleştirenlerin çoğu, fotoğrafların zaten mevcut olduğunu savunuyor. Tezimi çürütmek için "Bu veriler zaten mevcut. Facebook tüm profil fotoğraflarını almış" durumda deniliyor. Sosyal medyayı kasıp kavuran 10 Year Challenge'ta ilk profil fotoğrafı veya resmi yanında, 10 yıl sonraki halinin de konulması gerektiği söyleniyor. Evet, bu profil resimleri var. Çoğu kişinin resmi de açık durumda, ancak işin farklı bir yönü daha var. Bunu biraz daha açmak istiyorum.

Yaşa bağlı özelliklere, yaş ilerlemesine veya başka nedenlere göre (Mesela insanların yaşlandıkça nasıl görüneceği olasılıklarını içeren) bir yüz tanıma algoritması geliştirmek istediğinizi düşünün. İdeal olarak birçok insanın fotoğrafının bulunduğu, geniş, düzgün, kronolojik bir veri istersiniz. Belirli bir süreyi bilseydiniz bu konuda size oldukça yardımcı olurdu.

Elbette, profil fotoğrafları için Facebook'un her yerine bakılıp, çıkarılabilir. Kayıt tarihlerine veya EXIF verilerine de bakabilirsiniz. Ancak bu profil fotoğrafları çok işinize yaramayabilir. Çünkü insanlar kronolojik sıraya göre güvenilir şekilde fotoğraf yüklemezler ve kullanıcılar kendinden başka şeylerinde fotoğraflarını yükleyebilirler. Örnek vermek gerekirse, biri

ölmüş köpeğinin fotoğrafını profil resmi yapmış olabilir. Bir başkası çizgi film karakterinin resmini kullanırken, diğerlerinde ise soyut desenler veya başka şeyler olabilir. Yani maden büyük, ama düzgün ve yalın değil. Hatta karmaşık. İşte bu yüzden temiz, basit, sıralı ve faydalı şekilde etiketlenmiş olan bir dizi fotoğraf işe yarayacaktır.

Dahası da var, Facebook'taki profil fotoğraflarında, fotoğrafın yayınlama tarihi ile çekildiği tarih birbirine uymayabiliyor. Fotoğraftaki EXIF verileri bile tarihi değerlendirmek için her zaman güvenilir olmaz. Çünkü insanlar çevrimdışı fotoğrafları tarayıp koyabilir, yıllar içinde birden fazla fotoğraf yüklemiş olabilir. Bazı insanlar başka yerde bulunan fotoğrafların ekran görüntülerini alıp, yükleyebiliyor. Bazı platformlar gizlilik için EXIF verilerini de çıkarıyor.

Sosyal medyada fırtına estiren 10 Year Challenge bu bağlamda düzgün, kronolojik bir veri oluşturuyor. İnsanlar 10 yıl öncesi ve sonrası fotoğraflarına da bilgi ekliyor. Mesela '2008'de şu üniversitede çekilmiştim, 2018'de ise yurtdışı tatilinde buraya geldim' gibi bir şeyler ortaya çıkıyor. İşin ucunda çok büyük ve sıralı bir veri kümesi var.

Bazı insanlar bu kadar fazla verinin veya bilginin kullanılmayacak çok olduğunu söylüyor. Ancak veri araştırmacıları ve bilim insanları bu verilerin nasıl hesaplanacağını, kullanılacağını biliyor. Sahte fotoğraflara gelecek olursak, görüntü tanıma algoritmaları insan yüzünü tanıyacak kadar karmaşık yapıda.

Facebook 10 Year Challenge olayında herhangi etkileri olmadığını söylüyor. Bir sözcü yaptığı açıklamada, "10 Year Challenge kendi başına viral olan ve bir kullanıcı tarafından oluşturulmuş bir şey. Bir internet caps'i. Facebook olarak başlatmadık, bundan bir şey kazanmıyoruz" dedi.

Bu konu için sosyal mühendislik durumu yok diyelim, ancak son birkaç senedir veri toplamak için tasarlanan birçok sosyal oyun örnekleri var. Mesela herkesin bildiği Cambridge Analytica skandalı.

Yüz tanıma algoritması geliştirmek için birinin Facebook fotoğraflarını kullanması kötü bir şey mi? Bu yüzden tüz tanıma için farklı senaryolar var.

İyi senaryoyu ele alırsak, yüz tanıma teknolojisi kayıp insanları, çocukları bulmada yardımcı olabilir. Geçtiğimiz sene New Delhi polisi yüz tanıma teknolojisini kullanarak, dört günde 3000 kayıp çocuğun izini buldu. Eğer çocuklar uzun süreden beridir kayıp olsaydı, biraz daha farklşı görünebilirlerdi. Yaş ilerleme algoritması burada oldukça faydalı olabilir.

Diğer bir senaryoya geçelim. Yaş tanımlama, yaş ilerleme algoritması reklamcılık için faydalı olabilir. Yaş gruplarına uyarlanabilen, özellikleri ve ayırt edilebilir reklam gösterimleri yapılabilir. Diğer yandan bu veriler konum izleme, yanıt verme veya satın alma davranışları gibi diğer verilerle birlikte birleştirince ürkütücü bir etkileşime sebep olabilir.

Ortaya çıkan çoğu teknoloji gibi kötü niyetli kişilerin elinde dolandırıcılık için kullanılması durumu da var.

Amazon, 2016 sonunda gerçek zamanlı yüz tanıma hizmetini kullanıma sundu. Daha sonra bu hizmeti Orlando, Oregon'daki polis departmanları gibi kanun güçlerine ve devlet kurumlarına satmaya başladı. Polis suçlular ve şüpheliler için bu teknolojiden yararlandı. Ancak bu teknoloji büyük gizlilik endişelerini de dile getirdi. Amerikan Sivil Özgürlükler Birliği, Amazon'dan bu hizmeti satmasını bırakmasını istedi.

Teknolojinin insanlığı nasıl etkilediğini tam olarak vurgulamak zor. İnsanlığı daha iyi hale getirmemiz için bir fırsat var, ancak bunu yapmak için kötüye gidebileceği yolları da tanımak ve bilmek zorundayız.

İnsanlar fiziksel ve dijital dünya arasındaki bağlantı noktası. Nesnelerin İnternetini ilginç kılan şeylerin çoğunluğu. Verilerimiz, işletmeleri daha akıllı ve karlı yapan bir yakıt. İşletmelerin verilerimize saygılı davranmasını talep etmeliyiz, aynı zamanda kendi verilerimize de saygı göstermeliyiz."

Kaynak: http://quq.la/3LouH

773 MİLYON E-POSTA ADRESİ HACKLENDİ

Bilişim tarihinin en büyük güvenlik açığı koleksiyonu, internet güvenliği uzmanı Troy Hunt tarafından açığa çıkarıldı.

Hunt, aralık ayının ortasında MEGA isimli dosya paylaşım sitesi üzerinde paylaşılan ve toplam 87 GB yer kaplayan veriler içerisinde 772 milyon 904 bin 991 adet mail adresi tespit etti.

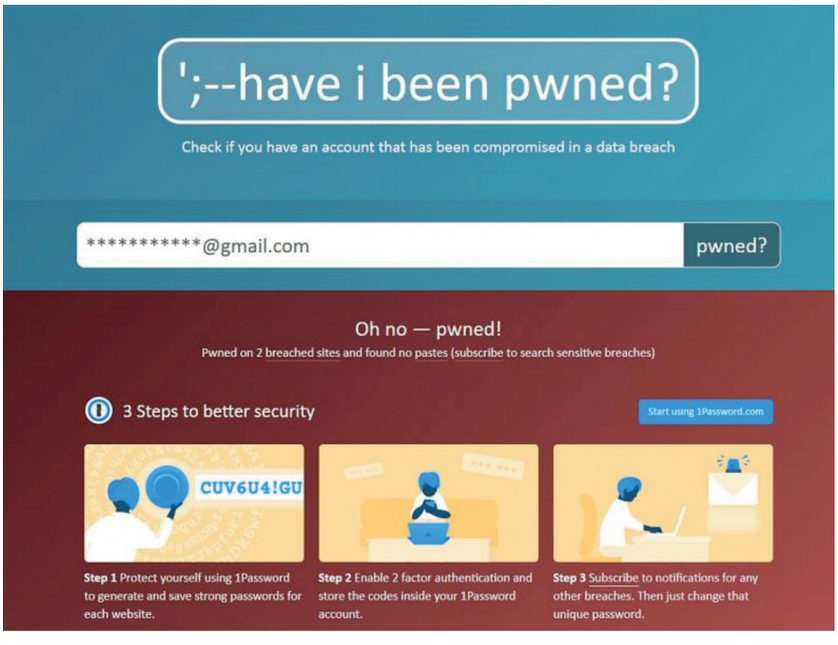
"Collection #1" olarak adlandırılan veri tabanını nasıl keşfettiğini ve içerisindeki verileri nasıl incelediğini kendi blog sitesinde açıklayan Hunt, koleksiyonun binlerce farklı kaynaktan elde edilen bilgilerden oluştuğunu dile getirdi.

E-Posta Adresiniz Hacklendi mi?

Troy Hunt ayrıca hacklenen mail adreslerinin sorgulanabileceği internet sitesi olan haveibeenpwned.com'un da kurucusu. Siz de bu siteye girerek e-posta adresinizi yazdığınızda, bilgilerinizin söz konusu veri tabanı içerisinde bulunup bulunmadığını kontrol edebilirsiniz.

Ancak sitede e-posta adresinize bağlı olarak hangi şifrenizin açığı çıktığı bilgisine yer verilmiyor. Yani eğer şifrenizi yakın zaman önce değiştirdiyseniz, korsanların mail adresinize girmesi zor olabilir. Ancak uzun süredir şifrenizi değiştirmediyseniz ve karşınıza "Oh no — pwned!" mesajı çıkıyorsa, parolanızı değiştirmenizde fayda var.

Kaynak: http://quq.la/rW1aG



SİBER SALDIRGAN İÇİN EN DEĞERLİ VARLIK: KULLANICI VERİSİ

Kullanıcı verilerinin siber saldırganlar için en değerli varlık olduğu ortaya çıktı.

Kaspersky Lab uzmanları, bu verilerin altın değerinde olduğunu belirterek, medyada geniş yer bulan olayların ve istenmeyen e-postalarla ilgili yapılan analizlerin de bunu kanıtlar nitelikte olduğunu vurguladı.

Siber saldırganların kullandığı sürekli gelişen yöntemlere karşı iki kat dikkatli olmak, özellikle de çevrim içi saldırılar söz konusu olduğunda çok büyük önem taşıyor.

Kaspersky Lab, dolandırıcıların en çok kullandığı 5 hileyi açıkladı:

Sosyal Ağlardan Gelen Sahte Bildirimler

Dolandırıcıların en sık kullandığı yöntem, popüler sosyal ağlardan geliyor gibi görünen sahte bildirimleridir. Bunlar genellikle yeni arkadaşlar, onların yaptıkları, yorumlar, beğeniler ve benzeri konularda olur. Bu tür mesajlar genellikle gerçeklerinden ayırt edilemez. Tek fark, çoğunlukla tespit edilmesi kolay olmayan kimlik avı bağlantıları içermeleridir. Bağlantıyı takip eden kullanıcıdan, kullanıcı adını ve şifresini sahte bir oturum açma sayfasına girmesi istenir.

Bir diğer yaygın kullanım ise sözde sosyal ağlardan gelen ve örneğin hesabınızda şüpheli bir etkinliğin tespit edildiğini veya yeni bir özelliğin kullanıma sunulduğunu ve şartları onaylamayan kullanıcıların hesaplarının engelleneceği tehdidini içeren mesajlardır. Durum ne olursa olsun, mesajda kimlik avı giriş sayfasının bağlantısına sahip bir düğme yer alır.

Bankacılık Kimlik Avı

Kullanıcıların banka kartı bilgilerini çalmayı amaçlayan kimlik avı saldırıları hala en popüler dolandırıcılık türü. Sahte mesajlar, ban-

ka veya ödeme sistemleri adına gönderilebilir. En yaygın mesaj konuları, müşterinin kişisel hesabının engellenmesi veya hesapta "şüpheli hareket" tespit edilmesi ile ilgilidir.

Hesaba erişimin yeniden sağlanması, kimlik bilgilerinin onaylanması veya yapılan işlemin iptali bahanesiyle kullanıcıdan sahte banka web sitesine banka kartı bilgilerini (genellikle CVV/CVC kodu dahil) girmesi istenir. Bu bilgiler alındığında, dolandırıcılar derhal kurbanın hesabından para çeker.Ödeme sistemlerinde de sistem aynı şekilde işler ancak bu durumlarda, kurbanlardan sadece hesaplarına giriş yapmaları istenir.

Popüler Hizmetler ve Satıcılardan Gelen Sahte Bildirimler

Benzer şekilde, popüler çevrim içi mağazaların, dağıtım hizmetlerinin, rezervasyon sitelerinin, multimedya platformlarının, iş arama web sitelerinin ve diğer popüler çevrim içi hizmetlerin adları kullanılarak sahte bildirimler oluşturulur. Siber suçlular, mesajlarının bu tür hizmetleri kullanan ve panik halinde ne görürse görsün tıklayacak veya dokunacak olan bir kısım kullanıcılara ulaşma ihtimaline güvenir.

E-Posta Hizmetlerinden Gelen Sahte Bildirimler

Dolandırıcılar, bu tür istenmeyen e-postaları, e-posta hizmeti kullanıcılarının kullanıcı adlarını ve şifrelerini elde etmek için gönderir. Yaygın olarak kullanılan iki bahaneden biri şudur: Kullanıcılar, şifrelerini yenilemeye veya güya dolu olan posta kutusunun hacmini artırmaya yönlendirilir. Bahanenin, posta kutusunun hacmini artırmaya yönelik olduğu durumlarda, kimlik avı bağlantısı, depolama kapasitesinde ciddi bir artış olacağını vaat eder. Yüksek miktarda veri depolama ihtiyacının sürekli olarak arttığı bulut bilişim çağında, bu vaat pek de şüpheli görünmez.

"Nijeryalı Prens" Dolandırıcılığı

Son olarak, en eski istenmeyen e-posta türlerinden biri de hala kullanılmaya devam ediyor. Bu dolandırıcılık türünde ölmüş bir milyonerin avukatı veya bir akrabasına yapılacak bir ödeme karşılığında bir servet vaat edilir. Aynı konunun değişik bir versiyonunda dolandırıcı, zor durumdaki bir ünlü olarak karşımıza çıkar.

Mağdurlara, banka hesaplarında mahsur kalmış parasını çekmek için talihsiz bir milyonere yardım etmeleri karşılığında büyük bir ödül vaat edilir. Bunu yapmak için öncelikle, mağdurların kendileri hakkında ayrıntılı bilgiler (pasaport bilgileri, hesap verileri vb.) vermesi ve evrak işleri için makul bir miktar para göndermesi gereklidir.Kaynak: http://quq.la/IQbYU

Kaynak: http://quq.la/IQbYU

İNTERNET GÜVEN(SİZ)LİĞİ

Yazan: Andy Bochman

Dijital savunma sistemlerine ne kadar yatırım yaparsanız yapın hacker'lardan tamamen korunmanız mümkün değil. Artık yeni bir stratejiye geçme zamanı.

Gelin acı gerçeği kabul edelim: Şirketinizin en son siber güvenlik donanımlarına, yazılımlarına, eğitimlere ve personele ne kadar yatırım yaptığının veya en önemli sistemlerini ne kadar izole edebildiğinin pek de bir önemi kalmadı. Eğer kritik sistemleriniz dijitalse veya bir şekilde internete bağlı ise (siz bağlı olmadıklarını sansanız dahi bağlı olabilirler) hiçbir zaman tamamen güvende değilsiniz demektir. Nokta.

Bu, son derece önemli bir tespittir zira bağlantılı sistemler ABD ekonomisinde neredeyse her sektörü etkiliyor. Ayrıca diğer tarafta bazı devletler, kriminal topluluklar ve terörist gruplar da bu gelişmelerin içerisinde yer alabiliyor. Örneğin ABD'de Atlanta yerel yönetimine ve dört doğalgaz şirketinin ortak kullandığı veri tabanına yapılan saldırılar, Equifax'a yapılan saldırı, WannaCry ve NotPetya gibi küresel çapta zararlı yazılım saldırıları henüz hafızalardaki yerini koruyor. Son yıllarda yaşanan bu elim hadiselerin büyük bir çoğunluğunda saldırıya uğrayan şirketler savunma hatlarının güçlü olduğuna inanıyorlardı.

ABD ekonomisi ve ulusal güvenliği için kritik öneme sahip kurumları izleyen ve bu kurumların kendilerini siber saldırılara karşı nasıl savunduklarını analiz eden bir kurum olan Idaho National Lab'de (INL) görev alıyorum. INL olarak özellikle endüstriyel kontrol sistemleri (elektrik hatlarında ve petrol rafinelerinde sıcaklık ve basıncı düzenleyen sistemler gibi) kullanan şirketlere odaklanıyoruz ve tüm konvansiyonel reçetelerin üzerinde bir çözüm oluşturmaya çalışıyoruz. Şu ana dek bulduğumuz çözüm şöyle: Devre dışı kaldığında işinize zarar verecek olan fonksiyonları belirleyin, bu sistemleri olabildiğince internetten izole edin, dijital teknolojileri minimuma indirin ve bu sistemlerin izlenme ve kontrol süreçlerinde analog araçlar ve güvenilir insan kaynağı kullanın. Her ne kadar metodolojimiz pilot aşamasında olsa da kurumlar bu yeni yaklaşımın birçok bileşenini hayata geçirebilirler.

Şunu söylemek lazım ki tamamen bilgi ekonomisine dayalı şirketler için çok fizibl olmayan bu yaklaşımımız bazı durumlarda operasyon maliyetlerini artırabilir ve verimliliğin düşmesine neden olabilir. Ancak kritik sistemlerin dijital unsurlar tarafından saldırıya uğramasını engellemenin tek yolu bu. Bu makalede laboratuvarımızın bu tür sistemleri belirleme konusundaki metodolojisini anlataca-

ğım. Kurumun liderlerinin çok fark edemediği ve saldırılara açık bazı fonksiyonlar veya süreçler o kadar önemli olabilir ki yaşanan bir sıkıntıda şirket çökebilir. Bu metodolojinin bileşenlerini birçok şirkette ve ordu kurumlarında bir süredir uyguluyoruz ve ABD'nin en büyük ikinci elektrik şirketi Florida Power & Light'ta da yöntemin tamamını bir yılı aşkın süredir hayata geçiriyoruz. ABD ordusunun bir kurumunda da ikinci pilotu başlatmak üzereyiz. INL olarak bu yaklaşımı ana akıma taşımak için de çalışıyoruz. Bu süreçte seçilecek mühendislik şirketleriyle iş ortaklığı yapmak ve onları bu yönteme dair eğitmek de söz konusu olacak.

Mevcut Tehdit

Endüstriyel şirketler uzunca bir zamandır mekanik pompalar, kompresörler, valfler, röleler ve tetikleyici mekanizmalar içeren sistemler kullanıyor. Eskiden, bu sistemlerin durumlarına dair bilgiler genellikle analog sensörlerden gelirdi ve alanında uzman mühendisler sistemlerin durumunu kontrol altında tutar ve gerektiğinde sabit hat telefonlarla genel merkezle iletişim kurardı. Sabotaj yapmak isteyen biri tedarik zincirine sızmadığı veya içeriden biriyle işbirliği yapmadığı takdirde direkt tesise girmek ve kapılardan, güvenlik görevlilerinden ve silahlı görevlilerden sakınarak içeri sızmak zorundaydı.

Bugün ABD İç Güvenlik Bakanlığı'nın kritik öneme sahip olarak nitelediği 16 altyapı sektörünün 12'si kısmen veya tamamen dijital kontrol ve güvenlik sistemlerini kullanıyor. İster fiziksel ister sanal olsun bu sektörlerdeki varlıklar, sistemler ve şebekeler son derece önemli zira bunların devre dışı kalması durumunda güvenlik, ekonomik güvenlik, sağlık ve toplumsal güvenlik veya bunların birkaçında büyük sıkıntılar çıkması söz konusu olabiliyor. Her ne kadar dijital teknolojiler muazzam bir yetkinlik ve verimlilik artışı getirse de siber saldırılara karşı daha açıklar. Büyük şirketlerin, devlet kurumlarının ve akademik kurumların sistemleri dark web'deki otomatik programlar tarafından sürekli taranarak açık aranıyor. Bu programların bir kısmı ücretsizken bazıları yüzlerce, binlerce dolara satılıyor. Eğer teknik destek de alınırsa bu fiyat artıyor. Genelde bunlar siber güvenlik sistemleri tarafından tespit edilebiliyor olsa da aylar hatta yıllar boyunca sürebilen, iyi planlanmış ve hedefli saldırılara karşı koyabilmek neredeyse imkânsız.

Siber saldırıların finansal etkileri de git gide artıyor. Son birkaç yılda WannaCry, NotPetya gibi saldırılar sırasıyla 4 milyar dolar ve 850 milyar dolarlık zarara neden oldu. ABD ve İngiltere'nin Kuzey Kore'yi sorumlu tuttuğu WannaCry saldırısının NSA'den çalınan bazı araçlarla gerçekleştirildiği belirtiliyor. Microsoft'un yayınladığı bir güvenlik yamasını yapmayan bilgisayarların Windows işletim sistemlerindeki açığı değerlendiren bu saldırı, 150 ülkede hastanelerde, okullarda, şirketlerde ve evlerde yüz binlerce bilgisayarın ele geçirilmesi ve kilidin açılması karşılığında fidye istenmesi şeklinde kurgulanmıştı. Rusya'nın Ukrayna politikasına karşı olan Özbekistan'ın neden olduğunu iddia ettiği NotPetya saldırısı Ukraynalı bir muhasebe yazılımının güncellenmesiyle yayıldı. Ukrayna hükümetine ve ülkedeki bilgisayar sistemlerine yönelik başlayan saldırı dünyanın farklı bölgelerine de yayıldı ve aralarında Hollandalı denizcilik şirketi Maersk, ilaç şirketi Merck, çikolata üreticisi Cadbury, reklamcılık devi WPP'nin de olduğu birçok şirketi etkiledi.

Açıklar Artıyor

Yapak zeka, makine öğrenmesi, bulut bilişim ve depolama, nesnelerin interneti ve otomasyon alanlarında yaşanan büyüme ile birlikte dijital dönüşümün hızı da artıyor. Karmaşık, yazılım ağırlıklı dijital teknolojilerin gelişmesi ve bunlara olan bağlılığın artması siber güvenlik anlamında ciddi bir sıkıntı da doğuruyor. Center for a New American Study'den Richard J. Danzig (deniz kuvvetleri eski komutanı ve CNAS'nin şimdiki başkanı) tarafından 2014 yılında yayımlanan bir makale dijital teknolojilere olan bağlılığımızı şöyle tanımlıyor:

Bu teknolojilerin muazzam bir gücü olsa da kullanıcıları daha az güvenli kıldıkları da bir gerçek. İletişim becerileri işbirliğini ve şebekeleri güçlendiriyor fakat aynı zamanda sızmalara karşı kapıyı aralıyor. Sistemlerin veriye odaklı ve manipülatif yapıları verimliliği ve ölçeği ciddi biçimde artırsa da başarılı bir saldırı sonucu çalınabilecek malzemenin boyutu da artıyor. Sistemlerin donanımlarının ve yazılımlarının karmaşık yapıları büyük yetkinlikler oluştursa da bu karmaşıklık, açık doğuruyor ve sızıntıları görmek zorlaşıyor. Özetle siber sistemler hepimize fayda sağlarken bir yandan da bizi zayıflatıyor ve zehirliyor.

Şu bir gerçek: Bu teknolojiler o kadar karmaşık ki bazı durumlarda bunları ortaya koyan üreticiler dahi sıkıntıları göremiyor. Üreticiler genelde otomasyon sistemlerini satarken insanlardan kaynaklanan hataları azaltmayı öne çıkarıyor ancak bu risklerin yerine başka riskler geliyor. Bilgi sistemleri şu anda o kadar karmaşık durumda ki korsanlık, veri koruma ve bilgi güvenliği politikaları alanında çalışan bir kurum olan Ponemon Institute'un verilerine göre ABD'li şirketlerin sistemlerine sızıntı olduğunu anlaması 200 günden daha fazla sürebiliyor. Ve bu şirketlerin

çoğu sızıntıları kendileri bulamıyor ve üçüncü partilerin yardımına ihtiyaç duyuyor.

Dünyanın her yerinde saldırıların sayısının ve verdikleri zararın artmasına karşın Target, Sony Pictures, Equifax, HomeDepot, Maersk, Merck ve Saudi Aramco gibi şirketlerdeki liderler dijital teknolojilerin sunduğu verimlilik artışı, iş gücünde azalma, insan kaynaklı hataların azaltılması veya ortadan kaldırılması, kalitede artış, müşterilere dair daha fazla bilgi toplama ve yeni teklifler oluşturma gibi vaatlerin cazibesine kapılmaktan kendini alamadı. Liderler her yıl yeni güvenlik çözümlerine ve maliyeti yüksek danışmanlara daha fazla kaynak ayırıyor, siber güvenlik konusunda konvansiyonel yaklaşımları devam ettirip en iyisini umuyorlar. Bu; boş yere umut beslemekten başka bir şey değil.

"Siber Hijyenin" Sınırları

Konvansiyonel yaklaşımlar ya da diğer tabiriyle "hijyen" şunları kapsar:

- Şirketin sahip olduğu donanım ve yazılım varlıklarına dair kapsamlı bir envanter oluşturmak.
- Uç nokta güvenlik çözümleri, firewall'lar ve sızıntı denetim sistemleri gibi en güncel savunma donanımlarını ve yazılımlarını edinip kullanmak.
- Çalışanları sızma e-postalarına karşı düzenli eğitimlere tabi tutmak.
- "Hava boşlukları" oluşturmak, yani önemli sistemleri diğerlerinden ayırmak. Aslında bu ayrımı tamamen yapabilmek de mümkün değil.
- Yukarıda sayılanların tamamını yapabilmek için farklı hizmetler ve hizmet sağlayıcılarla desteklenen geniş bir siber güvenlik ekibi kurmak.

Birçok şirket National Institute of Standarts and Technology (NIST) kurumunun siber güvenlik çerçevesi ve SANS Institute'un top 20 güvenlik kontrolü gibi işe yaradığı kanıtlanmış çerçeveler kullanmayı tercih ediyor. Bu çerçeveler yüzlerce etkinliği hatasız biçimde yapabilmeyi gerektiriyor. Çalışanların zor ve karmaşık şifreler kullanması, bunları düzenli olarak değiştirmeleri, transfer edilen verilerin şifrelenmesi, şebekelerin aralarında firewall'lar olacak şekilde segmente edilmeleri, hassas sistemlere erişimi olanların sayısının sınırlandırılması, tedarikçilerin yönetilmesi ve daha birçok adım gerekir.

"ŞİRKETİNİZİN SİBER HİJYENİ NE KADAR İYİ OLURSA OLSUN HEDEFLİ BİR SALDIRI ENİNDE SONUNDA ŞEBEKENİZE VE SİSTEMLERİNİZE ULAŞACAKTIR."

Birçok CEO, siber hijyen uygulamalarına sadık kalarak şirketlerini saldırılardan koruyabileceklerine inanıyor. Yüksek profilli birçok sızma ve saldırı bunun doğru olmadığını kanıtladı. Yukarıda adını saydığımız birçok şirketin geniş bir siber güvenlik ekibi vardı ve saldırıya uğradıkları dönemlerde ciddi siber güvenlik yatırımları yapmışlardı. Siber hijyen sıradan ve amatörce yapılan saldırılara karşı etkili olsa da sofistike düşmanlar tarafından yapılan, kritik varlıklara yönelik ciddi saldırılara karşı yetersiz kalabilir.

Enerji, ulaştırma ve ağır sanayi gibi varlık yoğun endüstrilerde hatasız bir uygulama sağlayacak bir insan kaynağı veya yatırım mümkün değildir. Aslında birçok şirket, genel çerçevenin ilk aşaması olan kurumun donanım ve yazılım varlıklarına dair envanteri bile yeterince oluşturamamıştır. Bu çok ciddi bir eksiklik, zira sahip olduğunuzu bilmediğiniz bir şeyin güvenliğini sağlayamazsınız.

En iyi uygulamalara dair bazı ödünleşimler de söz konusudur. Genelde güvenlik güncellemeleri için sistemleri kapatmanız gerekir ki bu her zaman uygun olmayabilir. Örneğin kamu hizmeti şirketleri, kimya şirketleri ve bazı diğer yapılarda süreklilik esastır ve her yeni güvenlik yamasını uygulamak için sistemi kapatmak mümkün olmayabilir. Bu tür sektörlerdeki şirketler genelde yamaları periyodik olarak yüklemeyi tercih eder ve bu periyotlar aylar sürebilir. Diğer bir konu da dağıtık varlıkları korumaktır. Örneğin büyük ölçekli kamu hizmeti şirketleri binlerce alt istasyonu yönetir ve bunlar binlerce kilometrekarelik bir alana yayılmış olabilir. Bunları güncellemek de kolay değildir. Eğer güncellemeleri yapmak için bir şebekeye erişmeniz gerekiyorsa kalifiye bir düşman da bu şebekeye girip kötü niyetini gerçekleştirebilir. Eğer çalışanlarınız bu noktalarda güncellemeleri fiziksel olarak yapıyorlarsa bu işlem çok maliyetli olabilir. Bu iş taşeronlara verildiğinde ise sadakat sorunları ortaya çıkabilir.

"CİHAZLARA KİM ERİŞEBİLİYOR?' SORUSUNA ÇOK ŞAŞIRACAĞINIZ YANITLAR ALABİLİRSİNİZ."

En iyi uygulamalar mükemmel biçimde hayata geçirilse dahi iyi derecede fonlanan, sabırlı, sürekli kendini geliştiren, sofistike hacker'lara karşı tam bir koruma sağlanamaz ve bunlar her zaman açık bir kapı bulabilir. Şirketinizin hijyen seviyesi ne kadar iyi olursa olsun hedefli bir saldırı, sisteminizi aşabilir. Hacker'lar bunun için haftalarca hatta aylarca uğraşabilir ve içeri sızabilirler.

Bu sadece benim görüşüm değil. American Electric Power'ın eski güvenlik üst yöneticisi ve şu anda SANS Institute'un başında bulunan Michael Assante, "Siber güvenlik

ayak bileğinizi ısıran tehditlere karşı yardımcı olabilir ve ütopik olsa da tam anlamıyla uygulandığında saldırganların yüzde 95'ini durdurabilir. Ancak gerçek hayatta bu yaklaşım belirli bir hedefe göz koyan sofistike saldırganlar için sadece bir hız tümseği görevi görecektir" diyor. Yahoo'nun ve Twitter'ın eski güvenlik üst yöneticisi olan Bob Lord, geçen yıl Wall Street Journal'a verdiği bir röportajda, "Kurumsal güvenlik yöneticileriyle konuştuğumda 'En sofistike saldırılara karşı savunma yapamıyorum. Yani bu kaybedilecek bir oyun. Bu nedenle de sorun hakkında detaylı düşünmek içimden gelmiyor.' diyorlardı." diyor.

Bu konuda bir örnek olay 2012'de yaşanan Saudi Aramco vakasıdır. İyi bir savunma sistemine sahip olan bu şirkete yönelik saldırı (ABD'li yetkililer bu saldırının İran tarafından yapıldığından şüpheleniyor) petrol şirketinin kurumsal bilgisayarlarının üçte ikisinin sistemlerindeki verilerin silinmesine neden oldu. 2018 yılının Mart ayında gerçekleşen başka bir saldırının amacı ise şirketin tesislerinden birindeki güvenlik kontrol mekanizmalarını kapatarak bir patlama gerçekleştirmekti. New York Times'a göre saldırganın kodundaki bir hata nedeniyle bu saldırı ucuz atlatıldı. Times, "Saldırganlar sadece sisteme nasıl sızacaklarını bilmekle kalmamış sistemin tasarımı ve tesisin yerleşimi konusunda da çok iyi bilgi edinmişler. Hangi boruların nereye gittiği, hangi valflerin kapatıldığında patlama olabileceği gibi bilgilere de sahiplermiş." diye yazıyordu.

INL'nin Radikal Fikri

Artık tamamen farklı bir yaklaşımı benimsemenin zamanı geldi: Tamamen dijital karmaşa ve bağlantı üzerine kurulu sistemlere güvenmeyi bırakmanın zamanı geldi. Bunu yapmak için en önemli süreçleri ve fonksiyonları belirlemek ve sonrasında saldırganların bunlara erişebilecekleri dijital yolları kapamak veya ortadan kaldırmak gerekiyor.

Idaho National Lab bu konuda adım adım bir yöntem geliştirdi. Bu yönteme durumsal, siber odaklı metodoloji (CCE) denilebilir. CCE'nin amacı sadece tek bir seferlik risk değerlendirmesi yapmak değil, aksine kıdemli liderlerin siber risklerin şirketlerine dair etkilerini düşünme ve değerlendirme biçimlerini değiştirmek. Her ne kadar bu yaklaşım pilot aşamasında olsa da sonuçları gayet iyi. CCE'nin 2019 yılında tamamen hayata geçmesini ve 2020 yılında bu konuda çeşitli şirketlerin lisanslandırılmasını umut ediyoruz. Ancak bugün bile CCE yaklaşımının ana konsepti herhangi bir şirket tarafından uygulanabilir. (Laboratuvarımız buna yardımcı bir çerçeve daha geliştirdi: Siber odaklı mühendislik [CIE] adı verilen bu yapı CCE'ye benzer olsa da mühendislik yaşam döngüsünün tamamında siber risklerden kaçınmayı öne çıkarıyor.)

Metodoloji aşağıda tanımlanan yapılar tarafından gerçekleştirilmesi gereken dört adımdan oluşuyor:

- CCE uzmanı – Şu anda INL'den bir yetkili bu rolü üstleniyor fakat gelecekte INL tarafından eğitilen şirketlerden kişiler de bu rolü üstlenebilecek
- Düzenlemelere uyum, hukuk ve riskten kaçınma alanlarındaki tüm liderler: CEO, COO, CFO, CRO, hukuk baş müşaviri, CSO.
- Temel operasyonel fonksiyonları yöneten kişiler
- Şirket için önemli süreçlere hakim olan güvenlik uzmanları, operatörler ve mühendisler
- Sistemlerin ve teçhizatın nasıl kötü amaçlar için kullanılabileceğini bilen siber uzmanlar ve süreç mühendisleri

Bu kişilerin bazıları için süreç stresli olacaktır. Örneğin çeşitli kurumsal risklere açık olmak CSO'yu rahatsız edecektir. Ancak genelde bu yükü CSO'ya yüklemek adil olmaz. Hiçbir CSO, güçlü bir saldırganın hamlesine karşı tam olarak hazırlıklı olamaz.

1. "En Değerli" Süreçleri Belirleyin

Tüm süreç; INL'nin durumsal önceliklendirme olarak tanımladığı işlemle başlıyor. Bu işlemin özünde olası katastrofik veya sonuçları ağır olabilecek olaylara dair senaryolar oluşturmak yatıyor. Bu noktada da şirket için çok önemli olan fonksiyonların ve süreçlerin belirlenmesi gerekiyor. Örneğin bir elektrik şirketinin faaliyetini kesintiye uğratacak bir trafo saldırısı veya bir doğalgaz şirketinin abonelerine gaz ulaştırmasını engelleyebilecek boyutta bir kompresör saldırısı... Başka örnekler arasında bir kimya veya rafineri tesisinin güvenlik sistemlerine yapılan, basıncın kontrol dışına çıkması ve bir patlama yaşanmasıyla birlikte yüzlerce veya binlerce kişinin hayatına mal olabilen, ciddi hukuki sonuçlar doğurabilecek, şirketin piyasa değerini etkileyebilecek ve şirketin yöneticilerinin işlerini kaybetmelerine neden olabilecek senaryolar verilebilir.

Sofistike siber düşmanların neler yapabileceğine aşina olan danışmanlar ile çalışmak olası düşmanların niyetlerini daha iyi okumaya yardımcı olabilir. "Eğer süreçlerinizi sekteye uğratmanız veya şirketinize zarar vermeniz gerekse siz ne yapardınız?" ve "Kırılması en zor olandan bir sonraki en önemli tesisiniz hangisi?" gibi sorulara cevap

arayarak en fazla zararın oluşabileceği ve saldırıya en açık yapılar belirlenebilir ve üst yönetimle istişare edilerek senaryolar oluşturulabilir. Bu adım, şirketin büyüklüğüne de bağlı olarak birkaç haftadan birkaç aya kadar sürebilir.

2. Dijital Ortamın Haritasını Çıkarın

Genelde bir tam hafta süren ancak daha da uzayabilen ikinci işlem; tüm donanımın, yazılımın ve iletişim teçhizatının; bunları işleten ve bunlara destek veren personelin (bunun içerisine üçüncü partiler de dahil) bir haritasını çıkarmaktır. Bu süreçte üretimin aşamalarını belirlemek, kontrol ve otomasyon sistemlerinin dahil olduğu mekanları belgelemek ve gerekli tüm fiziksel ve veri temelli girdileri sağlamak gereklidir. Tüm bu bağlantı noktaları saldırganların potansiyel hedefleridir ve şirketler bunların bir çoğunun farkında değildir.

Bu bileşenlere dair elde bulunan haritalar hiçbir zaman tüm gerçeği gösteremez. "Cihazlara kimler dokunuyor?" ve "Bilgi şebekelerinizden nasıl akıyor ve nasıl korunuyor?" sorularını yönelttiğiniz kişilerden çok sürpriz cevaplar alabilirsiniz. Örneğin ekibiniz, bir şebeke mimarından veya kontrol mühendisinden edindiği bilgiler sonucunda önemli bir sistemin sadece operasyonel ağa değil aynı zamanda muhasebe, tahsilat ve benzeri işlemler için kurumsal bilgi ağına da bağlı olduğunu öğrenebilir. Yani aslında bu sistem internete de bağlıdır. Ekibiniz, tedarikçileri yönetmekten sorumlu bölümle yaptığı değerlendirmede bu sistemleri tedarik eden şirketlerin bakım ve izleme amaçlı olarak bunlara kablosuz bağlantı ile doğrudan erişebildiğini fark edebilir. Bir güvenlik sistemi tedarikçisi teçhizat ile doğrudan iletişime geçemediğini söyleyebilir ancak mekanik yapıya ve güncellemelere yakından bakıldığında bunun bir yolu olduğu görülebilir. İşte böyle bir keşif tüm ekip için uyanış anı olacaktır.

3. Olası Saldırı Yollarını Belirleyin

Ekibiniz, Lockheed Martin'in geliştirdiği bir metodolojinin türevini kullanarak saldırganların yukarıda belirtilen hedeflere ulaşmasına imkân veren muhtemel ve en kısa yolları belirleyebilir. Bu yollar zorluk derecelerine göre önceliklendirilebilir. CCE uzmanları ve saldırganlar ve onların yöntemleriyle ilgili hassas bilgilere sahip olan kişileri de içeren dış uzmanlar bu süreçte önemli roller üstlenirler. Bu uzmanlar dünyanın başka ülkelerinde benzer sistemlere olan saldırılara dair devlet kaynaklarından edindikleri bilgileri paylaşırlar. Güvenlik sistemleri, şirketin siber saldırılara yönelik yetkinlikleri ve prosedürleri ve benzeri bilgiler sayesinde ekibiniz olası saldırı yolları listesini oluşturabilir ve bu listeyi dördüncü adımda tariflenecek olan, liderlere sunulacak senaryoları geliştirme sürecinde kullanabilir.

4. Riskten Kaçınma ve Riski Önlemeye Dair Seçenekler Oluşturun

Artık etkisi en fazla olabilecek siber risklere karşı çözümler oluşturma zamanı geldi. Eğer bir hedefe yönelik 10 yol varsa, ancak bunların hepsi belirli bir düğümden geçiyorsa savunmayı kurmak için ideal nokta bu düğümdür. Bu düğüme 'tripwire' olarak adlandırılan ve olası bir sorunu anında uzmanlara bildiren yüksek hassasiyete sahip bir sensör sistemi kurulabilir.

Bazı çözümler şaşırtıcı derecede basit ve uygun maliyetli olabilir. Örneğin dışarıdan bir sızma nedeniyle kendine zarar vermesi veya kendini imha etmesi komutu verilen bir fiziksel sisteme dair riski anlamak için donanım temelli bir hareket sensörü uygulamak yeterli olabilir. Biraz daha alt düzeyde olsa da belirli bir fonksiyonu yedekleyen ve gerektiğinde devreye giren bir yedekleme sistemi gibi diğer bazı çözümler daha fazla zaman ve kaynak gerektirebilir. Her ne kadar çözümlerden bazıları operasyonel verimlilik ve iş fırsatları oluşturma anlamında negatif etkiler ortaya çıkarmasa da bazıları bu konularda sıkıntılara neden olabilir. Bu nedenle şirketlerin liderlerinin hangi risklerin kabul edilebileceğini, hangilerinden kaçınmak gerektiğini ve hangilerinin önlenmesi gerektiğini belirlemesi ve bu yönde yollarını çizmesi gerekecektir.

Eğer ele alınan bir süreç, izleme veya bilgi aktarımı için dijital bir kanal içeriyorsa, olası sıradışı trafiği tespit etmek açısından bu sisteme erişim yollarını en aza indirgemek önem taşıyacaktır. Bununla birlikte, şirketler, katastrofik bir olaya neden olabilecek, dijital komutlar alabilen bir sistemi korumak için bir donanımdan yararlanabilir. Örneğin sıcaklığın veya basıncın belirli bir seviyeye erişmesini engelleyen bir mekanik anahtar veya valfin gözlemlenmesinde dijital sistemlerin yanında bir termometre veya basınç sensörü eklenerek cihazın gerçekten doğru verileri aktarıp aktarmadığı kontrol edilebilir. Eğer şirketiniz ciddi bir siber saldırı yaşamadıysa kritik sistemleri olabildiğince bağlantı dışına çıkarmak, eski model mekanik cihazları kullanmak ve otomatize edilen süreçlere insanları eklemek yavaşlatıcı ve çağdışı bir yaklaşımmış gibi gelebilir. Bu yaklaşım verimliliği azaltabilir ancak mevcut

yöntemlerinizin engelleyemeyeceği bir felaketin olası maliyetleri göz önüne alındığında bu akıllı bir hamle olacaktır.

CEO'ların ve COO'ların bu sürece şüpheyle yaklaşması muhtemel. On yıllardır tekrarlanagelen söylemlerin dışına çıkan bir değişim yönetimi projesinin zorlu bir süreç gerektireceği kaçınılmaz bir gerçektir. Özellikle erken aşamada karşılaşacağınız direnci tahmin etmeye çalışın. Şirketinizle ilgili bu kadar çok bilgiyi açığa çıkarmak ve daha önce farkına bile varmadığınız zayıflıklarınızı görmek ve bunlar hakkında tartışmak psikolojik olarak da kolay değildir. Daha ileriki aşamalarda mühendisler, sorumlu oldukları sistemlerin zayıflıklarıyla yüzleşecektir. Bu süreçlerde ekip üyelerinizin en zorlu analizlerde bile kendilerini güven içerisinde hissetmelerini sağlayın. Sonuçta düşmanların yaklaşımları ve neler yapabileceklerine dair bilgiler aydınlatıcı olacaktır. En fazla direnç gösteren ekip üyeleri bile riskleri gördüklerinde ve onlardan kaçınmaya dair yöntemleri anladıklarında sürece katkı vermeyi kabul edeceklerdir.

Bugünden Neler Yapabilirsiniz?

Düşmanlarınız gibi düşünmeyi öğrenin. Hatta kritik hedefleri ele geçirmeye çalışarak savunmanızın gücünü sürekli analiz eden ve değerlendiren bir ekip kurabilirsiniz. Bu ekipte ilgili süreçlere, kontrol ve güvenlik sistemlerine ve operasyonel şebekelere dair tecrübesi olan kişiler bulunabilir.

Yüksek seviyede siber hijyen elde etmiş olsanız dahi tedbiri elden bırakmayın. Bunu yapmanın en iyi yolu üst seviye kimya fabrikalarında ve nükleer tesislerde uygulanan güvenlik kültürünü hayata geçirmektir. En acemisinden en kıdemlisine dek tüm çalışanlar ilgi alanlarındaki bir sistemin veya cihazın normal dışında davranışlar göstermesi durumunda hızla reaksiyon vermenin ne kadar önemli olduğunu anlamalı. Bu tür bir durum bir cihaz arızası olabileceği gibi bir siber saldırı da söz konusu olabilir.

Son olarak, sizin veya ekibinizin en kritik fonksiyonları destekleyen sistemlere dair güveninizin azaldığı durumlarda devreye girecek bir B planı yapılması gerekir. Bu plan kapsamında şirketinizin kritik operasyonları, biraz azaltılmış bir seviyede olsa da devam edebilecek şekilde kurgulanmalıdır. İdealde yedekleme sistemleri, dijital teknolojilere dayanmamalı ve bir şebekeye, özellikle de internete bağlı olmalarıdır. Ayrıca orijinal sistemin bire bir aynısı olmamalıdır zira saldırganlar orijinal sisteme sızabildilerse yedek sisteme de sızabilirler.

Dijital teknolojilere ve internete bağımlı olan her kurum ciddi bir siber tehditle karşı karşıyadır. En yüksek seviyede siber hijyen bile Rusya, Kuzey Kore ve yüksek derecede yeteneklere sahip kriminal ve terörist örgütleri durdurmaz. Şirketinizi korumanın tek yolu teknolojik anlamda bir geri adım gibi görülebilen ancak mühendislik açısından bakıldığında ileri adım olarak nitelendirilebilecek bazı hamleler yapmaktır. Burada amaç, kritik fonksiyonların dijital teknolojilere ve internete olan bağlılıklarını mümkünse tamamen veya kısmen ortadan kaldırmaktır. Ortaya çıkacak maliyet işin durmasına kıyasla makul olacaktır.

ÖZETLE

SORUN

Şirketiniz en son siber güvenlik donanımlarına, yazılımlarına, eğitimlerine, personeline sahip olsa da kritik dijital sistemleriniz hiçbir zaman tamamen güvende değil. Dijital teknolojiler muazzam bir yetkinlik ve verimlilik artışı getirse de, şirketleri siber saldırılara karşı daha açık hale getiriyor. Bu siber saldırıların finansal etkileri günden güne artıyor. Siber hijyen uygulamalarına sadık kalarak şirketlerin saldırılara karşı korunabileceği fikri, yüksek profilli sızma ve saldırılarla çürütülmüş durumda.

SEBEP

Sistemlerin veriye odaklı ve manipülatif yapıları verimliliği ve ölçeği ciddi ölçüde artırsa da başarılı bir saldırıyla çalınabilecek malzemenin boyutu da artıyor. Bu karmaşık teknolojilerin üreticileri dahi bazı sıkıntıları göremeyebiliyor. Güvenlik çözümlerine ayrılan kaynaklar ve siber hijyen dediğimiz konvansiyonel yaklaşımlar boş yere umut beslemekten başka bir şey getirmiyor.

ÇÖZÜM

ABD ekonomisi ve ulusal güvenliği için kritik önemi olan kurumların siber saldırılara karşı geliştirdikleri savunmaları analiz eden INL tüm konvansiyonel reçetelerin üzerinde bir çözüm oluşturuyor. CCE denen bu durumsal, siber odaklı metodoloji belirli yapılar ve adımlar sunarak en önemli süreçlerin ve fonksiyonların belirlenmesine, ve saldırganların kullanabilecekleri yolların tıkanması veya ortadan kaldırılmasına dayanıyor. CCE, Kıdemli liderlerin siber risklerin şirketlerine etkilerini düşünme ve değerlendirme biçimlerini değiştirmeyi amaçlıyor.

Kaynak: http://quq.la/JwKxy

ŞAMPİYONLUĞU KAPTIRMAYAN ŞİFRE: 123456

Antivirüs ve internet güvenliği kuruluşu ESET, neredeyse her güvenlik önerisinde şifre ve parolaların güçlü düzenlenmesini öneriyor. Çünkü güçlü şifreler, siber güvenlikte en temel korunma önlemlerinin başında geliyor. Ancak bilgisayar kullanıcılarının bu konudaki karnesi iyi görünmüyor. ESET, 2018'in en kötü şifrelerini duyurdu.

Parola güvenlik şirketi SplashData'nın her yıl yayınladığı ve ESET'in de her yıl mercek altına aldığı, "en sık kullanılan en kötü şifreler" sıralamasında genel görünüm hiç de rahatlatıcı değil. Küresel seçimlerden yola çıkılarak hazırlanan listede ilk sırada "123456" yer alıyor. Bunu bir başka çılgınca seçim olan "password" takip ediyor. Aslına bakılırsa bu iki seçim, 5 yıldan beri ilk iki sırayı kimseye kaptırmayarak yaygın parolalar arasındaki en vazgeçilmez tercihler olarak göze çarpıyor. Sonraki beş sıra ise, sayıların kolayca tahmin edilebilmesi ve hatırlanabilmesine dayanan bazı seçimlerden oluşuyor.

ESET Türkiye İstanbul Teknik Müdürü Gürcan Şen, "Parolanız bu en yaygın tercihler arasında yer alıyorsa, bunu hızla değiştirmenizi öneriyoruz" açıklamasını yaptı. Şen, "Bu şifreler çok kolay tahmin edilebilir durumda, dolayısıyla en temel savunma refleksinden bile yoksun durumdasınız" bilgisini paylaştı.

İşte yılın en kötü 20 şifresi:

1. **123456**
2. **password**
3. **123456789**
4. **12345678**
5. **12345**
6. **1111**
7. **1234567**
8. **sunshine**
9. **qwerty**
10. **iloveyou**
11. **princess**
12. **admin**
13. **welcome**
14. **6666**
15. **abc123**
16. **football**
17. **123123**
18. **monkey**
19. **654321**
20. **!@#$%^&***

SplashData, toplumun neredeyse %10'unun "bu yılın listesindeki en kötü şifrelerden en az birini kullandığını" tahmin ediyor. Ayrıca neredeyse yüzde 3'ünün en yaygın zayıf parola olan "123456" kullandığı tahmin ediliyor. Bu yılki sıralama, çoğunlukla Kuzey Amerika ve Batı Avrupa'da bilgisayar kullanıcıları tarafından sızdırılan beş milyondan fazla şifreyi temel alıyor.

Konuyla ilgili orijinal ESET makalesi şuradan takip edilebilir: http://quq.la/Bk6KM

Kaynak: http://quq.la/148BK

AKILLI BELEDİYECİLİK VE BLOCKCHAİN

Yazan: Andy Bochman

Son dönemde yerel yönetimlerin gündeminde olan akıllı şehir uygulamalarının Blockchain tabanlı hale getirilmesi vatandaşa nasıl faydalar sağlayacak?

Şu sıralar belediye denildiğinde kamuoyunun gündemi 31 Mart'taki seçimlerle kuşatılmış durumda ama belediyecilik yani yerel yönetim hizmetleri uzun vadeli bakılması ve bu seçim gündemi kuşatmasının ötesinde değerlendirilmesi gereken bir olgu.

Yeni yılın hemen öncesinde yapılan Akıllı Belediyecilik Zirvesi'nde yer alan "Dijital Dönüşüm Çağında Akıllı Şehirler Kurmak" başlıklı panelde de bu amaca yönelik olarak akıllı şehir uygulamalarının "kent kaynaklarını akıllı ve verimli kullanan ve vatandaşla bütünleşen şeffaf ve katılımcı hizmetler geliştirme" vizyonu ışığında nasıl geliştirilebileceği ve bu bağlamda Blokchain'in akıllı şehir uygulamalarıyla nasıl kullanılabileceği konusunda kısa bir konuşma yaptım. Söz konusu konuşmayı aynı vizyon doğrultusunda ancak biraz daha geniş ve derli toplu biçimde sizlerle paylaşmak isterim.

Blockchain veya Blokzincir en temelde, insanların halihazırda yaptığı alışveriş, bilgi değişimi, bankacılık, ödeme, alım-satım gibi çeşitli günlük hayat işlemlerini İnternet üzerinden ama arada bir aracı kişi ya da kurum olmadan da güvenli hızlı ve şeffaf biçimde yapabilmesini sağlayan bir işleyiş. Blockchain'in yerel yönetimler için en önemli değeri ise, işlem kayıtlarının şeffaf olması ama kişisel bilgilerin mahrem kalabilmesini sağlayacak bir şifreleme yapısına sahip olması.

Zaten bu işleyiş biçimi Blockchain'i (Kripto paralardaki gibi bir dijital değiş-tokuş ve ödeme protokolü olmasının ötesinde) bir dijital güven protokolü haline getirmektedir. Blockchain tabanlı sistemler, güven amaçlı kullanılan ve iş süreçlerini merkezileştiren noter, banka gibi aracıları ortadan kaldıran değiştirilemez, taklit ve tahrif edilemez bir işleyişe sahiptirler ve hız ile şeffaflık gerektiren kayıtlar üretmek, yayınlamak ve saklamak (arşivlemek) için en elverişli çözümlerdir.

Bu bağlamda Akıllı Şehir ve Blockchain kavramlarını bir araya getirdiğimizde; "Kent kaynaklarını akıllı ve verimli kullanacak hız, şeffaflık ve vatandaşın katılımcılığı yüksek iş süreçleri tasarlamak ve bu bağlamda yerel yönetimdeki bürokrasiyi de azaltacak bir işleyiş yaratmak" gibi bir hedef belirleyebiliriz.

Burada Blockchain'in halihazırdaki akıllı şehir uygulamalarından en önemli farkı, mevcut uygulamaların bilgi analiz ve karar mekanizmalarının süpermerkezi otomotize veya yapay zekaya dayalı ve giderek birer büyük biradere dönüşmesi olası sistemler üzerinden çalışırken Blockchain sistemlerinin daha otonom ama konsensüs tabanlı sistemlere dayalı dağıtık bir işleyiş yaratmasıdır.

Bu sayede vatandaşların sisteme katılımı ve sistemi denetimi de kolaylaşmakta. Konuyu bu şekilde ele aldığımızda ise, belediyelerde nasıl pratik kullanımlar olacağına ilişkin bir kaç örnek de verilebilir. Mesela kentin bina, emlak ve arsa kayıtlarının şeffaf ve taklit edilemez biçimde envanteri çıkartılıp kayıt altına alınabilir ve bu kayıtlar da pafta ve ada bazında kent planlamalarında esas alınıp buradaki sicil işlemleri insan inisiyatifinden olabildiğince çıkarılarak gayrimerkezi halde de işler biçimde tutulabilir.

Bir başka örnek, kentteki akıllı tüm nesnelerin Blockchain üzerine taşınarak bu nesnelerden gelen trafik, afet, hava kirliliği gibi bilgilerin akıllı kontratlar üzerinden çeşitli aksiyonlara dönüşmesi (araçların rota değişikliği, afet bölgelerinde yapılacak altyapı sınırlamaları veya kesintileri gibi) olabilir.

Bu işleyişin normal yapay zeka sistemlerinden en büyük farkı, süper merkezi ve hacklenmesi halinde büyük felaketlere yol açacak sistemlerin daha dağıtık ve şeffaf bir konsensüs mekanizması ile işlemesi ve söz konusu riskleri azaltmasıdır.

Her daim söylediğim gibi, Blockchain projelerinin çoğu bir token veya kriptoparaya dönüştürüldüğünde iş süreçleri çok daha işlevsel ve rasyonel hale gelmekte. Akıllı Şehir kullanımı olarak çok önemli bir örneği de, İstanbul Kart'ın bir Kriptoparaya dönüştürülmesi üzerinden verebiliriz. Bu sayede İstanbulCoin'e dönüşmüş bir İstanbul Kart, sadece ulaşımda değil çok daha çeşitli bir hizmet portföyünün (su, doğalgaz faturaları, vergi kültür-sanat aktiviteleri, otopark, vd.) ödemeleri için de kullanılabilir. Burada da mevcut sistemden en büyük fark, tüm ödeme işlemlerinin anında ve açık biçimde muhasebeleştirilerek takip edilebilmesi. Ayrıca, bu işleyişi vatandaşla ilişkilerde bir ödül sistemi olarak da kullanıp, vatandaşlar kente yaptığı çeşitli katkılar (ağaç dikme kampanyalarına katılım, kaçak yapı ihbarı, kentle ilgili yaratıcı önerilerde bulunma) karşılığında ödüllendirilebilir. Belli sayıda etkinliğe katılanlara artı bir ödül, vergisini erken ödeyenler için indirim gibi bir ödül puan sistemi de kurulabilir.

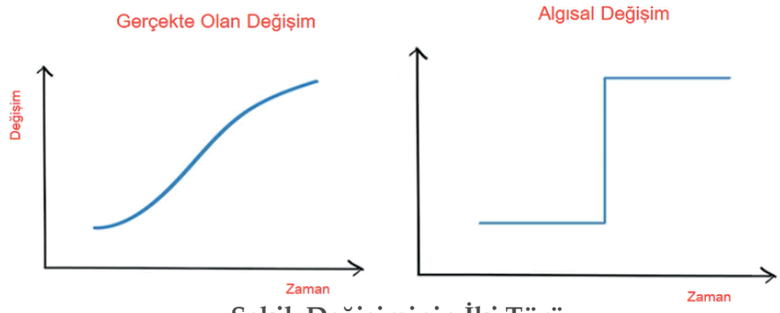
Özetle; Blockchain tabanlı akıllı şehir uygulamalarının artması, belediyecilik hizmetlerinin sadece daha akıllı biçimde icra edilmesinin ötesinde daha şeffaf, daha katılımcı bir yönetim anlayışına geçilmesini de beraberinde getirecek ve belediyelerin de yerel yönetimden yerel yönetişim anlayışına geçmesinde başrol oynayacaktır.

Kaynak: http://quq.la/KVPu0

DEĞİŞİM VE BLOCKCHAİN NE İFADE EDİYOR?

Yazan: Adnan Veysel Ertemel

Felsefi açıdan bakıldığında değişimin iki farklı türde gerçekleştiğini söylemek mümkün. Gerçekte olan değişim aşağıda bulunan soldaki grafikte olduğu gibi doğrusal iken algıdaki değişim sağdaki grafikteki gibi gerçekleşir; toplumlar değişimi algılama konusunda direnç gösterir.

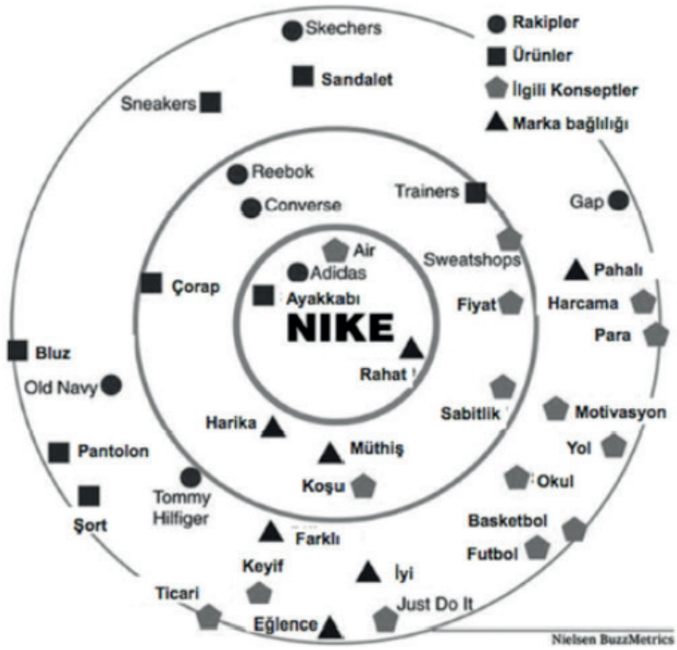


Şekil: Değişiminin İki Türü

Kritik bir eşik geçildikten sonra değişim tüm toplum tarafından bir anda algılanır. Tıpkı Bitcoin'in 2008 yılından beri var olmasına karşın 2017 yılının son aylarında tüm dünyada toplumun dikkatini çekmesi gibi...

İnternetin, bilginin yapısı üzerinde nasıl bir devrimsel değişim getirdiğini içinde bulunduğumuz çağda bile tam olarak algılayamayan kesimler söz konusu.. İnternet öncesi devirde televizyon "izlerdik", kitap "okurduk". Kısaca bilginin akışı tek yönlü olurdu... İnternetle birlikte bilginin akışı tek yönlü olmaktan çıkıp çift yönlü hale geldi.. İnternetin genetiğini çözümleyen vizyoner şirketler bu durumu stratejik avantaja çeviriyor. Netflix, kimin günün hangi saatinde hangi cihazdan tam olarak hangi dizi/filmi izlediğine, hangi sahneleri tekrar tekrar izleyip hangi sahnede rahatsız olup ekranı kapattığına bakarak büyük veri analiziyle ne tür bir prodüksiyonun gerçek anlamda hit olacağını kestirebiliyor. House of Cards dizisi tam da böyle bir çalışmanın ürünü... Amazon.com, e-kitap okuyucusu üzerinden niş bir konudaki belirli bir kitabı okuyan müşterilerine, kitabın hangi sayfasının hangi satırını işaretlediğine göre, aynı kitabın aynı sayfalarının aynı satırlarını işaretleyen diğer okuyucuların o konuda okuduğu diğer kitapları öneriyor. Google Trends, işletmelerin tüketici niyetini gerçek zamanlı takip etmesini sağlayan araçlardan biri... Bu aracı kullanan Türk Hava Yolları, söz gelimi bir Türk takımının bir Avrupa ülkesinde yapacağı futbol karşılaşmasının kurası çekildiği gün futbolseverlerin Google arama motorunda yaptığı arama hacmi (örn. İstanbul – Barselona uçak bileti) artışını takip ederek tüketiciler henüz THY web sitesini ziyaret bile etmeden uçak bileti fiyatlarını yükseltmeye başlıyor... Kısaca, dijital mecranın en büyük avantajı atılan her adımın ölçümlenebilmesidir. Yalın yeni girişim (lean startup), yaklaşımı, ölçümleme işinin stratejik inovasyon yönetimi mantığında gerçekleştirilmesini ifade ediyor.

Ölçümlemede sosyal medya takip araçları ve duygu (sentiment) analizi gibi teknikler öyle ilerledi ki, milyonlarca sosyal medya paylaşımı üzerinden analiz yaparak markaların toplum nezdinde tam olarak ne ifade ettiği, rakipleriyle ilişkisi gibi tüm unsurları bir araya getirerek içgörü elde etmeyi sağlayan Marka



Şekil: Marka İlişkisi Haritası: Nike Örneği

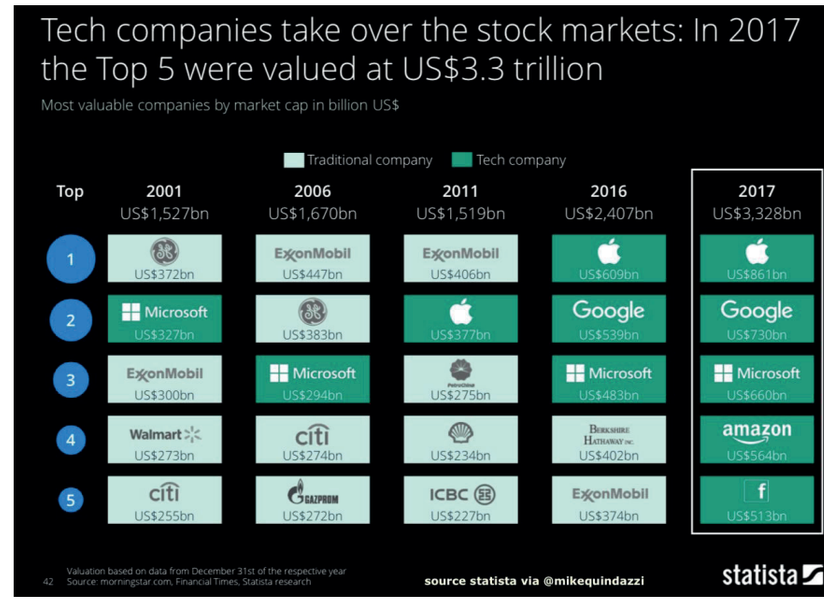
İlişki Haritaları (Brand Association Maps) oluşturmak mümkün...

Dijital İkiz (digital twin), ölçümlemeyi fiziksel nesneler için ve gerçek zamanlı gerçekleştirerek ürün tasarımının, operasyonunun ve kalibrasyonunun optimum hale gelmesini amaçlıyor.

Dijital mecrada farkında olmasak da bıraktığımız parmak izimiz öylesine değerli ki Facebook'un tüm gelir modeli, elde ettiği kullanıcı verisi üzerine kurulu... Kullanıcılarının her türlü "beğen"isi ve aktivitelerini analiz ederek bireysel bazda "öğrenen" platform işi, kullanıcılarının depresif bir dönemden geçtiğini tespit ederek bu içgörüyü el altından reklam verenlere pazarlamakla suçlanıyor...

Blockchain teknolojisi, internetten ne anlaşıldığını da köklü olarak değiştirecek ölçüde bir paradigma değişikliğini ifade ediyor... Klasik bakış açısıyla bakıldığında internetten bilginin transferi anlaşılıyordu. Bilinen anlamda bilişim altyapısı, müzik eseri, fotoğraf tarzı telife konu dosyaların kopyala/yapıştır mantığıyla istenildiği kadar çoğaltılması engellenemediğinden elektronik ortamda, internet üzerinden güvenilir transferinin gerçekleştirilmesi düşünülemezdi. Ancak eşler arası (peer-to-peer [P2P]) teknolojisini ileri kriptografiyle birleştiren Blockchain teknolojisi, Bitcoin örneğinde olduğu gibi en kritik varlık olan paranın güvenli biçimde transferini mümkün hale getirdi. Akıllı kontratlar (smart contracts) kullanarak paranın ötesinde 'değerlerin' transferini mümkün kılan Blockchain 2.0, internete bakış açısında yeni açılımları beraberinde getiriyor.

Kısaca, proaktif biçimde hareket ederek değişimi algılayan, dijitalleşmenin DNA'sını çözümleyen vizyoner şirketler bilgi çağı olarak karakterize edilen 21. yüzyılda sektör bağımsız biçimde en büyük rekabetçi avantaja sahip olacak. 5-10 yıl gibi kısa bir sürede, dünyanın en değerli şirket sıralamasının baştan aşağı değişip tamamen dijital odaklı şirketlerce domine edilmesi bu durumun en bariz göstergesi.

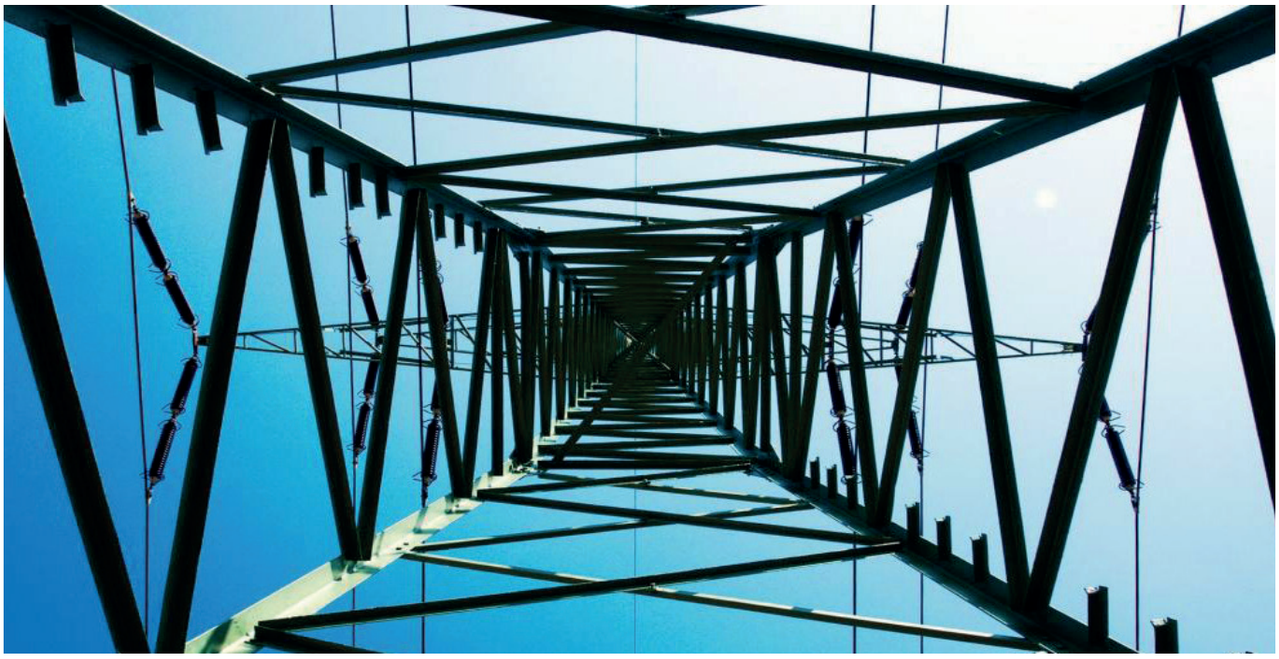


Not: 2001 yılında dünyanın en değerli şirketi olan General Electric, artık ilk sıralarda kendine yer bulamasa da hayatta kalabilmek için misyon ve vizyonunu değiştirmesi gerektiğini fark etti ve artık kendisini yazılım odaklı bir şirket olarak tanımlıyor. 1876 yılında kurulan 140 küsur yıllık bir şirketin misyon ve vizyonunu değiştirmeye ihtiyaç duyması gerçekten dikkate değer…

Kaynak: http://quq.la/oFmMK

KRİPTO PARALARI (ÇEVRESEL AÇIDAN) DAHA SÜRDÜRÜLEBİLİR HALE GETİRMEK

Yazan: Marc Blinder



Blockchain, dünyamızı pek çok açıdan daha iyi bir hale getirme gücüne sahip. Herhangi bir finansal kuruma bağlı olmayan veya bir banka hesabı olmayan kişiler için dijital cüzdan sunuyor, sahteciliği önlüyor ve eski sistemleri daha etkili yeni sistemlerle değiştiriyor. Fakat yine de, bu yeni ve gelişmiş dünyanın, içinde yaşamak istediğimiz dünya olduğundan emin değiliz. En büyük kripto paralar (Bitcoin, Bitcoin Cash ve Ethereum) fonksiyon göstermek için çok büyük enerji tüketimine ihtiyaç duyuyor. Blockchain, geçtiğimiz yıl Uruguay, Nijerya ve İrlanda'nın da içlerinde olduğu 159 ülkeden daha fazla enerji harcadı. Hiç şüphesiz bu, Paris'te yapılan iklim değişikliği anlaşması için bir tehdit oluşturan devasa bir çevre sorunu yaratıyor.

Bu sorun, üzerinde durulmadığı takdirde, böylesi umut verici bir teknoloji için istenmeyen sonuçlar doğuracak. Bu sorunun merkezinde ise "madencilik" yer alıyor. Bitcoin yaklaşık on yıl önce ilk defa ortaya çıktığında meraklı birkaç yüz kişi için, yani "madenciler" için niş bir meraktı. Madenciler, Bitcoin'i regüle edecek bir banka olmadığı için işlemleri doğrulamak amacıyla bilgisayarlarını kullanıyor ve tıpkı karmaşık matematik problemleri gibi, kriptografik problemleri çözüyorlardı. Sonra bu doğrulanmış işlemleri "bloklar" halinde birleştirdiler ve bunları belgelendirmesi için, bu kombinasyonu "blockchain"e (blok zinciri, tüm işlemlerin halka açık kaydı) eklediler. Tüm bunları hepsi, küçük bir miktarda bitcoin içindi. Fakat o zamanlar serbest piyasada tek bir Bitcoin bir peniden az bir fiyata satılırken şimdilerde Bitcoin yaklaşık 7 bin dolara satılıyor. Üstelik günde neredeyse 200 bin Bitcoin işlemi gerçekleştiriliyor. Kripto para "madenleri" yaratma teşvikleri, tıpkı bu rakamlar gibi her geçen gün artıyor. Bitcoin madenciliği çiftlikleri artık dünyanın dört bir yanına yayıldı ve genelde muazzam büyüklükteler. Günün 24 saati matematik problemi hesaplayan 25 bin makinenin harcadığı enerjiyi düşünebiliyor musunuz?

Çevre sorunlarına ek olarak, bu verimsizlik, blockchain'in şirketler için anlamlı bir platform olmasının yolunu tıkıyor. Yüksek enerji maliyetleri sistemin içine işliyor ve network işletme maliyetleri işlem ücretlerine yansıdığı için bu networkleri kullanan kişiler, bu kullanımları için para ödemek zorunda kalıyor. Bitcoin'i kullanan şirketler ilk başta bu finansal sonuçları görmeyebilir. Ancak sonuçlar büyüdükçe maliyetler öldürücü bir darbe niteliğinde olabilir.

Fakat iyi bir haberimiz var: Organizasyonların muazzam enerji masraflarını azaltmasına yardımcı olabilecek çeşitli alternatifler bulunuyor. Şu an için bunlar, hızlıca benimsenmiyor. Suyun üzerinde kalmak isteyen şirketler kendilerini eğitmeli. Aşağıda başlangıç için yararlı olabilecek iki alan sıraladık.

Yeşil Enerji ile Blockchain Madenciliği

Bu sorunları hızlıca çözebilecek uygulamalardan biri, güneş enerjisi ve diğer yeşil enerji kaynaklarıyla madencilik yapmak. Teksas, dünyada güneş enerjisiyle çalışmayan tüm santralleri değiştirmemiz için gerekenden daha fazla güneş enerjisini her gün tek başına karşılama gücüne sahip. Kripto madenciliğini yalnızca temiz, yenilenebilir enerji kullanan bitcoin madenciliği çiftliklerinde yapmak için çok sayıda ticari hizmet mevcut. Örneğin Genesis Mining, bitcoin ve ethereum madenciliğini bulut üzerinden yapma olanağı sağlıyor. İzlanda merkezli şirket yüzde 100 yenilenebilir enerji kullanıyor ve şu an, dünyadaki en büyük madencilerden biri.

Geleceğin blockchain'leri için de yeşil enerjiyi teşvik etmeliyiz. Blockchain kullanan her şirket aynı zamanda, madenci ücreti için kendi sistemini belirler. Yeni blockchain'ler madencilere, yeşil enerji kullanmaya ve en sonunda çevreyi kirleten madencileri saf dışı bırakmaya yönelik daha iyi teşvikler ve daha çok kripto para sunabilir. Aynı zamanda tüm madencileri yeşil enerji kullandıklarını kanıtlamak zorunda bırakarak, kullanmayanlara ödeme yapmayı reddedebilir.

Enerji Tasarruflu Blockchain Sistemleri

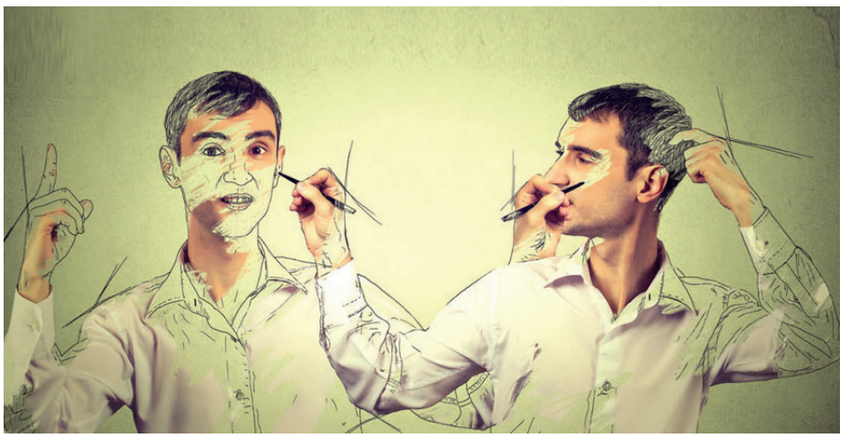
Bitcoin, Bitcoin Cash ve Ethereum'un üçü de fonksiyon gösterebilmek için "Proof of Work" (PoW) denilen, enerji tüketen kriptografik problem çözümünü kullanır. Yeni birçok blockchain de pazar teşviklerine dayanan "Proof of Stake" (PoS) sistemlerini kullanır. PoS sistemlerindeki server (sunucu) sahiplerine "doğrulayıcılar" denir, madenci değil. Bir depozito veya "hisseye" büyük miktarda kripto para koyarlar ve karşılığında blockchain'e blok ekleme hakkı elde ederler. PoW sistemlerinde madenciler birbirleriyle yarışarak, ödül için en hızlı biçimde kimin problem çözebileceğini görmeye çalışırlar. Bu durum, çok fazla enerji tüketir. Fakat PoS sistemlerinde doğrulayıcılar, "hisselerini" hesaba katan bir algoritmayla seçilir. Rekabet faktörünü denklemden çıkarmak enerji tasarrufu sağlar ve bir PoS sistemindeki her makinenin problemlerle teker teker uğraşmasını sağlar. PoW sistemlerinde ise çok sayıda makine aynı problemi çözmeye çalışır. Buna ek olarak eğer bir doğrulayıcı dürüst biçimde hareket etmezse networkten çıkarılabilir. Bu, PoS sistemlerinin doğru ve kesin olmasını sağlar.

Aynı şekilde umut vadeden başka bir sistem ise, bir ölçüde temsilî bir demokrasi gibi operasyon gösteren Delegated Proof of Stake sistemidir (DPoS). DPoS sistemlerinde kripto para jetonları olan herkes, hangi sunucuların blok üreticileri olacağı ve blockchain'i bir bütün olarak yöneteceği konusunda oy hakkına sahiptir. Fakat bunun bir dezavantajı var. DPos, PoW sistemlerine kıyasla sansüre daha az dirençlidir. Teoride sadece 21 blok üreticisine sahip olduğu için bu ağ, eşzamanlı çağrılar veya işlemi bırakma emirleri ile durdurulabilir. Bu durumda Ethereum'daki binlerce nod'a karşı daha savunmasız bir hale gelir. Fakat DPoS, daha az enerji tüketerek daha hızlı biçimde işlemleri gerçekleştirir. Bu, sektör olarak razı olmamız gereken bir ödünleşim.

En büyük kripto paralardan Ethereum, hâlihazırda PoS sistemine geçmeye çalışıyor. Bu hareketi hızlandırmak için daha çok kolektif aksiyon almalıyız. Geliştiriciler yeni PoW blockchain'ler yaratmadan önce oturup düşünmeli; zira başarıları artıkça çevre üzerine yapabilecekleri olumsuz etkiler de artacak. 10-20 yıl önce araba şirketleri bir araya gelip emisyon standartları koyacak bilgeliğe sahip olsaydı, ne olurdu düşünebiliyor musunuz? Bu, daha sağlıklı bir gezegen oluşturmaya yardımcı bir gelişme olurdu ve milyar dolarlık maliyetlerin önüne geçebilirdi. Blockchain sektörü şu an benzer bir dönüm noktasında. Sorulması gereken soru ise şu: Bizden önce gelen ve dünyayı değiştiren sektörlerden daha zeki olabilecek miyiz?

Kaynak: http://quq.la/1eTqJ

ENDÜSTRİYEL IOT'NİN DOĞAL SONUCU: DİJİTAL İKİZ



"Dijital ikiz" kavramının ortaya çıkışı 2001 yılına kadar dayansa da, bu alandaki uygulamalar yavaş yavaş ortaya çıkmaya başladı. Şu anda ağırlıklı şekilde imalat sanayinde kullanılan dijital ikiz, yakında başka sektörlerde karşımıza çıkacak.

Dijital ikiz en basit ifadeyle fiziksel bir ürünün sanal sunumu olarak tanımlanabilir. Diğer bir anlatımla gerçek olarak davranacak şekilde modellenmiş olan bir nesnenin sanal kopyası da denebilir. Bu teknolojiyi baştan sona kadar ürün tasarımı ve montaj sürecinin gerçekte aynısını yapma şeklinde de değerlendirmek mümkün. Kavram ağırlıklı şekilde endüstriyel nesnelerin interneti (IoT) bağlamında kullanılıyor. Şöyle açıklayabiliriz: Ürün tasarım, simülasyon, takip, optimizasyon ve servisi alanlarında dijital ikiz, endüstriyel IoT'nin yardımına koşuyor. Dijital ikiz, tasarımcı ve mühendislerin ürün geliştirmenin ilk aşamalarında kullandığı aynı bilgisayar destekli tasarım (CAD) ve modelleme yazılımlarında oluşturuluyor. Terimi ilk kez kullanan isimlerin başında gelen Ürün Yaşam Döngüsü Yönetimi isimli kitabın yazarı Michael Grieves'e göre, dijital ikiz için üç etmen gerekiyor: İlk sırada, ürünün gerçek ortamdaki hali, sanal ortamdaki hali ve bu iki hali birbirine bağlayan veriler. Aradaki bağlantıyı sağlamak içinse sensörlere ihtiyaç var. Ürüne bağlanan sensörler, gerçek üründeki verileri toplayarak dijital ikizine gönderiyor. Bu sayede sağlanan etkileşimle de ürünün performansında iyileştirmeler sağlanıyor. Şöyle bir örnekle durumu açıklayabiliriz: Bir otomobilin yağının değiştirilmesi gerektiğinde, bu bilgi araç sahibinin akıllı telefonunda veya imalatçının ürün yaşam döngüsü sisteminde bindirilmiş görüntü şeklinde görünüyor. Alet üreticilerinden Black&Decker gibi bazı firmalar dijital ikiz kavramını montaj hattı ve diğer fabrika sistemleri kapsayacak şekilde genişletmeye gidiyor.

Kaynak: http://quq.la/teJZC

Dijital İkizde Süreç Planlama

Tasarım: NX isimli ürün geliştirme yazılımı ve diğer CAD sistemleri kullanılarak ürünün bir modeli oluşturup görüntülenebilir. Bu yazılım saniyeler içinde ürünün binlerce varyasyonunu sanki fiziksel olarak geliştirilmiş gibi oluşturabiliyor.

Süreç Planlaması: Digital Twin teknolojisi, yapılması gerekenler ve bunların nasıl ve nerede yapılacağının tayin edilmesinde daha iyi bir planlama yapılabilmesi için tasarım ve imalat çalışanları arasındaki işbirliğini geliştirir.

Düzenleme: Üretim bölümü düzeni ile Digital Twin'in tüm mekanik, otomasyon ve kaynak detaylarında yaratılması ve ürün tasarım ve imalat eko sistemine ayrılmaz bir şekilde bağlanması önerilir. Ürün yaşam döngüsü araçlarının bir kombinasyonu kullanılarak, hücrelere, ekipmana ve personele kolayca hareket verip operasyonları simule edebilirsiniz. Süreç Doğrulaması: Bu adımda, Digital Twin montaj süreçlerinin doğrulamak için kullanılabilir.

Verimlilik Optimizasyonu: Digital Twin ayrıca planlanmış üretim sisteminize ulaşmak ve istatistiksel olarak simule etmek için de kullanılır. Digital Twin; insan gücünü mü, robotları mı yoksa ikisinin bir kombinasyonunun mu kullanılması gerektiğinin de değerlendirmesinde size yardımcı olur.

2050 ÖNGÖRÜSÜ: İNSAN BOTNETLER VE HACKLENEBİLEN HAFIZALAR

Dünyanın 2050 yılında ait öngörüler arasında çipli beyinler, hacklenebilen hafızalar ve insan botnetler var.

Earth 2050, insanlığın karşılaşabileceği küresel sorunları tanımlamak ve bunların olası çözümlerini belirlemek amacıyla önümüzdeki 30 yıl içinde gerçekleşebilecek sosyal ve teknolojik gelişmeler hakkındaki tahminleri bir araya getiren, ödüllü bir interaktif multimedya projesi. Kaspersky Lab'ın 20. kuruluş yıl dönümünde açılan web sitesinde birçok farklı konuyu ele alan çeşitli tahminler, gelecek senaryoları ve daha fazlası yer alıyor.

Son olarak siteye katkıda bulunan isimlerin arasına yenileri katıldı. Bunlar arasında İngiltere Kraliyet Astronomu, Cambridge Üniversitesi'nde Profesör ve Royal Society Başkanı olan Lord Martin Rees, yatırımcı ve girişimci Steven Hofman, insan hakları savunucusu Peter Tatchell'in yanı sıra Kaspersky Lab güvenlik araştırmacısı Dmitry Galov ve zararlı yazılım analisti Alexey Malanov bulunuyor.

2050 için ortaya konulan yeni görüşler arasında şunlar yer alıyor:

- Beyne yerleştirilen çipler sayesinde düşünce ile çalışan doğrudan bağlantıların mobil cihazların yerini alması. Bilgi ve beceri de yüklenebilen bu çiplerin bireysel bilinç ve düşünce gizliliğine etkisi.
- Gen düzenleme ile tüm canlıları genetik düzeyde değiştirebilme becerisi.
- Gelişmiş makine öğrenimi/yapay zeka sistemlerinin yaptığı hataların potansiyel etkileri.
- Mevcut politik sistemlerin gerilemesi ve sıradan insanların kanunlara onay verme yetkisine sahip olduğu 'vatandaş hükümetlerinin' yükselişi.
- Fosil yakıtların tükenmesiyle

tekno-endüstriyel çağın sona ermesi. Bununla birlikte ortaya çıkacak ekonomik ve çevresel çöküş.

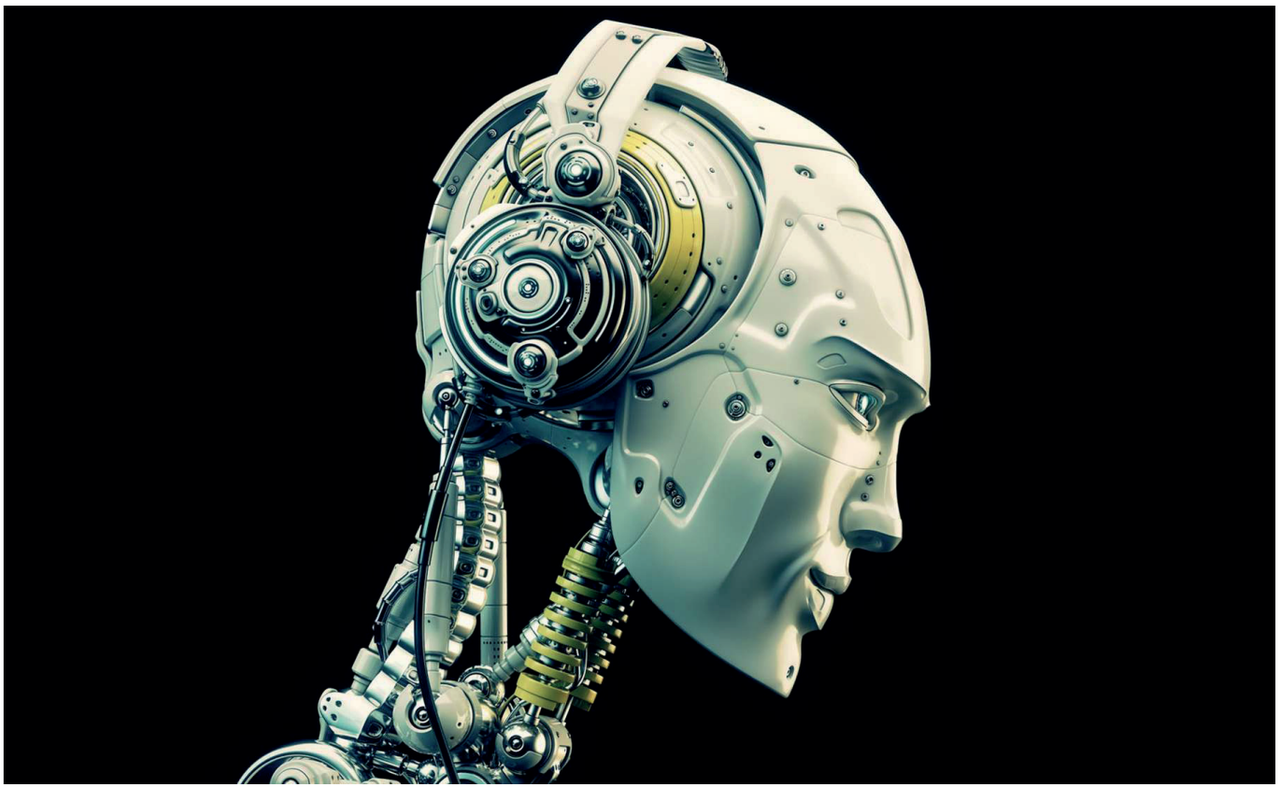
- Çoğu insanın vegan olmasıyla endüstriyel ölçekli et üretiminin sona ermesi ve ve etin açık alanda yetişen canlı hayvanlardan alınan biyopsi yoluyla üretilmesi.
- Yeni Bilgileri Öğrenmek Hızlanacak

Kaspersky Lab güvenlik araştırmacısı Dmitry Galov'un 2050 tahminleri ise şöyle: "2050'ye geldiğimizde, beynimizin nasıl çalıştığına dair bilgimiz ve beyni onarma becerimiz o kadar gelişecek ki her şeyi hatırlamak ve yeni şeyleri inanılmaz bir hızda öğrenmek normal hale gelecek. Çoğu çocuğa öğrenme becerilerine destek olmak için en yeni bellek geliştirme çipleri takılacak ve bu da eğitimi daha önce hiç olmadığı kadar kolay hale getirecek. Kafa yaralanmaları nedeniyle oluşan beyin hasarı kolaylıkla onarılabilecek, hafıza kaybı artık bir sorun olmaktan çıkacak ve depresyon gibi akıl hastalıkları hızla tedavi edilecek. Bunların temelini oluşturan teknolojiler 2010'ların sonundan beri mevcut. Bellek çipleri aslen 2018'deki derin beyin uyarı çiplerinin doğal bir uzantısı.

Siber Saldırıyı Açık Beyinler ve Hafızalar

Ancak her teknolojinin bir de karanlık yüzü var. 2050'de bellek geliştirici çiplerin tıbbi, sosyal ve ekonomik etkileri büyük olacak fakat bunlar aynı zamanda siber saldırılara da açık olacak. Bunların sonucunda ortaya çıkacak yeni tehditler arasında, politik olaylar veya anlaşmazlıklara dair anıların eklenmesi veya çıkarılmasıyla geniş insan gruplarını toplu bir şekilde etki altına almak gibi durumlar bulunacak. Hatta 'insan botnetler' bile oluşturulabilecek. Bu botnetler insanların beyinlerini, siber suçlular tarafından kontrol edilen bir ağ şeklinde birbirine bağlayabilecek. Kurbanların bundan haberi bile olmayacak.

Önceki yıllarda görülen siber tehditler yeni amaçlar edinerek siber casusluk için dünya liderlerinin hafızalarını hedef alacak. Ayrıca hafızalarını çalmak, silmek veya kilitlemek (örneğin fidye için) amacıyla ünlü kişiler, sıradan insanlar ve şirketler de hedefte olacak. Bu tehditlerin mümkün olmasının sebebi, bu teknolojilerin gelişmeye başladığı 2010'lu yıllarda gelecekte karşılaşılabilecek potansiyel güvenlik açıklarına öncelik verilmemesi ve sağlık ve güvenlik sektörleri, kanun koyucular ve diğerlerinin gelecekteki riskleri anlamak ve belirlemek için bir araya gelmiş olmamasıdır."



Kaynak: http://quq.la/VwouI

ALGORİTMALARI KULLANARAK ÖNYARGILARLA SAVAŞABİLİR MİYİZ?

Yazan: Rumman Chowdhury & Narendra Mulani

1971 yılında filozof John Rawls, adalet kavramını anlamak için bir düşünce deneyi yapmayı önerdi: Bilinmezlik perdesi. Rawls, "Eğer beyinlerimizi silebilseydik ve kim olduğumuza dair hiçbir şey hatırlamasaydık (ırkımız, gelir düzeyimiz, mesleğimiz; kısacası fikirlerimizi etkileyebilecek her şey) ne olurdu? Kimi korurduk ve ilkelerimizle kime hizmet ederdik?" sorularını sordu.

Bilinmezlik perdesi, adalet ve toplum ile ilgili felsefi bir düşünce pratiğidir. Fakat gelişmekte olan yapay zekâ (AI) alanına da uygulanabilir. Biz AI sonuçlarını matematiksel ve programa dayalı ve belki de duygu yüklü insan kararlarından daha iyi olmasıyla yerlere göklere sığdıramıyoruz. Peki AI, bizi objektif ve ideal sonuçlara götüren bilinmezlik perdesini sağlayabilir mi?

Bu sorunun cevabı, bizi şimdiye dek hayal kırıklığına uğrattı. Teknolojimizin ne kadar objektif olmasını istesek de teknolojiyi ve onu besleyen veriyi geliştiren kişiler, teknoloji üzerinde büyük etkiye sahip. Teknoloji uzmanları, AI'nın arkasındaki sosyal bağlamdan bağımsız objektif fonksiyonları tanımlamazlar. Veri objektif değildir; önceden var olan sosyal ve kültürel önyargıları yansıtır. AI gerçekte, önyargıları kalıcılaştırma yöntemi olabilir. Bu da istenmeyen negatif sonuçlara ve adaletsiz çıktılara yol açabilir.

Günümüzde çokça konuşulan; istenmeyen sonuçlar ve adil çıktılar konusu, pek de yeni değil. Hatta 1971'de ABD Yüksek Mahkemesi (farklı gruplara eşit şekilde davranıldığı görüntüsü veren tarafsız uygulamaların, gerçekte bir grubu diğerine karşı kayıran veya diğer gruba nazaran mağdur eden etkiler doğurmasına karşılık gelen) "farklı etki" kavramını geliştirdi. Bu, istenmeyen ayrımcılığı incelemek için kullanılan en etkili hukuk teorisiydi. Özellikle Griggs v. Duke Power Company'nin hükmü, niyetten bağımsız olarak, korunan sınıflar (bu durumda istihdam konusunda) için eşit olmayan ve ayrımcı sonuçların, Civil Rights Act of 1964'ün (1964 Medeni Haklar Yasası) 5. Maddesini ihlal ettiğini belirtti. Günümüzde bu hüküm, AI ayrımcılığı potansiyelini incelemek ve istihdam ve barınma kararlarını değerlendirmek için yasal dayanak olarak yaygın biçimde kullanılıyor. Özellikle, "istenmeyen sonuçlar"ın nasıl anlaşılacağı ve bir karar sürecinin sonuçlarının adil olup olmadığını belirliyor. AI düzenlemesi henüz daha ilk aşamalarında; fakat adalet kavramı, olumsuz etkilerin farkına varma konusunda en önemli etken olacak.

AI etiği alanı; disiplinler arası bir grup olan avukatlar, filozoflar, sosyal bilimciler, programcılar ve diğerlerinin ilgisini çeker. Bu topluluktan etkilenen Accenture Applied Intelligence, AI sistemlerinin temel taşı olan algoritmik modeller ve verilerdeki önyargıları anlamak ve ele almak için bir adalet aracı geliştirdi.

Bu Araç Nasıl Çalışıyor?

Geliştirdiğimiz bu araç farklı etkiyi ölçüyor ve eşit fırsat elde etmek için öngörücü eşitlik sağlıyor. Verileri ve modeli araştırarak potansiyel farklı etkiyi açığa çıkarıyor. Bu süreç, var olan veri bilimi süreciyle entegre. Araçtaki ilk adım, veri araştırma sürecinde kullanılıyor. İkinci ve üçüncü adımlar, bir model geliştirildikten sonra meydana geliyor. Şu anki şeklinde adalet değerlendirme aracı sınıflandırma modelleri için işe yarıyor (kullanım alanları arasında, örneğin, birine kredi verip vermeme kararı var). Sınıflandırma modelleri, insanları veya maddeleri benzer karakteristiklere göre gruplandırır. Bu araç, gruplandırmanın adaletsiz bir biçimde yapılıp yapılmadığını belirlemeye yardımcı oluyor ve eğer yapılıyorsa, düzeltmek için yöntemler sunuyor.

Bu aracı kullanırken izlenecek üç adım var:

- İlk kısımda, kullanıcının belirlediği hassas değişkenlerin diğer değişkenler üzerindeki gizli etkisini bulmak için veriler incelenir. Araç her bir değişkenin, modelin çıktısı üzerinde sahip olduğu etkiyi belirler ve ölçer. Bu sayede ikinci ve üçüncü adımlarda hangi değişkenler üzerine odaklanılacağı belirlenir. Örneğin AI, istihdam ve çalışan değerlendirmede yaygın olarak kullanılır. Fakat yapılan çalışmalar, cinsiyet ve ırkın hem maaş ile hem de kimin terfi ettirildiğiyle ilgisi olduğunu ortaya koyuyor. İK organizasyonları, bu araçları kullanarak iş rolleri ve gelir gibi değişkenlerin insanların ırk ve cinsiyetinden bağımsız olmasını sağlayabilir.
- Aracın ikinci kısmı, hassas bir değişkenin farklı sınıflarındaki model hatalarının dağılımını araştırır. Erkek ve kadınlardaki hata terimlerinde dikkat çekici ölçüde farklılık gösteren bir kalıp varsa (bu araçta görselleştirilir) bu, sonuçlar üzerinde cinsiyetin etkili olduğunu gösteren bir belirtidir. Geliştirdiğimiz araç, istatistiksel bozulma uygulayarak hata terimlerini düzeltir. Yani, hata terimleri farklı gruplar arasında daha homojen bir hale gelir. Düzeltme derecesine ise kullanıcı karar verir.
- Son olarak, araç farklı gruplardaki yanlış pozitiflik oranını inceler ve tüm gruplarda kullanıcının belirleyeceği eşit bir yanlış pozitiflik oranı sağlar. Yanlış pozitif oranlar, hata modelinin özel bir şeklidir: Cevap "hayır" olmalıyken model çıktısının "evet" dediği örnekler. Örneğin, eğer bir kişi düşük kredi riskine sahipse, kredi almışsa ve sonrasında bu krediyi ödeyemeyip mali acze düştüyse bu, yanlış pozitiftir. Bu model, kişinin düşük kredi riski olduğunu öngörmüş ve yanılmıştır.

Adaleti sağlamak için düzeltme yaparken modelin doğruluk hassasiyetinde bir düşüş gözlenebilir. Araç, bunun sebep olabileceği tüm değişiklikleri gösterir. Doğruluk hassasiyeti ve adalet arasındaki denge, bağlama bağlı olduğu için, ödünleşimi belirleme konusunda kullanıcıya güveniriz. Aracın bağlamına bağlı olarak; doğruluk hassasiyetini optimize etmekten ziyade, eşitlikçi çıktılar sağlamak daha yüksek bir öncelik olabilir.

Bu aracı geliştirirken bir önceliğimiz, günümüzde rekabetçi organizasyonların kullandığı çevik inovasyon süreciyle uyumlu olmaktı. Bu yüzden aracın büyük miktarlarda veriyle başa çıkabilmesi ve bu sayede organizasyonların uygulanabilir AI projelerini ölçeklendirmesine engel olmaması gerekiyordu. Aynı zamanda ortalama bir kullanıcı tarafından da kolaylıkla anlaşılabilmeliydi. Üstelik mevcut veri bilimi iş akışlarıyla birlikte operasyon gösterebilmeli ve böylece inovasyon sürecini engellememeliydi.

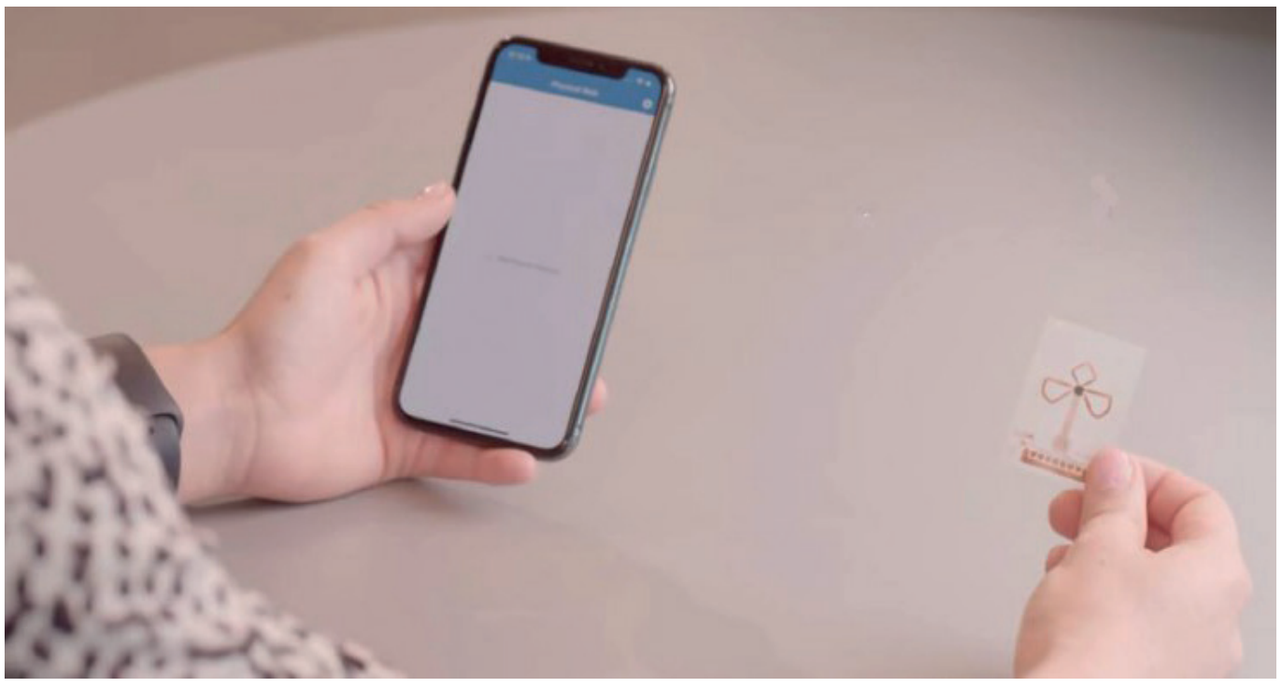
Geliştirdiğimiz bu aracın yapabildikleri, neyin adil olduğunu söylemenin ötesinde. Bu araç hassas değişkenler, hata terimleri ve yanlış pozitif oranlar tanımlaması gereken kendi kullanıcılarının belirlediği parametreler içinde önyargıları değerlendiriyor ve düzeltiyor. Bir organizasyon; paydaşlarıyla güven tesis etmek, şirketlerin karşı karşıya kaldığı riskleri tersine çevirmek ve topluma değer katmak için AI'yı kullanırken, bizim Responsible AI (Sorumlu AI) dediğimiz temel prensipleri izler. Bu kararlar, bir organizasyonun Sorumlu AI'a karşı nasıl bir anlayış geliştirdiğiyle kontrol edilmelidir.

Aracın başarısı sadece algoritmaları iyileştirmek için çözümler sunmaya değil, aynı zamanda çıktıları açıklama ve anlama yeteneğine de dayanır. Bu araç, veri bilimciler ile veri bilimci olmayanlar arasında daha kapsamlı bir iletişim sağlamak için geliştirildi. İnsan-makine işbirliğinde otomasyondan ziyade insan bağlılığını önceliklendiren bir araç geliştirmekteki amacımız, adalet tartışmasını AI gelişiminde eyleme geçirilebilir etik uygulamalara taşımak.

Kaynak: http://quq.la/JHEpx

PİLSİZ BLUETOOTH ETİKET SENSÖRÜ

Pilsiz etiket sensörü gücünü radyo frekanslarından topluyor. Wiliot, giysilerinize ve yiyeceklerinize bu etiketi kullandırabilir.

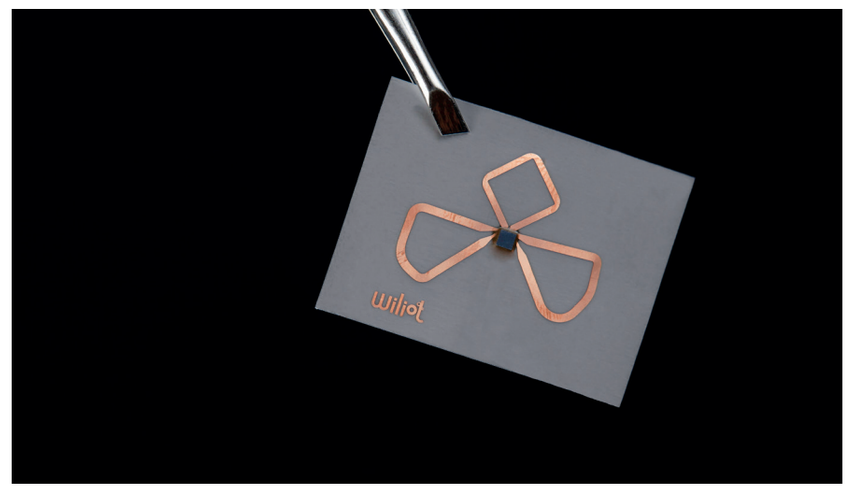


Akıllı sensörler, akıllı etiketlerler nesnelerin internetinde oldukça önemli bir rol üstlenmektedir. Elbette su sensörlerin çalışması için bir bataryaya ya da göze çarpan başka bir enerji kaynağına ihtiyaçları var. Ancak yakında yalnızca havadan enerji toplamak zorunda kalabilirler.

Wiliot, ister Bluetooth, ister hücresel veya Wi-Fi olsun, ortamdaki tüm radyo frekanslarından enerji toplayabilen bir Bluetooth Etiket Sensörü duyurdu. Tüm ARM bazlı çip kağıt ve plastik üzerine basılmış bir antenden ibaret ve herhangi bir batarya kullanmadan ağırlık ve sıcaklık gibi bilgileri iletebilir.

Bu pilsiz yeni yaklaşım, ürünlerdeki benzer çipli etiketlere yeni bir alternatif olabilir. Üstelik maliyetleri de daha aza indirebilir.

Yeni pilsiz bluetooth etiketler 2020 yılına kadar hazır olacak. Ancak bu zamana kadar Amazon, Samsung gibi teknoloji devlerinden yatırım almak için turlara çıkacak. Teknoloji devleri bu teknolojinin başarılı olmasını istiyor ve bu etiketler hazır olduktan sonra oldukça yaygın bir şekilde kullanıldığını görebiliriz.



Kaynak: http://quq.la/8fx8w

BAĞIMLILIK YARATAN DENEYİMLER: TASARIM TEKNİKLERİ VE FARKINDALIKLA KULLANIMI

Yazan: Ercan Altuğ Yılmaz

Tristan Harris belki de tüm dünyada her geçen gün artan 'ekran bağımlılığı' üzerine dikkat çekmeye çalışan ilk kişi değildi ancak bu deneyimleri yapmak üzere tüm taktikleri bilen firmanın birinden geliyor ve bu taktikleri tüm 'can yakan' benzetmeleriyle kariyeri pahasına açığa vuran ve basit tüyolar ile de çözümler öneren ilk kişilerden.

Geçtiğimiz aylarda ABD ana akım medya kanallarından biri olan CBS'teki 60 minutes adlı programın tanıtımlarında oldukça genç yaşlarında olan birisi elindeki akıllı telefonunu sallayarak, "Bu bir telefon değil slot (kumar) makinesi" diyordu.

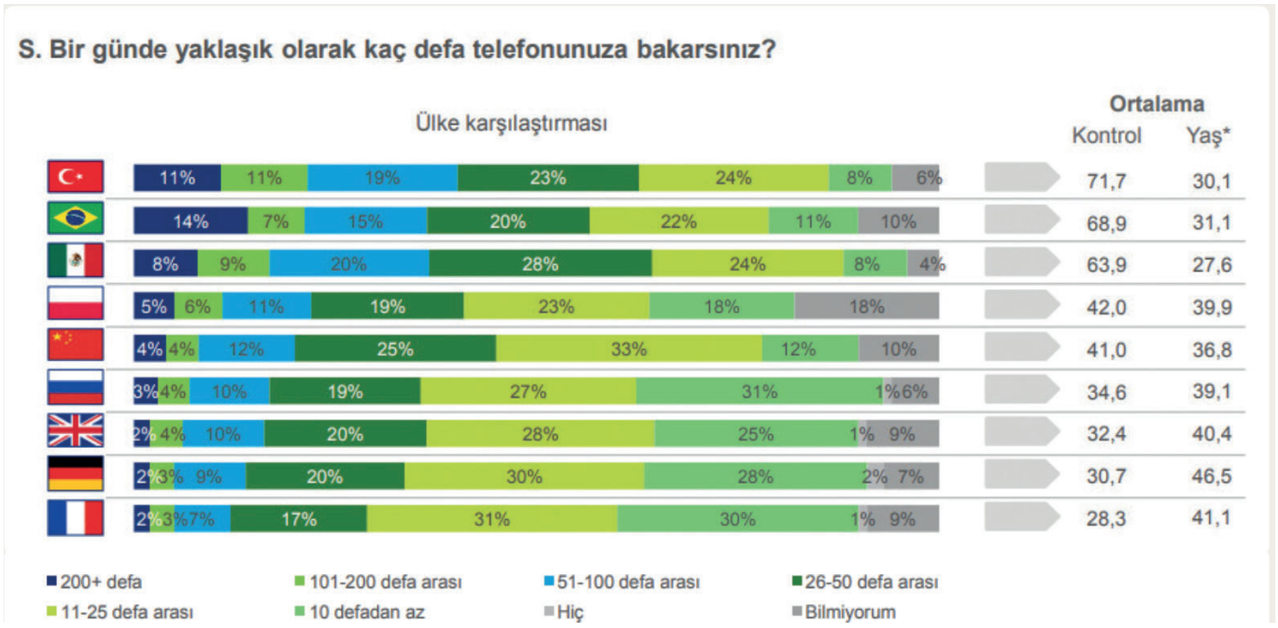
Görenlerin ilgisini üzerine çekmeyi hedefleyen eski Google Ürün Yöneticisi Tristan Harris, aslında bu giriş cümlesiyle oldukça başarılı olmuştu. Tristan Harris, Google şirketinin e-posta servisi olan Gmail ürününün mobil uygulamasından sorumluyken mobil cihazlardaki Gmail App'ini nasıl daha çok kullanılmasına (bağımlı gibi) kafa yoruyordu. Bir anda yapmaya çalıştıkları şeyin doğru olmadığı ve tam tersi mantıkta, Ben mobil cihazları e-posta servisi de dâhil tüm dijital ürünleri tasarlarken nasıl her e-posta geldiğinde ya da her seferinde daha çok değil sadece ihtiyaç duyulduğunda kullandırtıp devamında en hızlı şekilde geri bıraktırırım," üzerine düşünmeye başladı. Ve çok geçmeden bunu çalıştığı şirket dünyanın sayılı şirketlerinden birisi de olsa bunu o çatı altında başaramayacağını anlayıp Google'dan ayrıldı. Ve günümüzde insanlarda yaş bağımsız her geçen gün artan "ekran bağımlılığı"nı azaltmak üzere "Time Well Spent" adlı kâr amacı gütmeyen girişimini kurdu. Time

Well Spent aslında dikkatlice seçilmiş bir isim çünkü ekran bağımlılığının çözümü bazılarının önerdiği gibi cihazları kaldırıp atmaktan geçemez. Bu cihazlar bilgiye ve daha birçok gerekli işe bağlı olmamazı sağlıyor, ancak farkındalıkla kullanmak ve kullanım sonrası harcadığım süreye değdi diyebilmek işte Time Well Spent'in tam amacı bu: "Time Well Spent- Harcadığım Zamana Değdi" denilebilir.

Tristan Harris belki de tüm dünyada her geçen gün artan 'ekran bağımlılığı' üzerine dikkat çekmeye çalışan ilk kişi değildi ancak bu deneyimleri yapmak üzere tüm taktikleri bilen firmanın birinden geliyor ve bu taktikleri tüm 'can yakan' benzetmeleriyle kariyeri pahasına açığa vuran ve basit tüyolar ile de çözümler öneren ilk kişilerden. Tristan'ın beni etkileyen bir kaç sözüne sizi de etkilemek için örnek verecek olursam bunlardan ilki, "İstatistiksel olarak artık anneler gün içinde yeni doğan bebeklerinden daha çok telefonlarını kontrol ediyor" deyişiyle birlikte "Şirketler, arkalarına yaslanıp milyarlarca insanın kafası kesilmiş tavuklar gibi ortalarda koşuşturarak birbirlerine cevaplar sallayıp minnettar hissetmelerini keyifle seyrediyor " ifadeleri olur.

Günde Ortalama 71,7 Defa Akıllı Telefona Bakıyoruz

Teknoloji firmalarının kalbi Silikon Vadisi'nde ürün yazılımlarında etik konusu son dönemde



oldukça tartışılır oldu, nedeni de aslında çok basit : "Ekranlara tüm yaştan herkes ile bağımlı hale geldik!". Peki, siz bir gün boyunca ne kadar süre bir ekrana bakıyorsunuzdur?

Uluslararası danışmanlık şirketi Deloitte tarafından 2011 yılından bu yana yapılan "Global Mobil Kullanıcı Araştırması"nın 2015 sonuçları yayınlandı.** Türkiye'nin de aralarında bulunduğu 30 ülkeden 49 bin katılımcıyla gerçekleştirilen araştırma, mobil cihaz kullanımının geldiği nokta hakkında önemli veriler sunuyor.

Türkiye'den 18-50 yaş arası 1000 kişinin katılımıyla ortaya çıkan sonuçlara göre Türkiye akıllı telefon bağımlılığının en yüksek olduğu ülke. Türkiye'deki kullanıcılar günde ortalama 71,7 kez cep telefonunu kontrol ediyor, bu da yaklaşık tam 15 dakikada parlak bir ekran yüzü gördüğümüz anlamına geliyor.

Telefondan sıkılınca televizyona, televizyondan sıkılınca tablete geçiyoruz. TV izleme de ne yazık ki, dünya sıralamasında ABD gibi ülkelerle yarışıyoruz ve ortalama 4 saatleri bulmuş durumdayız. Dizi sektörümüzle övünüyoruz ancak tüketicilerimizi ve orada kaybedilen

günün en kıymetli zamanlarını TV izlemekten daha verimli geçirmeyi ne zaman düşüneceğiz?

Peki, bu böyle daha ne kadar devam edecek? Yapabilecek gerçekten hiç bir şey yok mu? Öncelikle hastalığa teşhis koymak lazım. Bu dijital ürünler nasıl bağımlılık yaratıyor?

New York Üniversite'sinden Adam Alter da bu yılın başında çıkan 2017 yılının en çok satanlar listesinde üst sıralarda yer alan kitabı 'Irresistible: The Rise of Addictive Technology and the Business of Keeping Us Hooked" karşı koyulmaz bağımlılık yaratan uygulamaların nasıl taktiklerle tasarlandıklarını bazı madde ve örneklerle sıralamış. Bunlardan bazıları: Goals (Hedefler), Feedback (Geri bildirim), Progress (İlerleme durumu), Escalation (Seviye yükselme), Cliffhangers (Hikâyenin en heyecanlı kısmında kesmek), Socialize (Sosyalleşme) ve Gamify (Oyunlaştırma, Puan, Rozet, Avatar gibi tasarımlar) olarak adlandırılıyor.

Nir Eyal'in Kanca Modeli

Buradaki uygulama tasarım taktikleri insan davranışlarını çok rahat yönlendirdiğini ve bunu teknoloji firmalarının artık çok başarılı bir şekilde yapabildiği için firmalar tarafında bazı regülatif etik kontrol listeleri ve devlet üzerinden de kısıtlamalara gidilmesi gerektiğini belirtiyor. Bunu da ünlü ekonomist Malcolm Gladwell'le olan bir söyleşisinde eski zamanlardan örnekleyerek şu şekilde anlatıyor: " Antik çağlarda krallar bile halkın arasında esrar içerdi ancak şuanda komple yasaklandı ve kontrol altında. ABD'nin yaklaşık 50 yıl önce yüzde 80'i sigara içiyordu, yakın zamana kadar otobüsler de dâhil her yerde serbest içiliyordu. Ancak şu an devlet tarafından kontrollü bölgelerde satılıp içiliyor ve kullanım oranı oldukça düştü. Telefon gibi teknolojik cihazlarda da yaş, süre ve lokasyon (tech-free area) gibi kısıtlamalar getirilmeli." diyor. Adam Alter uyarılarında gerçekten çok haklı ama ya önerilerinde? Biz tüketicilerin kitabının isminde de olduğu gibi 'Karşı konulamaz' durumda kalmamız ve yapacak hiçbir şeyimiz olmadığından bahsederek burada sorumluluğu şirketlere ve devletlere yönlendiriyor. Gerçekten öyle mi? Bizim bu cihazlara karşı yapabileceğimiz hiçbir şey yok mu ve bu ekran bağımlılıkları devletler ve şirketler tarafından "izinli pazarlama" benzeri bir "etik tasarım sözleşmesi" yayınlama gibi bir müdahaleye kadar bekleyecek miyiz?

Bu soruların cevabını Silikon Vadisi'ndeki firmalara nasıl bağımlılık yaratan uygulamalar tasarlama konusunda Hook (Kanca) isimli kendi oluşturduğu modelle danışmanlık veren birisi olan Nir Eyal'den almaya çalışalım.

Teknoloji şirketleri asla durmayacaklar, daha da gelişecekler ve daha kolay bağımlı hale getiren deneyimler tasarlayacaklar. Biz insanlar nasıl daha lezzetli ve renkli kurabiyeleri gördükçe daha çok yemiyor ve irademizle az tüketiyorsak aynen bu yeni cihazlarla da ilgili yine teknolojinin bağımlılığı azaltıcı iyi tasarlanmış uygulamalarıyla bunu çözmeliyiz diyor. Kendisiyle yeni kitap projem için yaptığımız Nir Eyal'le video röportajımda Antalya'da yaptığı yakın zamandaki bir tatilinde 'simit'e bağımlı hale geldiğini tüm gün otelde simit yemeğe başlayınca bu davranışına müdahale etmek zorunda kalmış. Eyal, "Türkiye'de yaşasaydım eminim kebap, döner, baklava, lokum ve birçok yemek yeme davranışlarıma müdahale etmem gerekirdi" dedi. Türk yemekleri dünya mutfağının Instagram'ı, Snapchat'i demek ki!

Nir'e söyleşimizde oyunlaştırmanın ekran bağımlılığına nasıl çözüm olabileceğiyle ilgili konuşurken bir anda eline Adam Alter'in kitabını alıp, "Eğer insanlara 'siz güçsüzsünüz ve karşı koyamazsanız' derseniz insanlar da buna inanır ve bu sorunlar çözülemez. Oyunlaştırma da dâhil kullanıcı tarafında yapacak çok işimiz var." demesi röportajın benim için en sürpriz ve etkileyici anlarındandı.

Ekran Bağımlılığyla İlgili Teknik ve Uygulamalar

Evet, "ekran bağımlılığı" sorununu teknolojik cihazlar buldu yine onların yardımıyla çözmek üzere bazı teknikler ve uygulamaları size listeleyeceğim. Önce Tristan Harris'in web sitesinde www.timewellspent.io/

take-control yayınladığı bazı küçük ve ama etkili önerilerle başlayalım.

- Push notification – uyarı ayarlarınızı minimuma indirin ve sadece insanlardan (istediğiniz) gelenlere izin verin.
- Mobil uygulama yerine tarayıcıdan mobil sayfasını kullanın. Bazen deneyimi zorlaştırmak bağımlılığı azaltır. Hem cihazınızdaki yerden tasarruf edin hem de şarj kullanımından büyük kazanç sağlayın. Hem istediklerinde push gönderemezler, siz istediğinizde girip güncellemeleri menüden görebilirsiniz.
- Telefon ayarlarınızı bir süreliğine siyah-beyaz getirin. Özellikle görsel odaklı sosyal medyalara bağımlılığınız varsa o zevki çok hızla azaltacaktır. Nasıl yapılıyor derseniz genelde Erişilebilirlik menüsü altında oluyor. iOS için adım adım: Ayarlar > Genel > Erişilebilirlik > Ekran Ayarları > Renk Filtreleri'ne gidin.
- Bağımlılık yapan uzun süre harcadığınız mobil uygulamaları ana ekranda tutmayın, bir klasöre koyup son ekranda tutun ve ilk zamanlar üst arama çubuğuna yazarak ulaşmayı alışkanlık haline getirmeye çalışın.

Taktikler güzel olmakla biraz farkındalıkta istediği için biraz daha davranışçıl ve otomatik yapan bazı uygulamalar da paylaşacağım. "Ölçülebileni ölçün, ölçülemeyeni ölçülebilir hale getirin." diyen Galilelo'nun izinde aslında her şey önce farkında olmak için ölçümlemekle başlar diyerek ekran kullanımlarınızı ölçümleme yapan uygulamalarla başlayalım:

Moments

Mobil cihazınızda hangi uygulamada ne kadar süre harcıyorsunuz Moments bunu size detaylı bir raporla sunuyor. Tabii ki, bu veriler sizin farkındalığınızı artırmak için yetmezse Telefonu 30 dakika bir yere koy, tüm akşamı telefonsuz geçir, bir gün notification'larını kapa, ana ekranını sadeleştir gibi görevler de vererek bu süreyi azaltmanızı sağlamaya çalışıyor. Zaten uygulama Tristan Harris tavsiyeli ve çok agresif bir dili var: 'Telefonu şimdi bırak ve hayata geri dön!

Rescue Time

Bilgisayarınızda hangi uygulamada ne kadar zaman harcıyorsunuz bilmek ister misiniz? Rescue Time ile kullandığınız uygulamaların tipine göre hangisinde ne kadar zaman harcıyorsunuz görebiliyorsunuz. Merak etmeyin otomatik kategoriler alsa da mesela Facebook'ta bir şirketin hesabını işiniz gereği yönetiyorsanız Facebook'un kategorisini Social Networking'ten Business'e taşıyabiliyorsunuz.

Checky App

Gün içinde sizce cep telefonunuza kaç kere bakıyorsunuz? Checky bu rakamı sizin için ölçüyor ve haftalık olarak arşivleyerek sizi azaltmanız için mini bir oyunlaştırma yapmak üzere meydan okuyor. Ayrıca lokasyonuna da izin verirseniz özellikle işte veya evde daha çok telefonunuza sarılıyorsanız öğrenebilir ve ona göre bir harekete geçebilirsiniz.

Space App

İngilizce 'instant gratification' diye bilinen 'anlık tatmin' olarak Türkçe'ye çevirebileceğimiz konuya çözüm olmaya çalışan Space App – yüklendikten sonra herhangi belirleyeceğiniz bir uygulama açılmadan size 10 saniye nefes aldırıyor ve meditasyon yapmanızı sağlıyor. Bu arada ufak mesajlarla gerçekten bu uygulamayı mı kullanmalısın yoksa sadece sıkılıp 'anlık tatminin' için mi açtığını düşündürüyor. Zaten 'anlık tatmini' o anda geçen kullanıcıların uygulamaları kullanım süreleri çok dramatik şekilde düşüyormuş. Siz de canınız sıkılınca açtığınız ilk verimliliğinizi olumsuz etkileyen uygulama hangisi takip edin ve onun üzerine bir Space verin.

Freedom

Bu uygulama gerçekten ilk duyduğumda beni çok şaşırtmıştı. Nir Eyal bir konuşmasında kitap yazarken Word'u açar açmaz evdeki tüm cihazlarda in-

terneti kesen bir yazılım olarak bahsetmişti Freedom'dan. Devamında da kitap yazması bitince otomatik olarak internete bağlanmayı da ayarlayabiliyorsunuz. Evet Freedom – yani Özgürlük uygulaması artık her an bağlı olduğumuz ve bize kanca takan internet uygulamalarından kurtulmayı istediğimiz an bize yardımcı olan bir uygulama. Daha da ilginci 7 kullanımdan sonra ücretli bir uygulama. Evet para ödeyerek eve bağladığınız interneti kesmek için yine para ödemek. Bu arada aslında ability-yapabilme konusu devreye giriyor ve BJ Fogg'u yine anıyoruz.

Focus App

Focus uygulaması Macintosh'lara özel ancak aynı Freedom gibi bilgisayarın belli süreli olarak yazı yazdığınız anda devreye girerek e-posta, sosyal medya ya da network'ten çıkacak notification'ları belli bir süre engellemenizi sağlıyor. Macintosh'u olanlar ve bir şeyler yazmaya niyetlenip her seferinde yarıda bırakanlar mutlaka denesinler. Bu uygulamada hoşuma giden ise mesela Instagram'a girmeye çalıştığında 'Vakit nakittir' gibi quato denilen özlü sözleri ilgili sitelere ekleyerek karşınıza çıkarıyor bence muazzam fikir!

Forest App

Forest uygulaması gerçekten bu konuda gördüğüm en ilginç ve gerçek hayata dokunan oyunlaştırılmış uygulama. Odaklandığınız süreyi mesela 90 dakika diye seçiyorsunuz ve telefonunuz o anda sanal bir ağacı büyütmeye başlıyor, telefona mesela Tumblr'dan bir notification geldi ve 90 dakika içinde ona tıklayarak açarsanız o ağaç kuruyor. Her gün hedeflerinizi tutturursanız uygulamanın adına da referans olarak ağaçlarınız bir ormana dönüşüyor ve Senegal'de TheTrees.org sosyal girişimi üzerinden sizin adınıza gerçek bir ağaç bağışlanıyor. Müthiş değil mi?

Özellikle ebeveynlerin çocuklara bunun bir oyun olarak iletişimini kurması için de özel yemeklerde herkes telefona gömülmesin diye Forest uygulaması bazı iletişim görselleri de hazırlamış çok çok hoşuma gitti.

Samsung Marshmallow

Sadece Samsung cihazlarda ve bir süredir Türkiye'ye açık olmayan ancak özellikle ebeveyn üzerinden çocukların sosyal medya, oyun ve internet bağımlılıklarını azaltmaya yönelik bir uygulamadan bahsetmek istiyorum : Marshmallow adı da ünlü çocuklar üzerinde uygulanan haz geciktirme testi olan Marshmallow testinden almış olan uygulama hem yüklendiği tablette hem de tanıttığınız evdeki diğer tabletteki uygulamalara kullanım süre hedefleri vermenizi sağlıyor. Bu hedefler aynı okullarda da uygulanan aylık çizelge üzerine atılan gülen yüzler gibi tutuldukça rozetlere dönüyor ve tüm ay hedefler tutulunca isterseniz Amazon'dan hediye çeki, Google Play'den kredi gibi ödüller yükleyebiliyorsunuz. Belki biraz dışsal ödüller ancak en azından ekran kullanımını takip ve azalttığı müddetçe bir kitap ve kahve hediyesi gayet masum kalır.

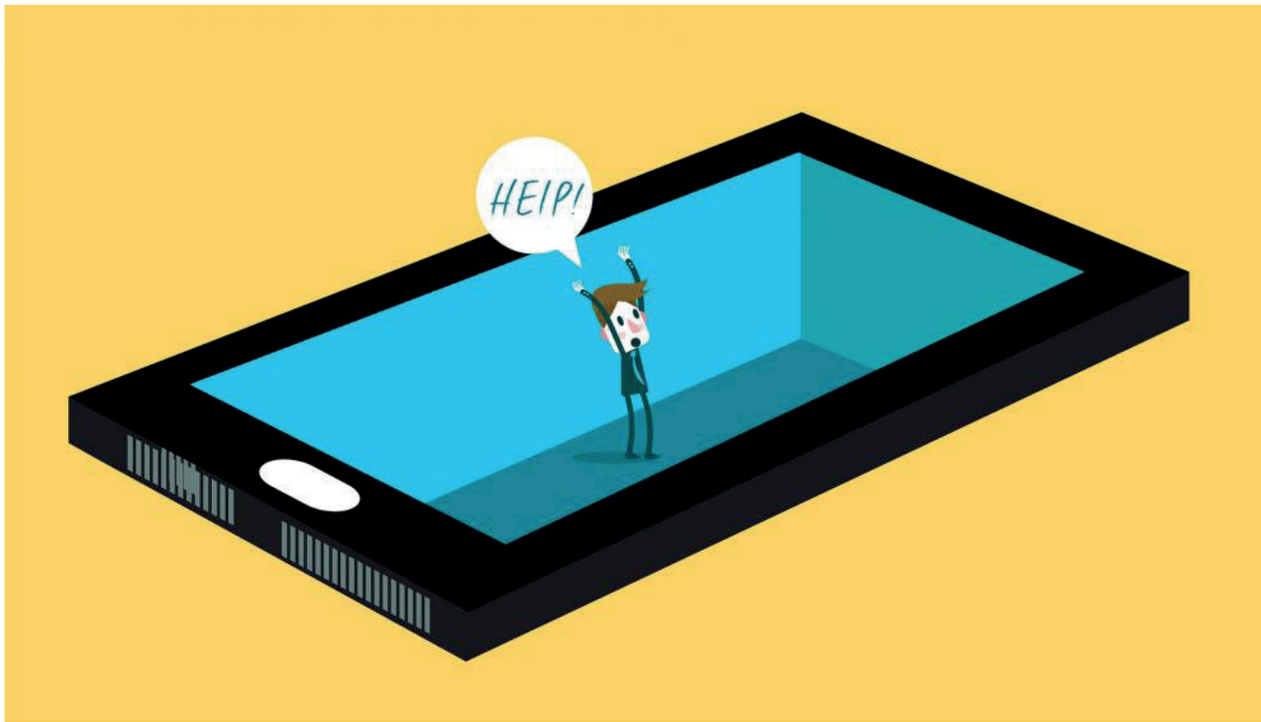
OnWard (internet sitesi)

Gabe Zichermann Gamification yani Oyunlaştırma konusunda dünyanın sayılı uzmanlarından biri. Halen bu konudaki dünyadaki en önemli kaynak olan www.gamification.co sitesini de yönetmektedir. Gabe oyunlaştırmanın gücünü yapay zekâyla birleştirerek bağımlılık problemlerini çözmek için 2016 yılında OnWard'ı kurdu. OnWard sizin cihaz kullanımlarınıza göre bir bot üzerinden size bir raporlama çıkarıyor. Devamında kullanımınızı öngörerek azaltmak ve engellemek üzere aksiyonlar yapıyor ve davranışlarınızı değiştirmeye çalışıyor. Gabe tüm sistemin tasarımının AI üzerinden cloud-bulut sistemlerinde tutulduğunu paylaşarak gizliliğe de vurgu yapıyor. Burada sadece sosyal medya ya da oyun değil kişiye özel internet üzerinden kumar, porno gibi kötü alışkanlıklarınızı da sadece siz takip edip bir yapay zekâ yardımıyla klinik doktorların önerileriyle azaltabiliyorsunuz.

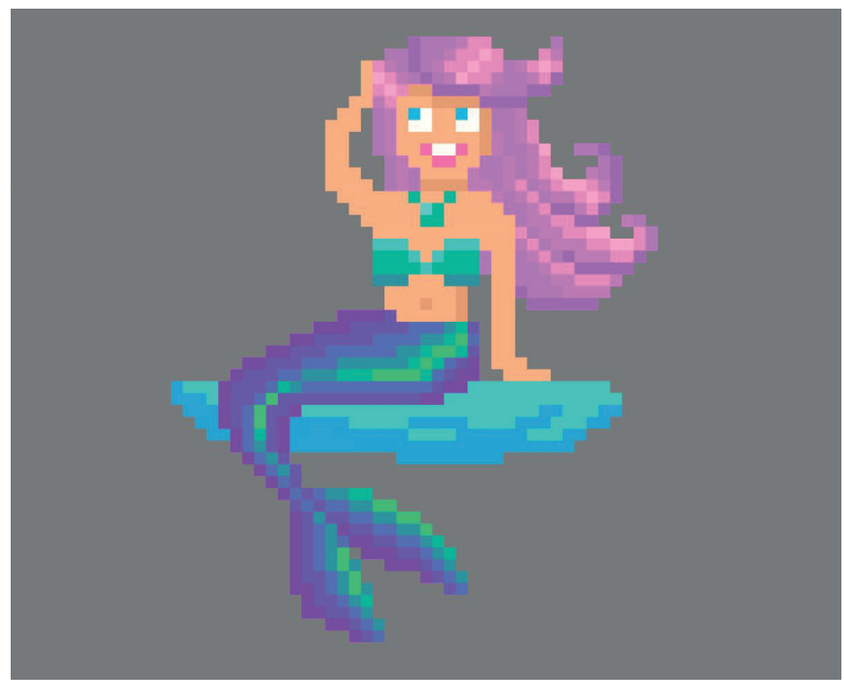
Kaynak: http://quq.la/HxhLo

AKILLI TELEFONUNUZA HİÇ BAKMADAN BU YAZIYI BİTİREBİLİR MİSİNİZ?

Yazan: Ercan Altuğ Yılmaz



Hiç belirli bir amaçla akıllı telefonunuzu elinize aldığınız ve amacınız dışında neredeyse her şeyi yaparak dakikalar geçirdiğiniz oldu mu? Yalnız değilsiniz.



Yüksek olasılıkla telefonu elinize aldığınızda bir sosyal ağın ya da anlık iletişim uygulamasının bildirimiyle karşılaştınız ve etkileşime geçtiğiniz anda dipsiz bir kuyunun içinde kaybolmanın ilk adımını atmış oldunuz. Bir süre sonra da kontrolünüzü ve odağınızı kaybettiğinizin farkına vardınız.

Artık günümüzde bu durumun bir adı var: "Vortex" yani "Ana-

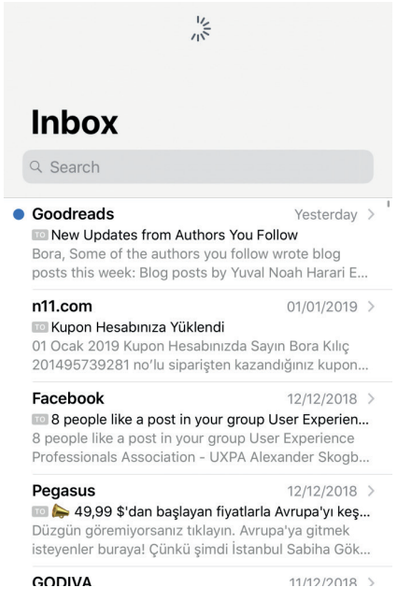
nizkızlarının cazibeli şarkılarına aldanan ve dönüşü olmayan bir yola giren denizciler gibi diyebiliriz.

İrrasyonel davranışlar konusundaki uzmanlığıyla bilinen Amerikalı ekonomist Dan Ariely de bu konu hakkında epey endişeli. Ariely'ye göre sokakta yürürken önünden geçtiğimiz her mağaza paramızı almaya, telefonumuzdaki her uygulama zamanımızı çalmaya uğraşıyor. Çevremizdeki her uyaranın çağrısına kapılsak, parasız kalmamız, obez olmamız ve sürekli dikkati dağınık bir şekilde dolaşmamız işten bile olmazdı. Bu nedenle artık bir savunma mekanizması ya da filtre olmadan hayata karışmak, oldukça riskli.

Teknolojinin Akıl Oyunları

Sokaktaki tehlikeleri bir kenara bırakarak, dijital dünyaya geri dönelim. Bizi anafora sokan başlıca etmenler bildirimler gibi gözükse de bu aslında buzdağının görünen kısmı. Google'da tasarım etiği üzerine çalıştıktan sonra kendi girişimini kuran Tristan Harris, teknolojinin psikolojik zayıflıklarımıza oynayarak (bilinçli ya da bilinçsiz) zihnimizi rehin aldığından bahsediyor.

Bir insanın günde ortalama 150 kez telefonunu kontrol ettiğini söylersem, buna neyin sebebiyet verdiği üzerine kafa yormayı eminim siz de anlamlı bulursunuz. Harris'e göre bunun ana sebebi, pek çok uygulamanın kullandığı eylem-ödül kurgusu. Kumarhanelerdeki kollu makineleri düşünün. Dünyanın en hızlı bağımlılık yaratan araçlarından biri. Kolu çekiyorsunuz, karşılığında bir ödül kazanıyorsunuz ya da bir dahaki sefere daha şanslı olacağınızı düşünerek tekrar deniyorsunuz. Basit bir eylem ve karşılığında sonuç alma beklentisi. Tıpkı yeni bir mail alıp almadığınızı görmek için ekranı tekrar tekrar yukarıdan aşağı doğru çekmek gibi değil mi?



Aslında telefonu cebimizden her çıkardığımızda bu mekanizma işliyor. Yeni bir arama ya da bildirim görme olasılığıyla hamle yapıyoruz ve sonuçtan bağımsız olarak bunu gün boyunca defalarca tekrarlıyoruz. Instagram "feed"'ini her yenilediğimizde ya da Tinder'da bir fotoğrafı her kaydırışımızda bu mekanizma devrede. Zihninizin "yeter" dediği ama parmaklarınızın eyleme devam ettiği durumlar da bu durumu kanıtlar nitelikte.

Tabii bunun bilinçli olarak yapıldığını söylemek yanlış bir genelleme olur. Neticede e-posta kutunuzu yeniledikçe Google ya da Apple daha fazla para kazanmıyor. İnsan psikolojisinin zayıflığını bilinçli olarak manipüle eden tasarımlar olsa da, bu davranış biçiminin kazara ortaya çıkan bir sonuç olduğu durumlar da mevcut.

Bizi anafora sokan olgulardan bir tanesi de "önemli bir şeyi kaçırıyor olma korkusu", İngilizce adıyla "FOMO" yani "fear of missing out". Bu olgu, Facebook'a uzun bir süre giriş yapmadığınızda arkadaşlarınızla ilgili önemli

bir gelişmeyi kaçırma, Twitter ya da Ekşisözlük'e bakmadığınızda trend olan hikâyeleri ıskalama korkusu şeklinde vücut bulabilir. Uzun süredir gerçekten ilgimizi çeken bir içerik sunmamış bültenleri takip etmeye devam etmemizin sebebi de bu aslında. Tabii bu korkunun sonu yok. 7/24 her mecrayı takip etme şansımız olmadığına göre, mutlaka bir şeyleri kaçıracağız.

Bu korkuyu yenmek için en sık kullandığınız uygulamayla bağınızı 1 haftalığına tamamen kesmeyi deneyin ve hayatınızda kayda değer bir değişiklik olup olmadığına bakın. Korkunun bir illüzyondan ibaret olduğunu fark edeceksiniz. Biraz felsefi bir yaklaşım olabilir ancak, farkında olmadığınız bir şeyi kaçırmış sayılmazsınız değil mi?

Bir şeyi kaçırıyor olma korsusu dijital mecraları ziyaret frekansımızı artırırken, otomatik çalma

özelliğine sahip ürünler de tüketim dozumuzu artırıyor. Cornell Üniversitesi'nde profesör olan Brian Wansink ilginç bir deney yapıyor. Çorba içen insanların kasesini onlar fark etmeden alttan sürekli dolduran bir düzenek hazırlıyor ve tüketim yüzde 73'e varan oranda artıyor! Teknoloji firmaları da doyduğumuzun farkına varmadan içerik tüketmeye devam etmemiz için otomatik çalma özelliğini kullanıyor. Netflix'te bir bölüm dizi izledikten sonra, ikinci bölüm otomatik olarak başladığında "e haydi bir tane daha izleyelim madem!" dediğiniz oldu mu hiç? Bunu söyleyerek aslında bilinçli bir karar almıyorsunuz. Karar sizin adınıza Netflix tarafından alınıyor, size de onaylamak kalıyor. Youtube ve Facebook'taki video içerik tüketiminin önemli bir kısmını yaratan özellik de bu. Instagram'ın sonsuz akışını da unutmayalım.

Kullanılan taktikler bunlarla sınırlı değil. Teknoloji girişimcilerinden kullanıcı deneyimi tasarımcılarına kadar pek çok insan grubu benzer yöntemlerle insanları ürünlerine daha bağımlı hale getirmek için teoriler ve uygulamalar üretiyor.

Firmalar Çözümün Bir Parçası Olabilir Mi?

Ekran bağımlılığı konusundaki farkındalığın ve endişenin artmasıyla birlikte, teknoloji firmaları insanları bilinçlendirmek ve kontrolü onlara geri vermek adına "Kaliteli Zaman Hareketi"ni (Time Well Spent) başlattı. Bu hareketin ana fikri, insanları teknolojik cihaz ve ürünleri nasıl kullandıkları hakkında bilgilendirerek, bağımlılıklarını azaltmaya destek olmak ve anafor içinde harcadıkları zamanın "daha kaliteli" olmasını sağlamak. Apple'ın hayata geçirdiği "Ekran Süresi" (Screen Time) özelliği bu hareketin güncel uygulamalarından biri

Bu özelliğin sunduğu panelde, telefonunuzu hangi gün ne kadar kullandığınızı, en çok hangi uygulamada vakit geçirdiğinizi görebiliyor ve dilerseniz kullanımınıza limit atayabiliyorsunuz.

Facebook ve Google'ın da benzer özellikleri söz konusu. Bu hareket kimi kanaat önderleri tarafından olumlu karşılansa da, kimileri inandırıcılığını hararetli bir şekilde sorguluyor ve bunu sigaranın zararları reddedilemez noktaya geldiğinde kullanıcılarına light ürünler sunmaya başlayan sigara firmalarına benzetiyor.

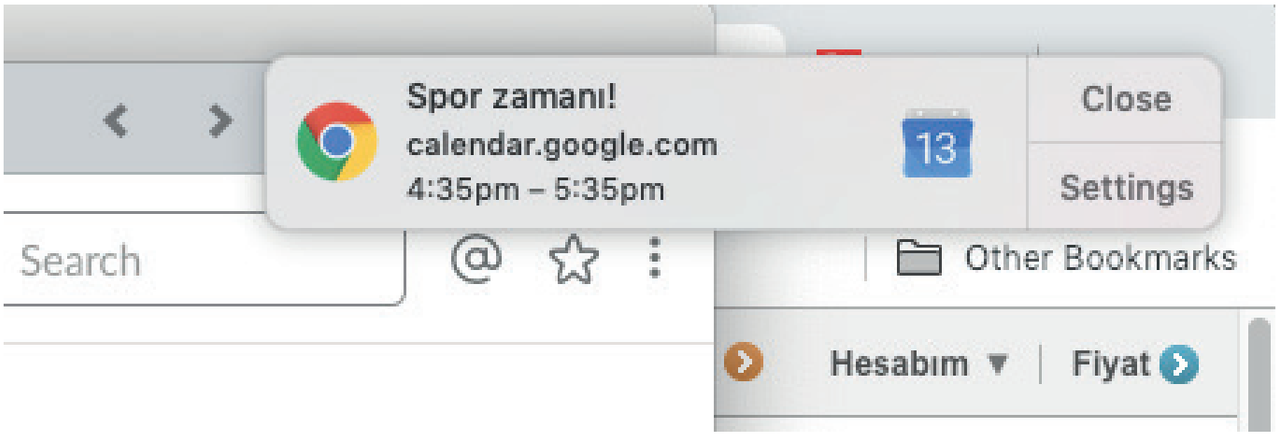
Biz Ne Yapabiliriz?

Kendimizi anafora kapılmaktan korumak için biz ne yapabiliriz? Aslında zayıflıklarımız üzerine kurgulanan bu taktiklerin farkına varmak bile başlı başına önemli bir adım. Böylelikle teknolojinin bize sunduğu (ve sunmadığı) seçenekleri bilinçli bir şekilde değerlendirebilir ve anafora girmekten kendimizi alıkoyabiliriz. Hatta yeterince kafa yorarsak, farkındalığın bir adım ötesine geçip bu taktikleri günlük hayatımızda kendimize fayda sağlamak için de kullanabiliriz.

Video içerik platformlarının otomatik çalma özelliğine geri dönelim. Buradaki püf noktası, bir sonraki içeriği tüketip tüketme-

me kararını kullanıcının elinden almak. Sizce Netflix dizinin diğer bölümünü başlatmadan önce, "Devam etmek istiyor musunuz?" diye sorsaydı, bir oturuşta tüm sezonu izleyen kullanıcıların sayısı azalmaz mıydı? Karar kullanıcı adına önceden alındıysa, yapılabilecek tek şey bu karara karşı çıkmak oluyor ki, "hayır" demenin "evet" demekten daha zor olduğunu hepimiz biliyoruz.

Peki bu taktiği, kazanmak istediğimiz alışkanlıkları güçlendirmek adına kullansak nasıl olurdu? Diyelim ki düzenli olarak spor salonuna gitmeyi hedefliyorsunuz ancak iş çıkışında "spora gitsem mi gitmesem mi?" diye kendinize sorduğunuzda, yanıt çoğu zaman olumsuz oluyor çünkü sınırlı bir kaynak olan iradenizin çoğunu ofiste tüketmiş oluyorsunuz. Bunun yerine haftanın başında spora gideceğiniz zamanları takvime işleseniz ve günü geldiğinde yapmanız gereken şey o anda bir



karar almak yerine, önceden aldığınız karara uymak olsa?

Peki, Ya Deneyimi Tasarlayanlar?

Farklı sektörlerden lider markalar için dijital deneyimler tasarlayan SHERPA ekibinin bir üyesi olarak, "iş hedeflerimiz mi daha öncelikli yoksa kullanıcıların istekleri mi?" sorusunu sıkça işitiyorum. İdeal çözüm kuşkusuz her ikisini de karşılayan bir deneyim kurgulamak olacaktır ancak bu her zaman mümkün olmayabilir.

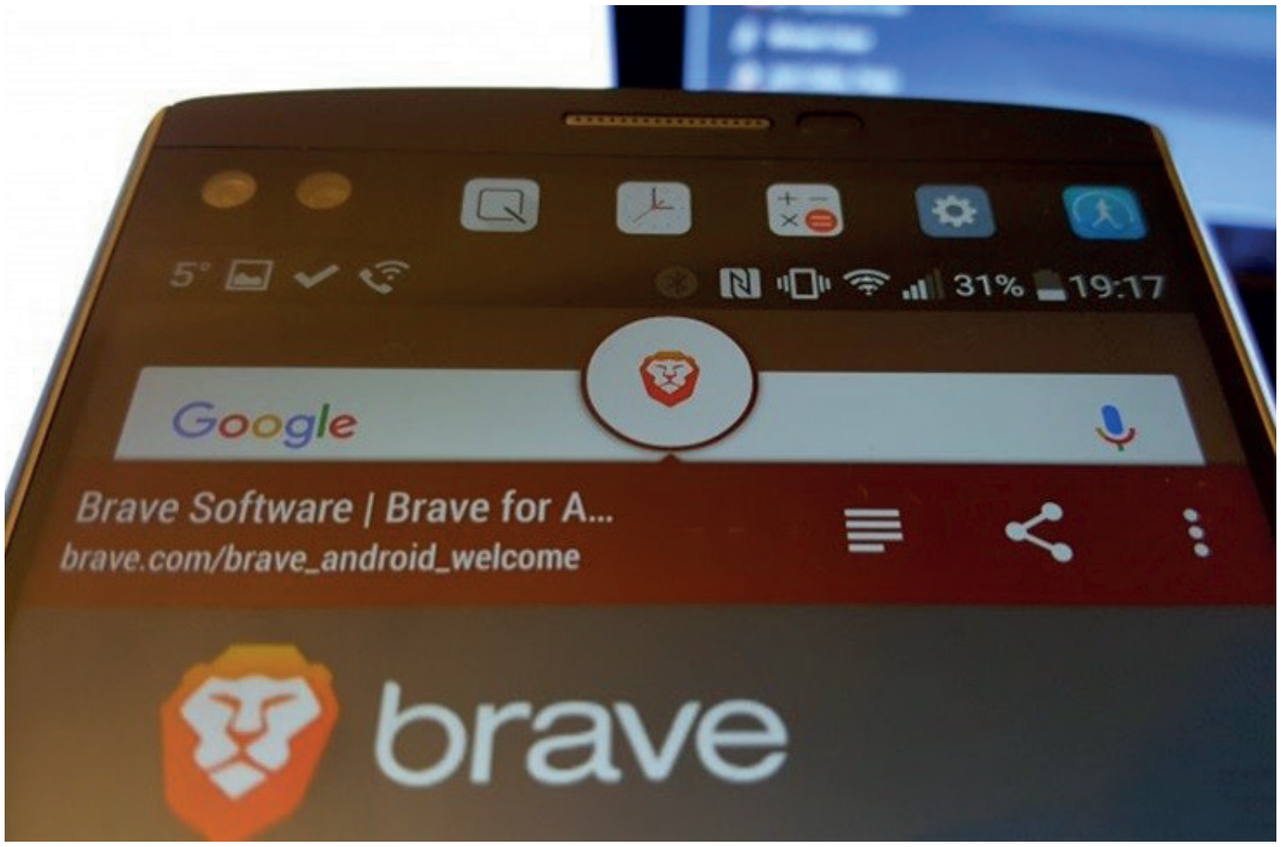
Kullanıcı deneyimi tasarımcıları hizmet verdikleri markanın hedefleri adına kullanıcıların aşil tendonlarını hedef aldığı sürece, anafor benzetmesi hayatımızda yer almaya devam edecek. Yazının genelinde sosyal medya üzerinden örnekler vermiş olsam da, e-ticaretten oyun endüstrisine kadar pek çok alanda kullanıcıların kontrollerini kaybetmesine neden olacak uygulamalarla karşılaşıyoruz.

Kullanıcı deneyimi alanında en köklü kuruluşlardan olan Nielsen Norman Group'tan Kate Mohan ve Kim Flaherty, kullanıcının dikkatini çekmek ya da onu ikna etmek için kurgulanan deneyimlerin mutlaka kötü olması gerektiğine inanmıyor. Onlara göre kullanıcıyı belli aksiyonları almaya yönlendirecek kurgular üretmekte bir sorun yok ancak bunun etik bir sınırı var. Ne zaman ki deneyim kurgusu kullanıcıların aleyhine çalışmaya ve kontrolü ellerinden almaya başlarsa, bu sınır da aşılmış oluyor.

Eğer yöneticisi olduğunuz ya da deneyimini kurguladığınız dijital ürünün bu etik sınırı aşıp aşmadığını öğrenmek istiyorsanız en doğru yol kullanıcıya gitmek olacaktır. Nasıl ki bir web sitesi ya da mobil uygulamanın kullanılabilirlik seviyesini ölçmek için kullanıcı testi yapılıyorsa, kurgulanan deneyimin anafor oluşturup oluşturmadığını anlamanın yolu da, ürünün kullanıcısını gözlemlemek, davranışları ve duygu durumu hakkında içgörü elde etmekten geçer. Unutmamak gerekir ki, kullanıcılarınıza maddi ya da manevi açıdan zarar verebilecek uygulamalar, kısa vadede metriklerinize olumlu yansısa da, mutsuz bir ilişkiyi kimse uzun süre devam ettirmek istemez.

Kaynak: http://quq.la/yejbY

REKLAMLAR İLE PARA KAZANDIRAN İNTERNET TARAYICISI: BRAVE BROWSER



Gizlilik odaklı internet tarayıcısı Brave Browser, reklamlar ile para kazandıracak. Brave Browser, reklamlara yönelik yenilikçi bir girişim başlatıyor.

Reklamlar İle Para Kazanmak Mümkün Mü?

Brave Browser tarafından yapılan açıklamada, kullanıcıların reklamlardan para kazanabileceği duyuruldu. Kullanıcılar Brave Browser'un 1.0 versiyonu ile günde yalnızca 20 adet reklam görecek. Sonraki yeni versiyonlarda ise kullanıcılar reklamlardan para kazanmaya başlayacak.

1.0 sonrasındaki versiyonlarda, kullanıcılar reklam gelirlerinin yüzde 70'ini alabilecekler. Böylelikle 5 milyon kullanıcıya sahip internet tarayıcısı, yeni bir reklam stratejisi deneyecek.

Kullanıcıların bu sisteme dahil olması için Brave Rewards özelliğini aktif hale getirmesi gerekiyor. Daha sonra internet tarayıcısı kullanıcıları takip etmeye başlayacak BAT bakiyeleri en fazla ziyaret ettikleri internet siteleri arasında dağıtılacak. Kullanıcılar Basic Attention Token (BAT) bakiyeleri biriktikten sonra çekebilecekler.

Kaynak: http://quq.la/pnQk5