Eylül 2026
btkibris.org

BTKıbrıs

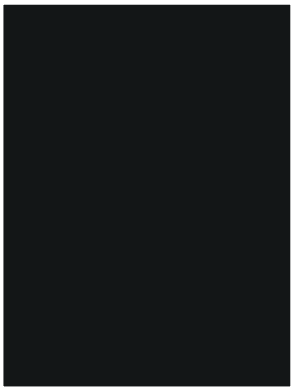
KIBRIS'IN ACISINI PAYLAŞIYORUZ

30 ağustos 2026 tarihinde Girne açıklarında yaşanan deniz faciasında hayatını kaybedenleri saygıyla anıyor, ailelerine, yakınlarına ve tüm Kıbrıs'a başsağlığı diliyoruz.

Sayı 6

Editörün yazısı:

Deniz faciası bir kader değil, Teknoloji Yoksunu Devlet Politikasıdır.



30 Ağustos'ta KKTC 'de denizde meydana gelen gemi faciasını yalnızca "kader" diyerek açıklamak, aslında sorumluluğu görünmez kılmaktır.

Denizde yaşanan her kazanın elbette öngörülemeyen yönleri olabilir; ancak modern dünyada can güvenliği için geliştirilen teknolojiler, erken uyarı sistemleri, iletişim altyapıları, takip ve denetim mekanizmaları tam da bu riskleri azaltmak için vardır.

Bir facianın ardından "kader" demek kolaydır; asıl zor olan, "**Bu olayın önüne geçmek için hangi tedbirleri almadık?**" sorusunu cesaretle sormaktır.

Devletin görevi yalnızca bir felaket yaşandığında müdahale etmek değil, felaket yaşanmadan önce gerekli teknolojik ve kurumsal altyapıyı kurmaktır. Gemilerin takibinin, deniz trafiğinin izlenmesini, acil durum haberleşmesini, konum belirlemesini, meteorolojik uyarılar, kaptan ve mürettabatın ve personelin yeterliliğini, denetim sistemlerinin çağdaş teknolojinin sunduğu imkânlarla güçlendirmekte devletin sorumluluğudur. Acil durumlar erken müdahale ve ara kurtarma yine devletin en büyük sorumluluğudur. Bunlar birer lüks değil, insan hayatını korumanın temel araçlarıdır.

Teknolojiyi zamanında kullanmayan, yatırım yapmayan veya mevcut imkânları etkin biçimde işletmeyen kamu politikalarının bedelini ise çoğu zaman karar vericiler değil, sıradan insanlar canlarıyla öder.

Teknoloji kendi başına mucize değildir; onu doğru planlayan, kullanan, denetleyen, uygulayan ve gerektiğinde geliştiren bir devlet aklı gerekir.

Teknolojiden kaçınmak, eski yöntemlere körü körüne bağlı kalmak veya "bugüne kadar bir şey olmadı" anlayışıyla hareket etmek, riskleri ortadan kaldırmaz. Tam tersine, bir sonraki felaketin zeminini hazırlar.

Bugün denizde yaşanan bir facia, yarın hava taşıtlarında, kara taşıtlarında kısaca başka bir ulaşım alanında, başka bir altyapıda veya başka bir kamu hizmetinde karşımıza çıkabilir. Çünkü mesele yalnızca bir gemi ya da tek bir kazadan ibaret değil, mesele, insan hayatını korumayı devlet politikasının merkezine koyup koymamaktır.

Artık her facianın ardından kaderi suçlamak yerine kendi tercihlerimizi sorgulamalıyız. Empati yapmalıyız.

Teknolojiyi doğru zamanda ve doğru biçimde kullanmayan, kullandırmayan, bilim, bilişim ve teknolojiyi meslek edinmiş kişilere önem vermeyen, bilimsel veriyi ve çağdaş güvenlik standartlarını karar alma süreçlerinin merkezine koymayan bir devlet, toplumu her defasında yeni bir acıyla baş başa bırakacaktır.

Kader, alınması gereken tedbirlerin yerine konulabilecek bir mazeret değildir. İnsan hayatını korumak bir tercihtir; bilime, teknolojiye ve liyakate yatırım yapmak da bir tercihtir. Devletin en temel sorumluluğu, insanların kaderlerine terk edilmesini değil, mümkün olan her durumda onların hayatlarını güvence altına almayı sağlamaktır.

Devlet olarak gerekeni yapılması bir vicdani görevdir.
Gerekeni yaptırmak hepimizin elindedir.
Daha fazla canlar yanmadan gerekeni yapın.

Ahmet HIZLI,
Bilgisayar Mühendisi

Fiyatı Düzenledik, Faturayı Düzenlemedik

Fiber optik ek protokolü Telekomünikasyon Dairesi'nin bilançosundan okumak

19 Eylül 2026'da Ankara'da imzalanan ek protokolün metni nihayet ortada. 8 madde, 5 sayfa. Karşısında duran ana protokol ise 11 madde, 10 sayfa ve 24 Eylül 2025 tarihli. Kamuoyunda tartışma büyük ölçüde "kazandık mı, kaybettik mi" ekseninde yürüdü. Oysa böyle metinler tek bir cümleyle özetlenmez. Bir yerde kazanılır, başka bir yerde kaybedilir; asıl mesele hangi yerde ne kazanıldığıdır.

Ek protokolü Telekomünikasyon Dairesi'nin penceresinden okuduğumda gördüğüm tablo şu: düzenleyici çerçeve ciddi biçimde iyileşti, Daire'nin bilançosuna ise hiç dokunulmadı.

Önce hakkını teslim edelim

Ana protokolde Yatırımcı, kuracağı altyapı üzerindeki toptan tarifeleri serbestçe belirliyordu. Ek protokolle bu yetki BTHK'nın kararlaştıracağı azami fiyat sınırlarına bağlandı. "Bu protokol kapsamındaki işlerde teknik ve ticari modelleri belirleme ve seçme yetkisi Yatırımcıdadır" diyen madde ise metinden tamamen çıkarıldı.

Bunlar küçük düzeltmeler değil. Bir de yaptırım geldi: 1 yıl içinde 150.000 bağımsız bölüme ulaşılamaması Yatırımcı'nın açık ve ispatlanmış ihlalinden kaynaklanıyorsa, KKTC farklı bir yatırımcı şirket talep edebilecek. Ana protokolde bu hedefin hiçbir karşılığı yoktu; taahhüt vardı, taahhüdün arkasında bir şey yoktu.

Protokole ayrıca bir çıkış kapısı açıldı. Mevzuata veya kamu yararına aykırılık halinde taraflar, 1 yıl önceden bildirimle protokolü feshedebiliyor. 25 yıllık bir metin için bunun önemi tartışılmaz.

İstihdam tarafında da imtiyaz kalktı: Yatırımcı'nın yapacağı her istihdam için önce Çalışma Dairesi'ne başvurulacak, uygun aday bulunamazsa Türkiye'den personel getirilebilecek.

Şimdi kasaya bakalım

Buraya kadar iyi. Sorun, düzeltilen maddelerin ortak özelliğinde: hepsi yetki ve tanım maddesi. Para maddelerinin hiçbirine dokunulmadı.

Sabit ses hizmetini ele alalım. Bu hizmette Daire son kullanıcıya satış yapıyor, faturayı kesiyor, tahsilat riskini taşıyor ve tahakkuk eden bedelin %50'sini Yatırımcı'ya ödüyor. Hiçbir gider düşülmeden. Kurumsal data devrelerinde de oran aynı: %50. Aradaki tek fark, orada yurtdışı çıkış bedelinin düşülebilmesi. Üstelik bu hizmetlerin çekirdek şebekesini işleten de Daire.

Bu %50'yi bir başka oranla yan yana koyun. Yatırımcı, kendi sunduğu toptan genişbant hizmetinin tahsilatından KKTC bütçesine penetrasyon oranına göre %5 ila %7 arasında pay veriyor. Yani devlete giden pay en iyi ihtimalle %7; Daire'den çıkan pay %50.

Özetle Daire şebekeyi işletiyor, müşteriyi buluyor, parayı tahsil ediyor, riski üstleniyor ve gelirinin %50'sini veriyor.

Bunun yanına masraf tarafını koyun. Sabit ses çekirdek şebekesi, ana omurga transmisyonu, kiralık devrelerin bakımı, enerji ve soğutma altyapısı, jeneratör yakıtı, elektrik tüketim giderleri, yedek kart bulundurma, yazılım güncellemeleri, siber güvenlik — hepsi Daire'nin sorumluluğunda. Ek protokol bu fıkraların hiçbirini açmadı.

Ve bir ayrıntı var ki metnin en sessiz maddesi, en riskli olanı: bakım ve işletme faaliyetleri "Yatırımcı'nın belirleyeceği standartlara göre" yapılacak. Standartlara uyulmazsa Yatırımcı gerekli tedbirleri alacak ve buradan doğacak ek maliyetten Daire sorumlu olacak.

Bir kamu kurumunun, karşı tarafın tek taraflı belirlediği ve tavanı olmayan bir yükümlülüğü üstlenmesi mali disiplinle bağdaşmaz. Bu tür bir hükümbütçelenemez, çünkü sınırını siz belirlemiyorsunuz.

Seçmediğiniz cihazın bakımı

Ek protokol, iyileştirme yatırımlarının ekipman seçimine bir ekleme yaptı: Yatırımcı bu hususlarda "ilgili KKTC kurumlarına bilgi verecek."

Bilgi vermek, onay almak değildir. Ekipmanı Yatırımcı seçiyor; o ekipmanın bakımını, yedek parçasını, yazılım güncellemesini ve güvenliğini 25 yıl boyunca Daire üstleniyor. Bir cihazın gerçek maliyeti satın alma bedeli değil, ömür boyu işletme bedelidir. Bu bedeli ödeyecek olan tarafın seçim kararına katılmaması, teknik bir ayrıntı değil, yapısal bir hatadır.

Tarifeler dolar, gelir Türk Lirası

Toptan tarifeler ABD Doları üzerinden tanımlanmış: 100 Mbps'e kadar sınırsız FTTH paketleri abone başına aylık 18 ABD Doları, her 100 Mbps artış için 5 Dolar ilave. Toptan sabit genişbant ve sabit ses için bağlantı ve nakil ücretleri 50'şer ABD Doları. Bu tutarlar Merkez Bankası kuruyla TL'ye çevriliyor ve 6 ayda bir TÜFE ile güncelleniyor.

Daire'nin son kullanıcıdan aldığı ücretler ise Ücretler Tüzüğü'ne ve siyasi karar mekanizmasına bağlı; en son ne zaman güncellendiğini hepimiz biliyoruz. Maliyet yılda 2 kez otomatik artıyor, gelir aynı hızda artmıyor. Bu makas 5 yılda kapanmaz, açılır. Bugün tartışılmayan bu madde, birkaç yıl sonra Daire'nin en büyük sorunu olacak.

Ölçülemeyen taahhüt

Ek protokolün en dikkat çekici yeniliklerinden biri, tarafların "yatırımlar sonucunda KKTC telekomünikasyon sektöründen elde edilen toplam gelir seviyesinde herhangi bir azalmaya sebebiyet verilmeyeceğini" taahhüt etmesi. Cümle güzel. Ama taahhüt sektör toplamı üzerine kurulu, Daire'nin geliri üzerine değil. Gelir Daire'den Yatırımcı'nın perakende şirketine kayarsa sektör toplamı değişmez, taahhüt de ihlal edilmiş sayılmaz. Baz yıl belirlenmemiş, ölçüm yöntemi tanımlanmamış, ihlal halinde ne olacağı yazılmamış.

Ölçülemeyen taahhüt, taahhüt değildir.

Aynı metinde iki farklı hüküm

Ek protokol, Daire'ye ait bina, depo, arsa ve sistem salonlarındaki teçhizatın Yatırımcı tarafından kullanımını rayiç bedeli aşmamak kaydıyla kira veya hizmet bedeline bağladı. Kazanım gibi görünüyor.

Ancak ana protokolün genel esaslar bölümündeki hüküm yerinde duruyor: Daire binalarının ve sistem salonlarının kullanılması durumunda Yatırımcı, kurulacak teçhizat için yer, enerji ve klimatizasyon ücretlerinden muaf tutulacak.

Aynı metinde biri bedelli, diğeri bedelsiz kullanım öngören iki hüküm var. Böyle çelişkiler uygulamada tarafsız çözülmez; güçlü tarafın lehine çözülür.

Yirmi beş yıl sonra kim devralacak?

Süre sonunda altyapı, "Telekomünikasyon Dairesi'ne veya KKTC Hükümeti tarafından belirlenecek ilgili kamu kurum veya kuruluşuna" devredilecek. Protokolün yürürlük maddesine eklenen ifade ise devrin "Kuzey Kıbrıs Türk Cumhuriyeti devletine" yapılacağını söylüyor.

Yani devir adresi bugünden belli değil. Bu arada FTTH şebekesini Yatırımcı'nın kendi personeli işletecek. Daire'nin saha kadrosu yeni yatırımın dışında kalacak, doğal yoldan yaşlanacak ve azalacak. 25 yıl, bir memurun neredeyse tüm hizmet süresidir; bugün işe başlayan teknisyen, devir günü emekli olmuş olacak.

25 yıl sonra kapıya bir şebeke gelecek. O şebekeyi devralıp işletecek teknik kapasitenin o gün mevcut olacağını güvence altına alan tek bir hüküm yok. Devir adresi belirsizse, o adresteki kurumun ayakta tutulması sorumluluğu da kimsenin üzerinde değil demektir.

Bir de veri meselesi

Daire, Mekansal Adres Kayıt Sistemi ile şebeke ve müşteri envanter verilerini Yatırımcı'ya temin etmekle yükümlü.

Aynı Yatırımcı'nın perakende şirketi, belirlenen aktivasyon eşiklerinin tutmaması halinde doğrudan perakende piyasaya girip hizmet verebilecek. Bu eşikler kademeli: mevcut servis sağlayıcıların aktif hizmete dönüştürdüğü bağlantı oranı 1. yıl %20, 2. yıl %35, 3. yıl %40, 4. yıl %45, 5. yıl %50 seviyesinin altında kalırsa kapı açılıyor. Kısacası Daire, ileride rakibi olabilecek bir yapıya kendi müşteri envanterini teslim ediyor. Bu yıl yaşadıklarımızdan sonra bu maddenin veri koruma boyutunu ayrıca konuşmamız gerekir.

Herkes ödüyor, bir kullanıcı ödemiyor

Ek protokole eklenen maddelerden biri şunu söylüyor: Türkiye Cumhuriyeti ilk 2 yıl içinde 27 milyon ABD Doları tutarında ve devamında ihtiyaçlar doğrultusunda Daire sistemlerine yatırım yapacak; buna karşılık Daire'nin ana omurgasının Türkiye Cumhuriyeti tarafından kullanılması halinde ayrıca bir kullanım bedeli talep edilmeyecek.

Bu ülkede GSM operatörleri ve internet servis sağlayıcıları Daire'nin ana omurgasını kullanırken bedel ödüyor. Yıllardır böyle. Şimdi aynı omurgayı kullanacak bir taraf, bu bedelden muaf tutuluyor.

Muafiyetin kapsamı da metinde giderek genişliyor. Birincisi, muafiyetin öznesi "Yatırımcı" değil, doğrudan "Türkiye Cumhuriyeti" olarak yazılmış. Protokolde Yatırımcı tanımlı bir kavram; burada kullanılan özne ise tanımsız ve daha geniş. İkincisi, ek protokol ana omurga transmisyon tanımına "bu teçhizatlar arasındaki iletişimi sağlayan fiber optik şebeke" ibaresini ekleyerek muafiyete konu varlığı büyüttü. Üçüncüsü, muafiyette hiçbir sınır yok: kapasite tavanı yok, trafik hacmi sınırı yok, süre kaydı yok. Yatırım 2 yıl için tanımlanmış, muafiyet 25 yıl sürecek.

Bu omurganın masrafını kimin ödediğini hatırlayalım. Ana omurga transmisyonunun bakımı ve işletmesi Daire'de. Enerji ve soğutma altyapısı, arıza işletmesi, jeneratör yakıt temini Daire'de. Elektrik tüketim giderleri Daire'de. Yedek kart, yazılım güncellemesi, siber güvenlik Daire'de.

Yani Daire, işletme maliyetinin tamamını taşıdığı bir varlıktan diğer bütün kullanıcılardan bedel alacak, tek bir kullanıcıdan almayacak. Bunun adı kamu bütçesinden yapılan çapraz sübvansiyondur.

Şimdi asıl soru: 27 milyon dolarlık fizibilitede omurga kullanım bedeli hesaba katıldı mı?

Katıldıysa muafiyet mükerrer bir avantajdır. Bedel bir kez yatırım kaleminde karşılanmış, bir kez de muafiyetle bağışlanmış olur.

Katılmadıysa ortada 25 yıl boyunca sürecek, hiç fiyatlanmamış bir kullanım hakkı var demektir. Bu durumda metnin "söz konusu yatırımların finansal dengesi ve kamu yararı gözetilerek" ifadesindeki denge, neye göre kurulmuştur?

İki ihtimalin de cevabı aynı yere çıkıyor: bu muafiyetin parasal karşılığını gösteren tek bir hesap kamuoyuyla paylaşılmadı.

Ne yapılmalı

Metin imzalandı, ancak Meclis onayı henüz tamamlanmadı ve protokolün kendisi ek protokollerle geliştirilmeye açık. Dolayısıyla bu tartışma bitmiş değil.

Öncelik verilmesi gereken beş başlık şu:

Ses ve kurumsal data hizmetlerindeki %50 gelir paylaşımı, abone başına sabit ve öngörülebilir bir bağlantı bedeline dönüştürülmeli. Yatırımcı bu hizmetlerde yalnızca erişim bağlantısı sağlıyor; gelirin %50'sini almasının teknik bir karşılığı yok.

Ekipman seçiminde "bilgi verme" mutabakata çevrilmeli. Ömür boyu maliyeti üstlenen taraf, seçim kararına katılmalıdır.

Yatırımcı için ölçülebilir bir hizmet seviyesi taahhüdü konmalı. Bugün metinde Yatırımcı'nın Daire'ye karşı tek bir sayısal kalite yükümlülüğü yok. Kesinti yaşandığında son kullanıcıya karşı sorumlu olan Daire, rücu edebileceği hiçbir hükme sahip değil.

Devir adresi tek bir kuruma sabitlenmeli ve mevcut altyapının mülkiyetinin Daire'de kaldığı açıkça yazılmalı.

Ana omurga kullanım muafiyeti ya kaldırılmalı ya da parasal karşılığı hesaplanıp kamuoyuna açıklanmalı. Bir kamu varlığından bir kullanıcının muaf tutulması, ancak muafiyetin değeri bilindiğinde tartışılabilir.

Son söz

Ek protokolde emek var, bunu kimse inkâr edemez. Düzenleyici çerçeve ana protokole göre belirgin biçimde güçlendi. Ancak bir kurumun geleceği yetki maddelerinde değil, gelir ve gider kalemlerinde belirlenir.

Telekomünikasyon Dairesi'nin adı bu metinde korundu. Kasası korunmadı.

Hakan ÜREDİ
uredihakan@gmail.com
0542 858 00 08

Her Şeyin Bir Uygulaması Olmak Zorunda mı?

Günümüzde hayatımızın neredeyse her alanında teknolojiyle karşılaşıyoruz. Sabah alarmımızı telefonumuzdan kapatıyor, işe giderken navigasyondan yararlanıyor, yemek sipariş ediyor, alışveriş yapıyor, bankacılık işlemlerimizi gerçekleştiriyor ve hatta evimizdeki cihazları bile telefonumuz üzerinden kontrol ediyoruz.

Bütün bunlar hayatımızı kolaylaştırmak için tasarlanıyor. Ancak son yıllarda dikkat çeken başka bir durum daha var: Neredeyse her şeyin bir uygulaması olmak zorunda.

Bir restorana gitmek için uygulama indiriyoruz. Bir kampanyadan yararlanmak için başka bir uygulama gerekiyor. Bir otelin hizmetlerini kullanmak için ayrı bir uygulama, otoparka girmek için başka bir uygulama, hatta bazen bir ürünü satın almak için bile önce uygulama indirmemiz isteniyor.

Peki gerçekten buna ihtiyacımız var mı?

Dijitalleşmek mi, Uygulama Yapmak mı?

Teknoloji sektöründe zaman zaman önemli bir ayrımı gözden kaçırıyoruz. Dijitalleşmek ile bir uygulama geliştirmek aynı şey değil.

Bir işletmenin dijitalleşmesi, müşterisinin hayatını kolaylaştırabilir. Fakat yalnızca "bizim de bir mobil uygulamamız olsun" düşüncesiyle geliştirilen bir uygulama, tam tersine kullanıcıya yeni bir yük getirebilir.

Çünkü bir uygulamanın var olması tek başına değer yaratmaz. Değer, gerçek bir problemi çözdüğü zaman ortaya çıkar.

Kullanıcının zaten tarayıcıdan birkaç saniyede gerçekleştirebildiği bir işlem için uygulama indirmesini, kayıt olmasını, bildirimlere izin vermesini ve telefonunda yeni bir alan açmasını istemek her zaman iyi bir kullanıcı deneyimi anlamına gelmez. Örneğin bir restoranın menüsünü görmek veya kısa süreli bir kampanyadan yararlanmak için web sayfası ya da QR kod çoğu zaman yeterlidir; buna karşılık sık kullanılan bankacılık veya harita gibi hizmetlerde uygulama gerçekten değer katar.

Bazen en iyi çözüm, hiç uygulama geliştirmemektir.

Telefonlarımız Uygulama Mezarlığına Dönüşüyor

Telefonlarımızdaki uygulamalara bir göz atalım.

Muhtemelen büyük bir kısmını her gün kullanmıyoruz. Bir dönem ihtiyacımız olduğu için indirdiğimiz, birkaç kez kullandıktan sonra unuttuğumuz onlarca uygulama telefonlarımızda bekliyor.

Her uygulama ayrı bir hesap, ayrı bir şifre, ayrı bildirimler ve ayrı güncellemeler anlamına geliyor.

Bir noktadan sonra teknoloji hayatımızı kolaylaştırmak yerine yönetmemiz gereken yeni bir liste oluşturuyor.

Aslında burada ilginç bir çelişki var.

Teknolojiyi hayatımızdaki işleri azaltmak için kullanıyoruz. Fakat yanlış tasarlandığında teknoloji, bize yeni işler ekleyebiliyor.

Yeni uygulamayı indir. Hesap oluştur. Bildirimlere izin ver. Şifreni belirle. Güncelleme yap. Ve bütün bunları yalnızca birkaç dakikalık bir işlem için yap.

Kullanıcı Teknolojiyi Değil, Çözümü İstiyor

Bir yazılımcı veya teknoloji şirketi için uygulama geliştirmek başlı başına bir ürün olabilir. Fakat kullanıcı açısından durum farklıdır.

Kullanıcı uygulama istemez. Kullanıcı çözüm ister.

Bir otobüs bileti almak istiyorsa biletini hızlıca almak ister. Bir restoranda rezervasyon yapmak istiyorsa rezervasyonunun kolayca gerçekleşmesini ister. Bir bankacılık işlemi yapmak istiyorsa işlemini güvenli ve hızlı şekilde tamamlamak ister.

Bunu mobil uygulamayla mı, web sitesiyle mi, QR kodla mı veya başka bir teknolojiyle mi yaptığımız çoğu zaman kullanıcı için ikinci plandadır.

Burada asıl soru "Hangi teknolojiyi kullanalım?" değil, "Kullanıcının işini nasıl daha kolay hale getiririz?" olmalıdır.

Teknoloji Görünmez Olduğunda Daha Başarılı Olabilir

Geleceğin en başarılı teknolojilerinden bazıları, kullanıcıların teknoloji olarak bile fark etmeyeceği çözümler olacak.

Çünkü iyi teknoloji kendisini göstermek zorunda değildir.

Bir işlem birkaç saniyede gerçekleşiyorsa, kullanıcı arka planda hangi API'nin çalıştığını, hangi veritabanının kullanıldığını veya hangi sunucunun cevap verdiğini düşünmez.

Ve aslında düşünmemesi iyi bir şeydir.

Teknolojinin başarısı bazen ne kadar çok özellik sunduğuyla değil, kullanıcıya ne kadar az şey düşündürdüğüyle ölçülmelidir.

Bu nedenle her probleme yeni bir uygulama ile cevap vermek yerine, bazen mevcut sistemleri birbirine bağlamak, web tabanlı basit bir çözüm sunmak veya kullanıcıya hiçbir şey yükletmeden işlemi gerçekleştirmek çok daha doğru olabilir.

Daha Fazla Teknoloji, Her Zaman Daha İyi Teknoloji Değildir

Teknoloji geliştikçe daha fazla imkanımız oluyor. Ancak imkanların artması, hepsini kullanmamız gerektiği anlamına gelmiyor.

Bir işletme için onlarca özellik içeren bir uygulama geliştirmek etkileyici görünebilir. Fakat kullanıcı bu özelliklerin yalnızca ikisini kullanıyorsa, geri kalan özelliklerin ne kadarının gerçekten değer kattığını sorgulamak gerekir.

Bazen sade bir sistem, karmaşık bir sistemden daha değerlidir. Bazen bir uygulama yerine iyi tasarlanmış bir web sitesi yeterlidir. Bazen yeni bir özellik eklemek yerine mevcut özelliği daha hızlı ve daha anlaşılır hale getirmek gerekir.

Ve bazen teknolojik açıdan yapabileceğimiz bir şeyi yapmamak, verebileceğimiz en doğru teknoloji kararıdır.

Belki de Doğru Soru Farklı

"Her şeyin bir uygulaması olmak zorunda mı?" sorusunun cevabı aslında tamamen "hayır" değil.

Elbette bazı hizmetler için mobil uygulamalar büyük avantaj sağlıyor. Sürekli kullanılan, kişiselleştirme gerektiren veya cihazın özelliklerinden yararlanan hizmetlerde uygulamalar oldukça değerli.

Ancak teknoloji üretirken kendimize sürekli şu soruyu sormamız gerekiyor:

"Bunu gerçekten kullanıcı için mi yapıyoruz, yoksa sadece yapabildiğimiz için mi yapıyoruz?"

Bu iki yaklaşım arasında büyük bir fark var.

Çünkü teknoloji, hayatımıza daha fazla araç eklemek için değil, hayatımızdaki gereksiz zorlukları azaltmak için var.

Belki de geleceğin en iyi dijital deneyimi, bize yeni bir uygulama indirtmeyen deneyim olacak.

Çünkü teknolojinin gerçek amacı hayatımızın merkezine yerleşmek değil; hayatımızı kolaylaşıp mümkün olduğunca sessizce geri çekilmektir.

Naim Sadıklar
Web Yazılım Geliştirme Takım Lideri

BTKıbrıs

KIBRIS'IN ACISINI PAYLAŞIYORUZ

30 ağustos 2026 tarihinde Girne açıklarında yaşanan deniz faciasında hayatını kaybedenleri saygıyla anıyor, ailelerine, yakınlarına ve tüm Kıbrıs'a başsağlığı diliyoruz.

Kara Sabandan Otonom İşletmelere

Bir sahneyle başlayalım: Güzelyurt; Bir ağustos gecesi, saat 03.00. Narenciye bahçesinin sahibi uyuyor. Ama bahçe uyumuyor. Toprağın on santim altındaki nem sensörü, gündüzün sıcağından sonra suyun azaldığını fark ediyor. Sulama ajanı hava tahminine bakıyor: yarın 41 derece, rüzgâr güneyden. Kuyu ajanı, çekilen suyun tuzluluğunun geçen haftaya göre biraz arttığını raporluyor. Finans ajanı bir sulama daha yapmanın elektrik maliyetini hesaplıyor. Pazar ajanı, limon fiyatının hangi yöne gittiğine bakıyor. Sonra sistem duruyor. Çiftçinin telefonunda tek satırlık bir mesaj bekliyor:

"Sabah 05.30'da damla sulamayı başlatayım mı? Önerim: iki saat, önce batı parsel. Onaylıyor musun?"

Bu sahne bilimkurgu değil. Buradaki teknolojilerin hiçbiri hayal değil; nem sensörü de, hava tahmini de, sulama otomasyonu da bugün var. Yeni olan şu: bunların birbiriyle konuşup ortak bir hedef için çalışması ve son sözü hâlâ insana bırakması. Bu yazı tam olarak o "son söz" hakkında.

Son üç-dört yılda gördüklerimizin yapay zekâ devriminin kendisi olduğunu düşünüyorsak yanılıyoruz. Bugüne kadar yapay zekâya bir şey sorduk, metin yazdırdık, görsel oluşturduk, kod ürettik. Yani onu çoğunlukla akıllı bir yardımcı, biraz da eğlenceli bir oyuncak olarak kullandık. Şimdi ikinci perde açılıyor: Agentic AI, yani "ajan" yapay zekâ. Artık yapay zekâ yalnızca cevap veren bir sistem olmaktan çıkıyor. Ona bir hedef veriyorsunuz; plan yapıyor, başka araçları kullanıyor, veri topluyor, sonuçları kontrol ediyor, gerekirse başka ajanlarla iş bölümü yapıyor ve işi bitirmeye çalışıyor. Temmuz 2026 tarihli bir United Nations University(1) çalışması da bu dönüşümü tam böyle tarif ediyor: tek seferlik metin üretiminden; planlayan, araç kullanan, hafızasını koruyan ve yazılım ortamlarında eyleme geçen ajanlara geçiş. Bahçedeki o gece nöbeti, ikinci perdenin küçük bir provasıydı. Ve bu değişim bana göre yalnızca bahçeleri değil, şirketlerin iskeletini de değiştirecek.

100 kişilik şirketi 10 kişi yönetebilir mi?

Eskiden bir girişim kurduğunuzda yazılımcı, tasarımcı, pazarlamacı, satışçı, finansçı, müşteri destek ekibi… uzun bir kadro büyütmeniz gerekirdi. Her yeni süreç, yeni bir maaş veya hizmet alımı demekti. Şimdi aynı girişimcinin yanında görünmeyen mesai arkadaşları beliriyor:

Satış ajanı → Pazarlama ajanı → Finans ajanı → Kodlama ajanı → Müşteri destek ajanı → Araştırma ajanı

Uyumuyorlar, öğle tatiline çıkmıyorlar, pazartesi sabahı morali bozuk gelmiyorlar ve aynı anda yüzlerce işle ilgilenebiliyorlar. Bu "insansız şirket" demek değil. Tam tersine: az sayıda ama çok yetkin insanın yönettiği, büyük bir dijital iş gücü demek. Güncel ve çarpıcı bir örnek bugünlerde İngiltere'den geliyor. Cosine adlı yaklaşık 30 kişilik bir girişim, İngiltere'nin egemen frontier AI modeli olmayı hedefleyen Lumen Sovereign(2) üzerinde çalışıyor. İddia gerçekleşir mi, zaman gösterecek. Ama 30 kişilik bir ekibin bir ülkenin yapay zekâ altyapısına talip olabilmesi bile yeni dönemin ölçeğini anlatıyor. Otuz kişi. Bizde kalabalıkça bir aile kahvaltısı veya Mangal demek.

Peki bir Otonom işletme nasıl görünecek ve Neye benzeyecek?

Gece 03.00'teki bahçe sahnesini şimdi küçük bir e-ticaret şirketine taşıyalım. Satış ajanı son 24 saatin verisine bakıyor ve bir ürünün satışlarının düştüğünü fark ediyor. Araştırma ajanı rakip fiyatlarını tarıyor. Pazarlama ajanı yeni bir kampanya öneriyor. Finans ajanı kampanyanın kâr marjına etkisini hesaplıyor. Stok ajanı depoyu kontrol ediyor. Kritik karar anında sistem yine duruyor:

"Bu kampanyayı başlatmak ister misiniz?"

İşte benim gelecekte görmek istediğim yapı bu. Yapay zekâ düşünsün, araştırsın, alternatif üretsin, hatta yüzlerce işi kendi arasında koordine etsin. Ama şirketin iradesi hâlâ insanda olsun. Bu noktada teknoloji dünyasının yeni gözde kavramı devreye giriyor: harness. Türkçesi koşum takımı. Kara saban çağında öküz ne kadar güçlü olursa olsun, sabanın nereye gideceğini öküz değil, koşum ve onu tutan el belirlerdi. Bugün de ajanın ne kadar akıllı olduğu tek başına yetmiyor. Hangi araçlara erişebildiği, hangi sınırlar içinde hareket ettiği, yaptığı işin nasıl doğrulandığı ve insanın dizginleri ne zaman eline aldığı asıl meseleye dönüşüyor.

Yeni girişimcinin en büyük sermayesi insan sayısı olmayacak: Girişimcilikte çok temel bir soru değişiyor. Dünün sorusu şuydu: "Kaç kişilik ekibiniz var?" Yarının sorusu belki şu olacak: "Kaç insan ve kaç yapay zekâ ajanıyla ne kadar değer üretiyorsunuz?" Bu soru Kıbrıs gibi küçük bir ülke için hayati. Küçük nüfus ve sınırlı insan kaynağı geçmişte açık bir dezavantajdı; en parlak gençlerimiz için "burada iş yok" cümlesi neredeyse bir kaderdi. Yapay zekâ çağında ise küçük ama iyi eğitimli, dünyaya bağlı ve bu araçları ustalıkla kullanan ekipler, kendilerinden yüz kat daha büyük organizasyonlarla rekabet edebilir. Üstelik artık rekabet edebilmek için her yere fiziksel olarak ulaşmanız da gerekmiyor; ne de olsa bir yapay zekâ ajanının direkt uçuşa ihtiyacı yok.

Önce beyaz yakalı işler mi değişecek? Burada gençlerin pek hoşuna gitmeyecek bir şey söylemem gerekiyor. Üretken yapay zekânın ilk büyük dalgası fabrikadaki işçiyi değil, klavyenin başındaki bizi vuracak. ILO'nun 2025 tarihli küresel çalışması(3) yaklaşık 30 bin görevi inceleyerek mesleklerin üretken yapay zekâya ne kadar "maruz"

olduğunu ölçüyor. Buradaki kritik ayrım şu: maruz kalmak, mesleğin yok olacağı anlamına gelmiyor; mesleğin içindeki görevlerin bir bölümünün yapay zekâ tarafından dönüştürülebileceği anlamına geliyor. 2026'da yayımlanan ABD iş ilanları araştırması(4) da benzer bir tabloyu çiziyor: dönüşüm işlerin toptan kaybolması şeklinde değil, şirketlerin kimi işe aldığını ve mevcut işlerin içindeki görevleri yeniden tasarlamasıyla yaşanıyor. En sert değişim junior pozisyonlarda. Yani kariyer merdiveninin ilk basamağı daralıyor. Bu, işe yeni başlayacak bir genç için okuması en zor cümle. Dolayısıyla soru artık "hangi mesleği seçmeliyim?" değil. Soru şu:

"Seçtiğim mesleğin hangi kısmını yapay zekâ yapacak ve ben hangi kısmında vazgeçilmez olacağım?"

Berber, kasap ve kebapçı neden biraz daha rahat! Bir berber dükkânı düşünün. Randevuları yapay zekâ alabilir. Müşterinin geçmiş saç modellerini hatırlayabilir. Stok siparişini verebilir, muhasebeyi hazırlayabilir. Hatta yarın bir robot kol saç kesiminin bir bölümünü bile üstlenebilir. Ama aynada göz göze gelip "Abi yanları biraz daha mı alalım?" diyecek berber muhtemelen uzun süre orada olacak. Aynı şey kasap, kebapçı, tesisatçı, marangoz ve el becerisi gerektiren pek çok meslek için geçerli. Fiziksel dünya dağınık, öngörülemez ve her seferinde biraz farklı. Bu yüzden bu mesleklerin tam otomasyonu, yalnızca ekranda yapılan işlere göre çok daha zor. Ama dikkat: onların işletmeleri de dönüşecek. Burada unutulmaması gerekn ana konu ise asıl meslekler kalır; mesleğin çalışma biçimi değişir.

Jetgiller aslında bize bir şey söylüyordu; Benim kuşağım Jetgiller'i hatırlar. Uçan arabalar, görüntülü konuşmalar, robot hizmetçiler, kendi kendine çalışan evler… Gençlere küçük bir ödev: İnternetten eski bir The Jetsons bölümü bulun ve bugünün gözüyle izleyin. Önce biraz güleceksiniz. Sonra telefonunuza, robot süpürgenize, görüntülü görüşmeye, akıllı saatinize ve cebinizdeki yapay zekâ asistanına bakın. Asıl şaşırtıcı olan Jetgiller'in ne kadar hayalperest olduğu değil; bizim o hayale ne kadar yaklaşmış olduğumuz.

Kara sabandan otonom traktöre:

Ben bu dönüşümü hep tarım üzerinden düşünürüm. Çünkü tarım, insanın teknolojiyle ilişkisinin en eski hikâyesidir. İnsan önce toprağı eliyle işledi. Sonra hayvanı koştu. Kara saban geldi. Ardından traktör. Bugün ise tarlada kendi kendine çalışan otonom traktörlerden söz ediyoruz. Bu artık gelecek senaryosu değil. John Deere'ın mevcut otonom sistemlerinde 360 derece görüş sağlayan 16 kamera, yüksek hızlı işlemci ve yapay zekâ kullanılıyor(5); traktör belirli tarla işlerini kabinde kimse yokken yapabiliyor. Peki çiftçi ortadan kalktı mı? Hayır. Çiftçinin kullandığı araç değişti. Bugün yapay zekâ kullanmayı reddetmek, bana otonom traktörün yanında kara sabanla tarla sürmeye çalışmak gibi geliyor. Ama diğer uç da aynı derecede tehlikeli: Traktöre binmek sizi çiftçi yapmadığı gibi, ChatGPT kullanmak da sizi girişimci, yazılımcı, araştırmacı ya da düşünür yapmaz.

Peki Kıbrıs'ın tarlası bu oyunun neresinde?

Bu soruyu sormadan yazıyı bitirmek olmaz. Çünkü otonom traktör hikâyesi Amerika'nın ufka kadar uzanan mısır tarlalarında geçiyor. Bizim gerçeğimiz başka. KKTC'de tarım meselesi aslında bir su meselesidir. Yağış az, yazlar uzun ve sert, kurak yıllar sıklaşıyor. Güzelyurt'un yıllarca aşırı çekilen yeraltı suyu tuzlandı; bedelini portakal bahçeleri ödedi. Anamur'dan borularla gelen su büyük bir şans; ama nereye gittiği ölçülmeden dağıtılan su, ölçülmeden serpilen tohum gibidir. Tarlalarımız küçük ve mirasla parça parça olmuş; bir dev otonom traktör bizim parselde dönemez bile. Tarlanın başındaki çiftçi yaşlanıyor; gençler tarımı "eski iş" sayıyor. Mazot, gübre ve yem pahalı; tepemizde yılın büyük bölümünde güneş varken elektrik hâlâ pahalı ve zaman zaman kesiliyor. Ürünümüz dünyaya çoğu zaman dolaylı yollardan, fazladan maliyetle gidiyor. Ama iki büyük kozumuz var: dünyanın tanıdığı, coğrafi işaretli bir ürün olan hellim ve nüfusa oranla dünyanın en yoğun üniversite ekosistemlerinden biri. Yani hem satacak bir hikâyemiz hem de o hikâyeyi teknolojiye çevirecek gençlerimiz var. O hâlde otonom traktörden önce bizim tarlaya yakışan yapay zekâ için önerilerim şunlar:

BİZİM TARLAYA YAKIŞAN YEDİ ÖNERİ

1. Önce suyun ajanı. Her kuyuya seviye ve tuzluluk sensörü, her bahçeye toprak nemi sensörü, hepsinin üstüne de bir sulama ajanı. Bu ajan hava tahminini, bitkinin gelişim dönemini ve suyun maliyetini birlikte değerlendirip her bahçe için o günün sulama önerisini üretir. Güzelyurt akiferinin dijital ikizi çıkarılırsa, kimin nereden ne kadar su çektiği ilk kez gerçek zamanlı görülür. Anamur suyunun sulama ayağı da bu akıl olmadan işletilmemeli. Tarımda yapay zekânın bize ilk kazandıracağı şey verim değil, kurtardığı su olacak.

2. Mesarya'nın gözü gökyüzünde olsun. Kuru tarım yapılan buğday ve arpa tarlaları için uydu görüntüsü ve drone, çıplak gözün göremediğini gösterir: hangi parsel susuz, hangisi hastalıklı, hangisinde gübre boşa gidiyor. Aynı gözler patates tarlasında hastalığı yayılmadan yakalar. Kurak bir yılda hangi çiftçinin gerçekten zarar gördüğü de tahminle değil veriyle belgelenir; destekler daha adil dağıtılır.

3. Küçük tarlaya küçük robot; tek çiftçiye değil köye teknoloji. Bizim parsellere dev makineler değil; ilaçlama ya da yabani ot temizliği yapan küçük otonom robotlar, hizmet olarak kiralanan drone'lar ve kooperatif çatısı altında paylaşılan ekipman yakışır. Bunları kim koordine edecek? Tek tek çiftçiler değil; köy ölçeğinde çalışan, "bu hafta hangi makine hangi tarlada" sorusunu optimize eden bir kooperatif ajanı. Kooperatifçilik zaten bizim eski kültürümüz; yapay zekâ ona sadece yeni bir beyin ekler.

4. Güneşin altında iki hasat. Panelleri tarlanın üstüne kuran agrivoltaik sistemler hem elektrik üretir hem de gölgesiyle buharlaşmayı azaltır. Pompasını güneşle çalıştıran, iklimini yapay zekânın yönettiği, topraksız üretim yapan seralar hem su hem enerji tasarrufu sağlar. Bizim kadar güneşi olan bir ülkenin serası elektrik kesintisinde karanlıkta kalmamalı.

5. Hellimin dijital kimliği. Coğrafi işaretli bir ürün, "hangi sütle, nerede, nasıl üretildi" sorusuna belgeli cevap ister. Sürüdeki hayvanların sağlığını izleyen sensörlerden sütün toplanmasına, soğuk zincirden paketin üstündeki QR koda kadar kesintisiz bir izlenebilirlik zinciri, hellimi dünya raflarında premium bir ürün yapar. Aynı zincir harnup pekmezi, zeytinyağı ve narenciye için de kurulabilir. Üstüne bir de pazar ajanı ekleyin: hangi ülkede, hangi mevsimde, hangi niş pazarda bizim ürünümüze talep var; gece gündüz tarasın.

6. Çiftçinin cebinde bir ziraat mühendisi. Türkçe konuşan, yaprağın fotoğrafını çekince hastalığı tanıyan, don ve sıcak hava dalgası uyarısı veren, destek başvurusunun evrakını hazırlayan, günün ürün fiyatını söyleyen bir tarım asistanı. Klavyeyle değil sesle çalışmalı ki 70 yaşındaki çiftçi de kullanabilsin. Amaç Tarım Dairesi'nin uzmanlarını yok etmek

değil; onların bilgisini aynı anda her çiftçiye ulaştırmak.

7. Genç çiftçi bir veri çiftçisidir. Üniversitelerimizin tarım ve mühendislik fakülteleri, teknopark ve Tarım ve Doğal Kaynaklar Bakanlığı aynı masaya oturup Güzelyurt'ta, Mesarya'da ve Karpaz'da birer "dijital örnek çiftlik" kurmalı. Gençlerin gidip görebileceği, denemelere katılabileceği, kendi girişimini test edebileceği canlı laboratuvarlar. Bir genç için tarım, traktör sürmek değil de sulama ajanının önerisini okuyup "hayır, bugün sulamıyoruz" diyebilecek bilgiye sahip olmak anlamına gelirse, o genç tarlaya döner.

Bu yedi maddenin ortak noktasına dikkat edin: Yapay zekâ ölçüyor, hesaplıyor, öneriyor. Ama "bu yıl patates mi, arpa mı?" sorusuna hâlâ çiftçi cevap veriyor.

En büyük tehlike işimizi değil, irademizi kaybetmek!
Ben gençlerin asıl bundan endişelenmesini isterim. Yapay zekânın sizin yerinize araştırmasına izin verin. Hesap yapmasına, alternatif üretmesine, kod yazmasına, veriyi analiz etmesine, yüzlerce sayfayı sizin yerinize okumasına izin verin. Ama mümkün olduğunca sizin yerinize düşünmesine ve özellikle sizin yerinize karar vermesine izin vermeyin. Çünkü insanın yapay zekâ çağındaki en değerli özelliği belki de bildiklerinin miktarı değil; neyi istediğine karar verebilmesi, doğru soruyu sorabilmesi, üretilen cevabı sorgulayabilmesi ve sonucun sorumluluğunu üstlenebilmesi olacak. Gece 03.00'te telefonda bekleyen o soruyu hatırlayın: "Onaylıyor musun?" O soruya cevap verecek biri olduğu sürece tarlanın da şirketin de sahibi hâlâ insandır. Asıl tehlike, o sorunun bir gün artık sorulmaması. O gün kaybettiğimiz şey işimiz değil, irademiz olur.

Yeni yaşam mücadelesi: Gelecek biraz korkutucu görünebilir. Normaldir. Traktör geldiğinde de çiftçi korktu. Otomasyon geldiğinde fabrika işçisi korktu. Bilgisayar geldiğinde ofis çalışanı, internet geldiğinde koca sektörler kendi sonunun geldiğini düşündü. Bazıları gerçekten ortadan kalktı. Ama yepyeni meslekler ve yepyeni şirketler de doğdu. Şimdi yeni bir dönüşümün başındayız. Üstelik bu kez değişim doğrusal değil; ivmelenerek geliyor. Bu yüzden gençlere "yapay zekâdan korkmayın" demek bana yetmiyor.

Ben başka bir şey söylemek istiyorum: Yapay zekâyı öğrenin. Kullanın. Harness edin; yani koşumu siz takın. Yönetin. Ama dizginleri ona teslim etmeyin. Çünkü yapay zekâ oyunu daha yeni başlıyor. Ve bu oyunda kazananlar ne yapay zekâya karşı savaşanlar olacak ne de peşinden düşünmeden gidenler. Kazananlar, onu güçlü bir araca dönüştürüp direksiyonda kalmayı başaranlar olacak.

Kara sabanı bırakın. Ama tarlanın sahibi siz kalın.

KAYNAKLAR
1.Temmuz 2026 tarihli United Nations University çalışması — Jia An Liu, Engineering and Governing the Agent Harness: A Technology and Policy Framework for the Runtime Layer of Agentic AI, UNU Macau, 21 Temmuz 2026. https://unu.edu/publication/engineering-and-governing-agent-harness-technology-and-policy-framework-runtime-layer (PDF: https://unu.edu/sites/default/files/2026-07/Engineering_and_Governing_the_Agent_Harness.pdf)
2.Cosine ve Lumen Sovereign — Cosine'ın koalisyon duyurusu, 8 Haziran 2026: https://cosine.sh/blog/building-lumen-sovereign-uk-industry-coalition · Tech.eu haberi: https://tech.eu/2026/06/08/cosine-secures-industry-backing-for-britain-s-first-sovereign-frontier-model/ · "Yaklaşık 30 kişilik ekip" bilgisi Financial Times'ın haberine dayanıyor; Cosine'ın basın sayfasında alıntılanmıştır: https://cosine.sh/newsroom
3.ILO'nun 2025 küresel çalışması (yaklaşık 30 bin görev) — Gmyrek vd. (ILO–NASK), Generative AI and Jobs: A Refined Global Index of Occupational Exposure, ILO Working Paper 140, Mayıs 2025. https://www.ilo.org/sites/default/files/2025-05/WP140_web.pdf · ILO basın duyurusu (20 Mayıs 2025): https://www.ilo.org/resource/news/one-four-jobs-risk-being-transformed-genai-new-ilo%E2%80%93nask-global-index-shows
4.2026'da yayımlanan ABD iş ilanları araştırması — Fangyan Wang, Zaiyan Wei ve Yang Wang (Purdue Üniversitesi), Generative AI and the Reorganization of Labor Demand, arXiv:2605.23159, Mayıs 2026. https://arxiv.org/pdf/2605.23159
5.John Deere otonom traktör (16 kamera, 360 derece görüş) — John Deere basın açıklaması, CES 2025: https://www.deere.com/en/news/all-news/autonomous-9RX/

Ahmet Bilgen
Teknoloji Girişimcisi - Melek Yatırımcı - Zamanını Vakfeden

Bu Teknoloji Kimin için Yapıldı?

Bir çocuğun korunması ailesinin doğru ayarı bulmasına, bir insanın hizmete erişmesi telefonunun yeniliğine bağlı olmamalı.

Yalnızca 42 numara ayakkabı üreten bir fabrika düşünün. Ayakkabıları sağlam, şık ve kendi ölçülerine göre kusursuz. Ancak çocuğa büyük geliyor, ayağı daha büyük olana dar. Farklı bir ayak yapısına sahip olan ise ayakkabıyı hiç kullanamıyor.
Şikâyetler gelince fabrika üretim anlayışını değiştirmiyor. Dolgu malzemeleri, esnetme aparatları, özel bağcıklar çıkarıyor. Sonra da "Artık herkese uygun" diyor.
Oysa ayakkabı hâlâ aynı. Uğraşması, uyum sağlaması ve ek bedel ödemesi beklenen insan.
Dijital dünyaya da bu gözle bakabiliriz. Bir uygulamayı kullanamayan kişiye hemen "Teknolojiden anlamıyor" demeden önce, belki de uygulamanın kimi düşünerek yapıldığını sormalıyız.

Her tasarımın aklında bir kullanıcı vardır

Bir uygulama hazırlarken karşımızda şöyle birini düşündüğümüzü varsayalım: Yazıyı rahatça okuyabiliyor, sesi duyabiliyor, küçük düğmelere kolayca dokunabiliyor. Açıklamaları ilk seferde anlıyor, hata yaptığında ne yapacağını biliyor. Telefonu yeni, interneti hızlı. Üstelik yetişkin.
Bu hayalî kişiye "varsayılan kullanıcı" diyebiliriz. Yani sistemin, karşısında olduğunu kabul ettiği insan.
Sorun, böyle insanların bulunması değil. Sorun, herkesin böyle olduğunu düşünerek tasarım yapmak.
Çünkü küçük yazıları okuyamayan birinin, internet bağlantısı sık sık kesilen birinin ve henüz okumayı öğrenen bir çocuğun ihtiyaçları aynı değil. Bir işlemi her gün yapan kişiyle ilk kez yapmaya çalışan kişi de aynı yardıma ihtiyaç duymuyor.
Üstelik ihtiyaçlarımız değişiyor. Elimiz yaralandığında, gözlüğümüz yanımızda olmadığında veya güneş altında ekranı göremediğimizde, normalde rahatça kullandığımız bir uygulama bizim için de zorlaşabiliyor. Erişilebilir tasarım, engelli kişilerin karşılaştığı güçlüklerin yanında bu geçici ve duruma bağlı engellerin de azalmasına yardımcı oluyor.
Bu nedenle "Herkes kullanabilir" demekle herkesin gerçekten kullanabilmesi arasında önemli bir fark var. O farkı görmek için de yalnızca işlemini tamamlayanlara değil, daha ilk ekranda zorlananlara bakmak gerekiyor.

Korunmak için uzman olmak gerekmemeli

Ek adımı, güvenli bir ortama ulaşmak için çocuk değil; yetişkinlere özgü seçeneklere geçmek için yetişkin atmalı.

Daha da iyisi, hiç kimsenin gereksiz bir ek adım atmak zorunda kalmamasıdır.

BUGÜN	ÖNERİ
çocuk	çocuk
↓ *ek adım*	**güvenli ortam**
↓ *ek adım*	yetişkin
↓ *ek adım*	↓ *ek adım*
güvenli ortam	**yetişkinlere özgü seçenekler**
Ek adımları bulmak, açmak ve takip etmek ebeveyne kalır.	

Ek adım yer değiştirdiğinde korunmak, kullanıcının çabasıyla elde ettiği bir ayrıcalık olmaktan çıkar.
Çocukların da erişebildiği bir hizmette neden önce herkesi yetişkin kabul edip ardından ailelerden korumayı açmalarını bekleyelim? Bir ebeveynin ek uygulama indirmesi, ayarları araştırması, filtreleri düzenlemesi ve bunları sürekli takip etmesi gerektiğini düşünün. Böyle bir durumda çocuğun korunmasını, ailesinin teknik bilgisine ve ayırabildiği zamana da bağlamış oluruz.
Ebeveynin sorumluluğu elbette var. Ancak bu sorumluluk, hizmeti sunanın sorumluluğunun yerine geçmemeli. Temel korumalar baştan etkin olmalı; çocuk bunlara ulaşmak için bir yetişkinin doğru menüyü bulmasını beklememeli.
Peki, bunun için herkesten kimlik mi isteyeceğiz?
Her koruma için yaşımızın bilinmesi gerekmiyor. Örneğin kişisel bilgilerimizi kendiliğinden herkese açmamak, yalnızca çocukların değil, yetişkinlerin de yararlanabileceği bir koruma.
Birleşik Krallık'ın veri koruma kurumu ICO'nun çocuklara uygun tasarım rehberi, bu konuda somut bir örnek sunuyor.

Çocuğun yararı açısından güçlü bir gerekçe bulunmadıkça, yüksek mahremiyet ayarlarının başlangıçta etkin olmasını esas alıyor. Ayrıca bu veri koruma kurallarının bütün kullanıcılara uygulanabileceğini belirtiyor. Böylece söz konusu korumaları sağlamak için önce herkesin yaşını öğrenmek gerekmiyor.
Gerçekten yetişkinlerle sınırlandırılması gereken içerik ve özelliklerde ise güvenilir yaş kontrolü ayrı bir ihtiyaç. Burada amaç, gerekli kontrolü mümkün olan en az kişisel bilgiyle yapmak olmalı. Herkese temel koruma sunmak, herkese çocuk gibi davranmak değildir; yetişkinlere farklı seçenekler sunmak da onların mahremiyetinden vazgeçmesini gerektirmemeli.
Kısacası güvenlik, ayarlar menüsünde saklanan ve ancak arayanın bulduğu bir özellik olmamalı.

Yeni telefon almak tek çözüm mü?

Bir hizmeti kullanabilmek için önce yeni bir telefon almak zorunda mıyız? Yoksa hizmet, insanların zaten sahip olduğu araçlara göre sunulabilir mi?
Kenya'da 2007'de başlayan M-PESA, bunun örneklerinden biri. Sistem, insanların temel cep telefonlarıyla birbirlerine para gönderebilmesini sağlamak için geliştirildi. Dijital bir hizmetten yararlanmak için herkesin önce akıllı telefon sahibi olması beklenmedi.
Machankura ise başka bir örnek. Hizmetin kısa kodla erişimi desteklediği şebekelerde, kullanıcılar akıllı telefona veya kendi internet bağlantılarına ihtiyaç duymadan Bitcoin gönderip alabiliyor. Telefonda kısa bir kod tuşlayarak açılan yazılı menüden işlem yapılıyor; başka bir Machankura kullanıcısına telefon numarası üzerinden gönderim yapılabiliyor. Telefon şebekesi hâlâ gerekli, ama kullanıcının internet paketi olması şart değil.
Burada asıl önemli olan Bitcoin veya başka bir para birimi değil. Kullanıcının elindeki telefonun bir eksiklik olarak görülmemesi. "Telefonunu değiştir, sonra gel" demek

hizmete ulaşmanın başka bir yolunun sunulması.,

Elbette erişimin kolay olması, bir hizmetin güvenlik ve mahremiyetle ilgili bütün soruları çözdüğü anlamına gelmez. Ama tasarımın nereden başladığını gösterir: İnsanı değiştirmeye çalışmaktan mı, onun koşullarını anlamaktan mı?

M-PESA'da küçük ama önemli bir ayrıntı daha var. Safaricom'un sunduğu telefon menüsünde, para gönderilmeden önce alıcının kim olduğunun kontrol edilmesi ve işlemin onaylanması isteniyor. Bu adımın amacı, yanlış kişiye para gönderilmesini önlemeye yardımcı olmak.

Demek ki her ek adım kötü değil. Para göndermeden önce alıcıyı kontrol etmek başka; bir hizmete ulaşabilmek için yeni cihaz almak veya korumayı açmak için karmaşık menülerle uğraşmak başka.

Amaç bütün adımları kaldırmak değil; insanı koruyan adımlarla, tasarımın eksiğini kullanıcıya tamamlattıran adımları ayırmak.**Kuzey Kıbrıs'ta nereden başlayabiliriz?**

Dünyanın büyük teknoloji şirketlerinin bütün kararlarını değiştiremeyebiliriz. Ama kendi sunduğumuz ve satın aldığımız hizmetlerde söz sahibiyiz: Hastane randevuları, kamu işlemleri, okul duyuruları, belediye hizmetleri…

Bu hizmetlerin bir kısmını dışarıdan satın alıyoruz; bir kısmını kendi kurumlarımızdaki ekiplerle geliştiriyoruz. İkisinde de kimin düşünüleceğine dair söz söyleme imkânımız var.

Bir hizmetin internete taşınması, ona erişimin kendiliğinden kolaylaştığı anlamına gelmez. Yanlış tasarlanmış bir sistem, gişedeki kuyruğun yerine ekrandaki bir engeli koyabilir.

Bu yüzden önce basit sorular sormalıyız. Bir okul duyurusunu okumak için mutlaka yeni bir uygulama indirmek gerekiyor mu? Basit bir işlem için e-posta hesabı şart mı? İnterneti kullanamayan kişi, aynı hizmete başka bir yoldan ve daha kötü koşullara mahkûm olmadan ulaşabiliyor mu?

M-PESA ve Machankura örneklerinden çıkaracağımız ders, bütün hizmetleri aynı teknolojiyle sunmak değil. Hizmete ulaşmanın tek bir yolu olması gerektiğini varsaymamak.

Başarıyı nasıl ölçtüğümüz de önemli. Bir randevu sitesine yüz kişinin girdiğini ve doksanının işlemini tamamladığını düşünün. İlk bakışta iyi bir sonuç gibi görünebilir. Ama diğer on kişi neden tamamlayamadı? Yazıları mı okuyamadı? Hata mesajını mı anlayamadı? Bağlantısı mı kesildi?

Dahası, siteye hiç giremeyenler bu sayının neresinde?

Birleşmiş Milletler'in “kimseyi geride bırakmama” yaklaşımı da kimin ve neden geride kaldığını anlamayı öne çıkarıyor. Kalkınma hedefleri, yaş, engellilik durumu ve yaşanılan yer gibi farklılıkları görebileceğimiz bilgilerin üretilmesini öngörüyor. Böylece genel sonuçların gizleyebildiği güçlükleri fark etmek mümkün oluyor.

Bunu kendi hizmetlerimize uyguladığımızda anlamı açık: “Çoğu kişi kullanıyor” demekle yetinmemek; kullanamayanın neden kullanamadığını öğrenmek.

Bunun yolu da herkesten daha fazla kişisel bilgi toplamak olmamalı. Hizmeti farklı ihtiyaçlara sahip insanlarla denemek, zorlandıkları yerleri dinlemek ve özel bilgilerini açığa çıkarmadan sorunları raporlamakla başlayabiliriz. Yalnızca mevcut kullanıcılarla değil, hizmete henüz ulaşamayanlarla da konuşmalıyız.

Ardından bu beklentileri, yazılım satın alınırken hazırlanan şartnameye, yani sistemin neleri yapması gerektiğini belirleyen belgeye koymalıyız. Yalnızca “kolay kullanılacak” yazmak yetmez. Yazı büyütüldüğünde form kullanılabilir kalmalı. Görme engelli kişilerin kullandığı yardımcı yazılımlarla temel işlemler yapılabilmeli. Bir alan yanlış doldurulduğunda yalnızca “Hata” yazmamalı; neyin nasıl düzeltileceği anlaşılmalı. Bunlar sistem bittikten sonra hatırlanan istekler değil, teslim alınmasının koşulları olmalı.

Aynı beklentiler, yazılımı kendi ekiplerimizle geliştirdiğimizde de geçerli. Orada bir şartname olmayabilir; ama bir gereksinim listesi, bir iş sırası ve bir teslim kontrolü genellikle bulunur. Bu maddelere o listede baştan yer vermek, sonraya bırakmaktan daha kolay.

Kendi geliştirdiğimiz yazılımlarda bunları bize hatırlatan bir sözleşme olmayabilir; bu da onları en başta kendimizin not etmesini değerli kılıyor.

Kendi geliştirdiğimiz sistemlerin bu konuda bir avantajı da var. Dışarıdan alınan bir üründe düzeltme talebi sözleşmeye, bütçeye ve karşı tarafın takvimine bağlı olabilir. Kendi yazdığımız yazılımda ise sorunu fark ettiğimiz an düzeltmeye başlayabiliriz. Bu avantajdan yararlanmak için de sorunları görebileceğimiz bir çalışma biçimi kurmamız gerekiyor.

Web standartlarını geliştiren W3C (Dünya Çapında Ağ Konsorsiyumu) de erişilebilirliğin en baştan düşünülmesini ve geliştirme boyunca kontrol edilmesini öneriyor. Sorunları erken fark etmek, yapılmış işi sonradan yeniden düzenleme ihtiyacını azaltıyor. Üstelik otomatik kontrol araçları tek başına yeterli değil; insan değerlendirmesi de gerekiyor.

Elbette bunların bir maliyeti var. Ama kullanılamayan bir hizmetin de maliyeti var: Harcanan zaman, tekrar tekrar yapılan başvurular, yardım için başkasına bağımlı kalmak ve sonunda vazgeçmek.

Kaynakları doğru kullanmak, yalnızca çalışan bir sistem kurmak değil; insanların o sistemden gerçekten yararlanabilmesini sağlamak.

İyi teknoloji, insanın yükünü azaltır

Bir kaldırım rampasını düşünün. Tekerlekli sandalye kullanan kişinin geçişini sağlarken bebek arabası iten veya bavul taşıyan kişiye de kolaylık sunar. Altyazı da işitme güçlüğü yaşayan kişinin yanında, sesi açamadığı bir ortamda video izleyen kişiye yardımcı olur. Bir ihtiyacı karşılamak için geliştirilen çözüm, başka insanlara da yarar sağlayabilir.

Ama bir rampanın değerli olması için üzerinden bebek arabalarının da geçmesi gerekmez. Bir insanın hizmete erişebilmesi, başlı başına yeterli bir gerekçedir.

Başlangıçtaki ayakkabı fabrikasına dönersek mesele, herkese daha fazla aparat dağıtmak değil. Tek bir ölçünün herkese uymayacağını kabul ederek üretime başlamak.

Çocuğun korunmasını ailesinin doğru ayarı bulmasına, bir insanın hizmete erişmesini yeni telefon almasına, bir başkasının işlemini tamamlamasını sürekli yardım istemesine bağlamamak.

Teknolojik ilerlemeyi yalnızca sistemlerin ne kadar hızlı ve güçlü olduğuyla değil, insanların omzundan ne kadar yük aldığıyla da ölçmeliyiz. Her yeni uygulamanın, her yeni hizmetin karşısına bu soruyla oturmalıyız:

Bu teknoloji kimi düşünerek yapıldı — ve kimi, kendi başına bir çözüm bulmak zorunda bıraktı?

Seniha S. Öztemiz Tulgar
Bilgisayar Mühendisi
https://linkedin.com/in/senihaoztemiz

Dijital Kapıdaki Yabancı:
İyi Niyetli Hackerlar ve Hukukun Çıkmazı

Siber güvenlik, modern çağın en görünmez ancak en hayati savaş alanlarından biridir. İnternet ortamında faaliyet gösteren kurumlar, şirketler ve devletler, dijital kapılarının ne kadar güvenli olduğunu her an sorgulamak zorundadır. Ancak bu kapıları test eden herkes kötü niyetli değildir. Bir kişi, tamamen iyi niyetle bir web sitesinin veya sistemin açıklarını bulup bunu sistem sahibine bildirdiğinde, karşılığında bir teşekkür mü beklemelidir yoksa mahkeme celbi mi? Bu soru, özellikle Kuzey Kıbrıs Türk Cumhuriyeti (KKTC) gibi bilişim mevzuatının henüz olgunlaşma aşamasında olduğu ülkelerde ciddi bir hukuki çıkmaz yaratmaktadır.

Dijital sistemlerin karmaşıklığı arttıkça, bu sistemleri korumak kurumların kendi iç ekiplerinin kapasitesini aşmıştır. Bağımsız güvenlik araştırmacılarının dışarıdan sağladığı gözlemler, güvenliği sağlamada kritik bir rol oynamaktadır. Ancak bu dış gözlemlerin hukuki bir zemine oturtulmaması hem araştırmacıları hem de sistem sahiplerini büyük risklerle karşı karşıya bırakmaktadır. Siber saldırıların her geçen gün daha sofistike hale geldiği bir dünyada, iyi niyetli hackerların (beyaz şapkalı hackerlar) potansiyelini hukuki bir çerçevede değerlendirememek, ülkelerin siber savunma hatlarında ciddi zafiyetlere neden olmaktadır. Bu makale, KKTC hukuk sistemi çerçevesinde izinsiz güvenlik araştırmalarının ve sorumlu açık bildiriminin mevcut durumunu, sistem sorumlularının yükümlülüklerini ve bu alanda yapılması gereken yasal ve pratik düzenlemeleri detaylı bir şekilde incelemeyi amaçlamaktadır.

Endişelerin Temeli

KKTC Bilişim Suçları Yasası (32/2020) ve Kişisel Verileri Koruma Yasası (KVKK) (89/2007) çerçevesinde, bilişim sistemlerine yetkisiz erişim açıkça suç olarak tanımlanmıştır [1] [2]. Bilişim Suçları Yasası'nın 3. ve 4. maddeleri, hukuka aykırı erişimi üç yıla kadar hapis veya para cezaları ile cezalandırmaktadır. Hukuki açıdan, "yetkisiz" bir giriş, niyeti ne olursa olsun suç teşkil eder. Sistem sahibi ile önceden yapılmış yazılı bir sözleşme yoksa, açık bulan kişinin eylemi "hukuka aykırı" kabul edilir. Türkiye'de de benzer şekilde Türk Ceza Kanunu'nun (TCK) 243. ve 244. maddeleri, bilişim sistemine girme ve veriyi bozma suçlarını düzenlerken, eylemin hukuka uygunluğu ancak önceden alınmış yazılı bir rıza ile sağlanabilmektedir [3].

Bu durum, iyi niyetli güvenlik araştırmacıları için büyük bir risk oluşturur. Bir açık bulan kişi, bunu bildirdiğinde "sistemime izinsiz girdin" suçlamasıyla karşılaşabilir. Bu korku, araştırmacıların buldukları açıkları bildirmekten çekinmesine yol açar. Bildirilmeyen açıklar ise, kötü niyetli aktörler tarafından keşfedildiğinde çok daha yıkıcı sonuçlar doğurur. Hukukun bu katı yaklaşımı, dijital güvenliği sağlamak yerine sistemleri daha savunmasız hale getirmektedir. Zira bir sistemin açığı olduğunu bilmek ve bunu gizlemek, o açığın eninde sonunda kötü niyetli birileri tarafından kullanılacağı gerçeğini değiştirmez. Mevzuatın amacı sistemleri korumakken, uygulamada bu katılık, iyi niyetli uyarı mekanizmalarının işlemesini engelleyerek paradoksal bir şekilde güvenliği zayıflatmaktadır. Bu paradoks, siber güvenlik ekosisteminin sağlıklı bir şekilde büyümesinin önündeki en büyük engellerden biri olarak karşımıza çıkmaktadır.

Gerçek Sorun ve Sistem Sorumlusunun Yükümlülükleri

Asıl sorun, yasalardaki katı tanımlardan ziyade, iyi niyetli bildirimin sistem sahibi tarafından nasıl karşılandığıdır. Açığı bulan kişi bunu bildirdiğinde, sistem sorumlusu genellikle bu durumu bir "yardım" olarak değil, kendi işini eksik yaptığına dair bir "başarısızlık belgesi" olarak algılar. Sistemin güvenliğinden sorumlu olan kişi, kendi yetersizliğinin ortaya çıkmasından rahatsızlık duyabilir ve bildirim yapana karşı savunmaya geçerek cephe alabilir. Bu psikolojik defans mekanizması, sorunun çözülmesinden ziyade üstünün örtülmesine hizmet eder.

Daha önceki bildirimlere bakıldığı zaman ise Sistem sorumlularının ve / veya bildimi resmi olarak kabul eden merkezin ilgililere bildirimi esnasında veya sonrasında bir bildirimi karşılamasındaki niyeti iyi algılamaması diğer bir ifadeyle kabullenmemesi durumu üç maymunu oynamayı tercih etmesi veya Kıbrıs ağzıyla Sinda gülle geçsin veya başka bir ifade biçimiyle Sin de gülle geçsin yaklaşımı sorunu ortadan kaldırmamaktadır.

Bu noktada, KKTC'de sistem sorumlularının yetkinlikleri ve eğitim düzeyleri kritik bir tartışma konusu haline gelmektedir. Bir sistem yöneticisinin, dışarıdan gelen bir zafiyet bildirimini kişisel bir saldırı olarak algılamaması için belirli bir profesyonel olgunluğa ve siber güvenlik kültürüne sahip olması şarttır. Türkiye'de ve dünyada kamu kurumları ile büyük ölçekli şirketlerde görev alan sistem yöneticileri ve siber güvenlik sorumlularının CISSP (Certified Information Systems Security Professional), CISA (Certified Information Systems Auditor) veya en azından CompTIA Security+ gibi uluslararası geçerliliği olan sertifikasyonlara sahip olmaları beklenmektedir [4]. Bu sertifikasyonlar, yöneticilere sadece teknik bilgi değil, aynı zamanda kriz yönetimi, risk değerlendirmesi ve sorumlu açık bildirimi gibi süreçlerin nasıl yönetileceği konusunda da eğitim vermektedir.

KKTC'de ise bu tür sertifikasyon gereksinimleri henüz standartlaşmamıştır. Birçok kurumda, çevrimiçi platformların ve kodların sorumluluğunu üstlenen kişilerin siber güvenlik alanında yeterli akademik veya profesyonel geçmişi bulunmayabilmektedir. Oysa bir sistem sorumlusu, kuruma entegre edilen veya kurum içinde geliştirilen yazılımların kod güvenliğinden (secure coding), sızma testlerinin periyodik olarak yaptırılmasından ve ortaya çıkan zafiyetlerin ivedilikle yamalanmasından birincil derecede sorumludur. Bir çevrimiçi sistem kuruma alınırken veya devreye sokulurken; veri sınıflandırmasının yapılması, erişim kontrol mekanizmalarının belirlenmesi, şifreleme standartlarının (örneğin güncel SSL/TLS protokolleri) uygulanması ve bağımsız bir kurum tarafından sızma testinin (penetration test) gerçekleştirilmesi asgari güvenlik prosedürleri arasında yer almalıdır [5]. Bu prosedürlerin eksikliği, sistemleri dış saldırılara açık hale getirirken, sistem yöneticisinin defansif tutumu da iyi niyetli

uyarıların dikkate alınmasını engellemektedir. Ayrıca, sistem yöneticisinin bu tür standart prosedürleri uygulamaması, KVKK kapsamında veri sorumlusu olan kurumun idari para cezalarıyla karşı karşıya kalmasına neden olabilmektedir.

Bu durumun pratik sonuçları, KKTC'de yakın zamanda yaşanan siber güvenlik olaylarında acı bir şekilde görülmüştür. Örneğin, 2026 yılında KKTC Sağlık Bakanlığı sistemlerinde yaşanan ve 364 binden fazla kişinin sağlık ve kimlik bilgilerinin sızdırılmasıyla sonuçlanan veri ihlali, siber güvenliğin ne kadar kritik olduğunu göstermiştir [6]. İyi niyetli bir araştırmacı bu açığı önceden fark edip bildirseydi ve bu bildirim yetkin bir sistem sorumlusu tarafından profesyonelce dikkate alınsaydı, böylesi bir felaket önlenebilirdi. Benzer şekilde, KKTC Çalışma İzinleri Portalı'na yapılan saldırılar da, sistemlerin dışarıdan gelecek iyi niyetli uyarılara ve liyakatli sistem yöneticilerine ne kadar muhtaç olduğunu kanıtlamaktadır [7].

Türkiye ve Kıbrıs'ta Sistem Nasıl İşliyor?

Türkiye'de "Sorumlu Açık Bildirimi" (Responsible Disclosure) süreci son yıllarda kurumsallaşmaya başlamıştır. Türkiye Siber Güvenlik Başkanlığı (SGB), zafiyet bildirimleri için resmi bir portal kurarak süreci belirli kurallara bağlamıştır. Türkiye'de bir açık bulan araştırmacı, bunu doğrudan SGB'ye bildirebilmektedir. SGB, bildirilen açığı doğruladıktan sonra üretici firmaya iletmekte ve zafiyetin kritiklik derecesine göre 1 ila 4 hafta arasında kapatılmasını beklemektedir. Açık kapatıldıktan sonra ise araştırmacının ismi "Zafiyet Bildirimi Onur Listesi"nde yayınlanmaktadır [8]. Ayrıca Arçelik ve İş Bankası gibi büyük Türk şirketleri de kendi iç zafiyet bildirim prosedürlerini (Bug Bounty programları) oluşturarak, kurallara uyan araştırmacılara hukuki yaptırım uygulamayacaklarını taahhüt etmekte ve hatta onları finansal olarak ödüllendirmektedirler [9]. Bu yaklaşım, güvenlik araştırmacılarını sisteme zarar vermeden çalışmaya teşvik eden en sağlıklı modeldir.

Buna karşın, Kıbrıs Cumhuriyeti ve KKTC'de süreç oldukça belirsizdir. Kıbrıs Cumhuriyeti'nde Dijital Güvenlik Otoritesi (DSA) siber güvenlik alanında bölgesel merkez olma vizyonuyla hareket etse de, henüz Türkiye'deki gibi standartlaşmış, merkezi ve araştırmacıyı koruyan bir ulusal zafiyet bildirim prosedürü yaygınlaşmamıştır. KKTC'de ise ne Bilgi Teknolojileri ve Haberleşme Kurumu (BTHK) bünyesinde resmi bir bildirim portalı ne de şirketlerin yayınladığı açık bir politika bulunmaktadır. Bu nedenle Kıbrıs'ta açık bulan bir kişi, doğrudan kurumla iletişime geçmek zorunda kalmakta ve her an "yetkisiz erişim" suçlamasıyla yüzleşme riski taşımaktadır. Bu belirsizlik, adadaki siber güvenlik yeteneklerinin gelişmesini engellemekte ve sistemleri dış tehditlere karşı daha kırılgan hale getirmektedir.

Takip Mekanizması ve Küresel Yaptırımlar

Sorumlu açık bildirimi sürecinin en kritik aşaması, bildirimin yapılmasından sonraki "takip ve yaptırım" sürecidir. Zafiyeti bildiren kişinin iyi niyetli davranışı neticesinde, resmi sorumlu kurumun (örneğin BTHK) ilgili sistem sahibine resmi bildirimde bulunması yeterli değildir. Bu açığın yasal sürede kapatılıp kapatılmadığının düzenli olarak kontrol edilmesi zorunludur. Eğer sistem sahibi, kendisine tanınan makul süre (genellikle dünyada 45 ila 90 gün) içerisinde bu zafiyeti gidermezse, ağır yaptırımların devreye girmesi gerekmektedir. Aksi takdirde bildirim mekanizması işlevsiz kalacaktır.

Dünya genelinde bu mekanizma oldukça katı kurallarla işletilmektedir. Örneğin, ABD Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), Koordineli Zafiyet Bildirimi programı kapsamında, kritik altyapı sistemlerindeki açıkları üretici firmaya bildirdikten sonra süreci yakından takip eder [10]. Eğer üretici firma 45 gün içinde açığı kapatmazsa, CISA bu açığı kamuoyuyla (KEV Kataloğu üzerinden) paylaşma yetkisine sahiptir. Hatta kritik sistemlerde, açık kapatılıncaya kadar söz konusu sistemin internet erişiminin askıya alınması veya ağdan izole edilmesi (hizmet kesme) uygulanmaktadır. Bu tür sert müdahaleler, sistem güvenliğinin kurumun inisiyatifine bırakılamayacak kadar önemli olduğunu göstermektedir.

Avrupa Birliği'nde ise Genel Veri Koruma Tüzüğü (GDPR) çerçevesinde benzer bir süreç işler. Bir zafiyet bildirildiği halde sistem sahibi tarafından kapatılmaz ve bu durum bir veri ihlaline yol açarsa, ilgili kuruma küresel cirosunun %4'üne veya 20 milyon Euro'ya kadar devasa para cezaları kesilmektedir [11]. Ayrıca Google Project Zero gibi inisiyatifler, sistem sahiplerine 90 günlük katı bir süre tanır; bu süre dolduğunda açık yamalanmamış olsa bile tüm detaylarıyla internette ifşa edilir [12]. Bu tür ifşa ve ceza mekanizmaları, sistem sahiplerini "açığı görmezden gelme" lüksünden mahrum bırakır ve onları proaktif bir güvenlik anlayışına zorlar.

Çözüm Yolları ve Sektörel Fırsatlar

Bu çıkmazı aşmak için hukuki zeminde "Sorumlu Açık Bildirimi" kavramının tanımlanması gerekmektedir. KKTC mevzuatında, iyi niyetli güvenlik araştırmacılarını koruyan istisnai hükümler acilen getirilmelidir. Bir açık, sisteme zarar vermeden, veriler kopyalanmadan veya değiştirilmeden tespit edilmiş ve sadece sistem sahibine gizlilik içinde bildirilmişse, bu eylem suç kapsamından çıkarılmalıdır. Bu hukuki koruma, araştırmacıların yeteneklerini yeraltı dünyası yerine toplumsal fayda için kullanmalarının önünü açacaktır.

Ancak sadece araştırmacıyı korumak yetmez; sistem sahibinin de kendisine bildirilen bir açığı makul bir süre içinde kapatma yükümlülüğü yasal olarak tanımlanmalıdır. Eğer resmi kurum tarafından bildirilen açık belirtilen sürede kapatılmazsa, sistemin güvenlik gereği sorunu çözülünceye kadar erişime kapatılması değerlendirilmelidir. Açığın kötü niyetli kişilerce kullanılması durumunda, bildirimi görmezden gelen sistem sahibi ve yetersiz sistem yöneticisi KVKK kapsamında birincil derecede sorumlu tutulmalı ve ağır yaptırımlara çarptırılmalıdır. Bu yaptırımlar, sadece para cezası ile sınırlı kalmamalı, ihmali bulunan sistem yöneticilerinin mesleki sertifikasyonlarının iptali veya görevden alınması gibi sonuçlar da doğurmalıdır.

Sorumlu açık bildirimi mekanizmalarının yasal güvence altına alınması, KKTC'de siber güvenlik sektörünün gelişimine büyük bir ivme kazandırır. Etik hackerların desteklendiği bir ekosistem, yerel yeteneklerin keşfedilmesini teşvik eder. Şirketler, dışarıdan gelen iyi niyetli bildirimleri bir tehdit değil, bedelsiz bir güvenlik denetimi olarak görmeye başladığında, genel güvenlik seviyesi hızla yükselecektir. Ayrıca, sistem yöneticilerinin sertifikasyon zorunluluklarının getirilmesi, adadaki bilişim profesyonellerinin küresel standartlara ulaşmasını sağlayacaktır.

Sonuç ve Öneriler

Dijital dünyada kapılarımızı tamamen kapatmak imkansızdır. Önemli olan, kapıyı zorlayan kişinin niyetini doğru okuyabilmek ve bu niyeti sistemin yararına kullanabilmektir. KKTC mevzuatı, kötü niyetli saldırganları cezalandırırken, iyi niyetli araştırmacıları koruyacak esnekliğe kavuşturulmalıdır.

Bu sürecin sağlıklı işletilmesi için şu adımlar atılmalıdır:

İlk olarak, Bilişim Suçları Yasası'na "Sorumlu Açık Bildirimi" istisnası eklenmeli ve yetkisiz erişimin hangi şartlarda suç sayılmayacağı net bir şekilde tanımlanmalıdır.

İkinci olarak, KKTC'deki kamu ve özel sektör sistem yöneticileri için uluslararası geçerliliği olan (CISSP, CompTIA Security+ vb.) sertifikasyon zorunlulukları getirilmelidir. Çevrimiçi sistemler kuruma alınırken bağımsız güvenlik denetimleri ve sızma testleri standart bir prosedür haline getirilmelidir.

Üçüncü olarak, Türkiye'deki SGB modeline benzer şekilde, BTHK bünyesinde araştırmacıların buldukları açıkları güvenli bir şekilde bildirebileceği resmi bir platform oluşturulmalıdır.

Dördüncü olarak, bildirimi alan BTHK'nın, sistem sahibine resmi bildirim yaptıktan sonra açığın kapatılıp kapatılmadığını periyodik olarak kontrol etmesini sağlayacak yasal bir takip mekanizması kurulmalıdır.

Beşinci olarak, bildirilen açıkları makul sürede kapatmayan kurumlar için KVKK kapsamında caydırıcı yaptırımlar uygulanmalı; gerekirse kritik sistemler için açık kapatılana kadar erişim engeli veya hizmet kesintisi devreye sokulmalıdır.

Son olarak, kurumların bilgi işlem yöneticileri, dışarıdan gelen bildirimleri bir saldırı değil, bir iyileştirme fırsatı olarak görmeleri yönünde eğitilmelidir. İyi niyetli hackerları düşman değil, dijital dünyamızın gönüllü bekçileri olarak görmenin zamanı çoktan gelmiştir. Güvenlik, sessiz kalarak değil, şeffaf ve işbirliğine dayalı bir ekosistem inşa edilerek sağlanabilir.

Referanslar

[1] KKTC Bilişim Suçları Yasası (32/2020), Bilgi Teknolojileri ve Haberleşme Kurumu (BTHK) (https://www.bthk.org/Documents/yasa-duzenleme/Bili%C5%9Fim%20Su%C3%A7lar%C4%B1%20Yasas%C4%B1.pdf) .
[2] KKTC Kişisel Verilerin Korunması Yasası (89/2007), Kişisel Verileri Koruma Kurulu.(https://kvkk.gov.ct.tr/Portals/24/89-2007%20Kisisel%20Verilerin%20Korunmas%20Yasasi.pdf)
[3] Türk Ceza Kanunu (TCK) Madde 243 ve 244, Penetrasyon Testi ve Hukuk Değerlendirmesi (https://altinyuzuk.av.tr/bilisim-suclari-turk-ceza-kanunu-m-243-244/).
[4] "Siber Güvenlik Sertifikasyonları: CEH, CISSP ve Daha Fazlası", BT Akademi, 24 Mayıs 2024 (https://www.btakademi.com/blog/siber-guvenlik-sertifikasyonlari-ceh-cissp-ve-daha-fazlasi).
[5] "KVKK – Teknik Tedbirler ve Sistem Yöneticisi Rehberi", Birol Bozkurt, 10 Nisan 2020 (https://bbozkurt.wordpress.com/2020/04/10/).
[6] "Sağlık Bakanlığı sistemlerine yapılan siber saldırı sonucu 364 bin kişinin verileri sızdırıldı", Yeni Düzen Gazetesi, 22 Haziran 2026 (https://www.yeniduzen.com/tarihi-skandal-196573h.htm).
[7] "Çalışma İzinleri Portalı'na siber saldırı girişimi", KKTC Çalışma ve Sosyal Güvenlik Bakanlığı Açıklaması, Haziran 2026 (https://www.kibrispostasi.com/c35-KIBRIS_HABERLERI/n605807-bakanlik-acikladi-calisma-izinleri-portalina-izinsiz-erisim-girisiminde-supheli-yakalandi).
[8] T.C. Siber Güvenlik Başkanlığı Zafiyet Bildirim Politikası, (https://siberguvenlik.gov.tr/zafiyet-bildirim-politikasi).
[9] Arçelik Zafiyet Bildirim Prosedürü ve Onur Listesi Uygulamaları, (https://www.arcelikglobal.com/zafiyet-bildirim-proseduru/, https://www.arcelikglobal.com/zafiyet-bildirimi-onur-listesi/).
[10] Coordinated Vulnerability Disclosure Program, Cybersecurity and Infrastructure Security Agency (CISA),(https://www.cisa.gov/resources-tools/programs/coordinated-vulnerability-disclosure-program).
[11] Fines and Penalties, General Data Protection Regulation (GDPR) Information Portal (https://gdpr-info.eu/issues/fines-penalties/).
[12] Vulnerability Disclosure Policy, Google Project Zero (https://projectzero.google/vulnerability-disclosure-policy.html).

Kazım Ateş
Elektronik ve Bilişim Uzmanı

WhatsApp yakında bu telefonlarda kullanılamayacak!

WhatsApp'ın sistem gereksinimleri, uygulamanın en son güvenlik güncellemeleriyle korunmasını sağlamak için her yıl güncelleniyor. Bu bağlamda yakında bazı iPhone ve Android cihazlarda çalışmayacak - **Kaynak: donanimhaber.com**

Meta, WhatsApp'ın Android ve iOS cihazlarda çalışması için gereken yazılım gereksinimlerini bir kez daha güncelledi. 8 Eylül 2026 itibarıyla uygulama yalnızca Android 6 veya üzeri sürümlerde desteklenecek. 30 Kasım 2026'dan itibaren ise yalnızca iOS 15.5 veya daha yeni sürümleri çalıştıran iPhone'larda desteklenecek.
WhatsApp'ın sistem gereksinimleri, uygulamanın en son güvenlik güncellemeleriyle korunmasını sağlamak için her yıl güncelleniyor. Şirket, işletim sistemlerini analiz ettiğini ve en az kullanıcısı olan en eski işletim sistemlerine desteği kestiğini belirtiyor. Geçen yıl, minimum gereksinimi iOS 15.1 ve Android 5.0'a yükseltmişti.
30 Kasım 2026 itibarıyla iOS 15.5 ve daha yeni iOS sürümleri desteklenecek.
8 Eylül 2026 tarihinden itibaren yalnızca Android 6 ve daha yeni Android sürümleri desteklenecek
WhatsApp neden desteği kesiyor?
WhatsApp, “Cihazlar ve yazılımlar sık sık değişiyor, bu nedenle desteklediğimiz işletim sistemlerini düzenli olarak gözden geçiriyor ve güncellemeler yapıyoruz. Ayrıca bu cihazlar en son güvenlik güncellemelerini almamış olabiliyor ya da WhatsApp'ı çalıştırmak için gereken işlevselliğe sahip olmayabiliyor.” diyor.

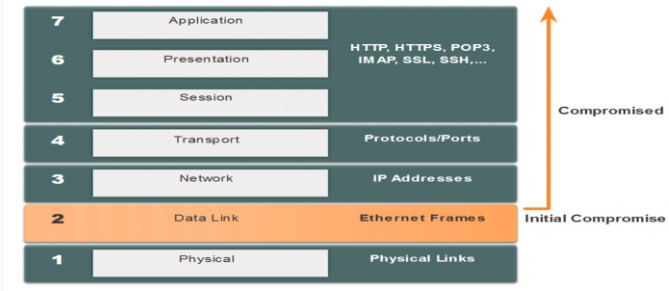
Layer 2 Saldırıları ve Önleme Teknikleri -1-

Bu yazımda sizlere OSI Reference Model katman 2'deki tehditleri ve açıkları tesbit edip nasıl tedbir alınması gerektiğni anlatacağım. Zaafiyetler,Switch Saldırı Kategorileri ve önleme tekniklerinden örnekler vereceğim. Daha önce lab ortamında ve gerçek network üzerindeki deneyimleri aktaracağım.Tabiiki layer 2 saldırı konuları çok geniş bir konu olduğundan burda hepsi anlatılmamaktadır.Burda yazıyı okuyanlar bu saldırı tekniklerini gerçek network yerine isole olmuş networkte denemelidir. Bununla beraber ilgili savunma teknikleri networkümüzde uygulanması faydalı olacaktır. Bu yazımı yazarken 16-18 Mayıs 2022 de Kemerde düzenlenen 14. Tübitak Ulaknet Çalıştayı Layer 2 Saldırıları ve Önleme Teknikleri sunumundan yararlandım. Bu yazıyı okuduktan sonra uygulamak tamamiyle ilgili kişi sorumluluğundadır.Bu yazının yazarını bağlamamaktadır.

Amaçlar :

- OSI Reference Katman 2 de tehditleri ve açıkları öğrenip tedbir almak.
- Zaafiyetler
- Switch Saldırı Kategorileri
- Saldırı Önleme Teknikler
- Örneklerle lab ortamı bazı tecrübeleri paylaşmak
- Yazım tüm layer 2 saldırı ve tedbirlerini kapsamamaktadır
- Bu yazımı ileriki zamanında workshop ortamına taşıyarak öğrenmek isteyenlerle paylaşmak.

OSI ve Layer 2 Zaafiyetler
L3-L7 Güvenlik(Firewall,IPS,VPN)



Şekil 1: L2 saldırıların diğer katmanlardaki güvenlikle ilişkisi

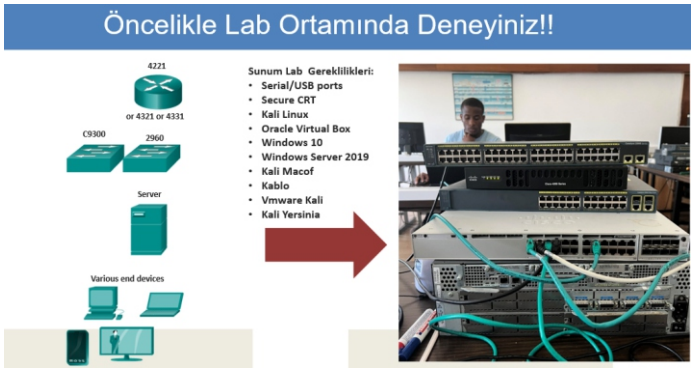
Şekil 1 de görüldüğü gibi L2 de meydana gelebilecek sızıntıların L3-L7 Güvenlik (Firewall,IPS,VPN vs) çözümleri nasıl savunmasız bırakabileceğini görmekteyiz. Yani pratik yaşamdaki deyişle switch configurasyonlarında özellikle port tanımlamalarında yapılacak yanlışlıklar tüm katmanları da doğrudan etkileyecektir.

Konu Kaynakları:

Konunun tam anlaşılabilmesi için CCNA: Switching, Routing, and Wireless Essentials kursu ve CEH v11+ Study Guide beraber değerlendirilmesi çok faydalı olacaktır.

Öncelikle lab ortamınızı oluşturun ve herşeyin denemesini burda yapınız.Burdaki elde edeceğiniz neticeler doğrultusunda doğrudan onay alarak ölü bir zamanda gerçek network üzerinde de deneyebilirsiniz. Herşey hazır olduktan sonra onay aldığınız network üzerinde tüm denemeleriniz ve geri dönüşleriniz 1 dakik içerisinde tamamlanacaktır.

Yukarda oluşturulan lab ortamında Cisco router ve switchler bulunmaktadır. Diğer ara ve saldırı ürünleri resimde gösterilmektedir.Sunum 2020 de gerçekleştirildiğinden windows



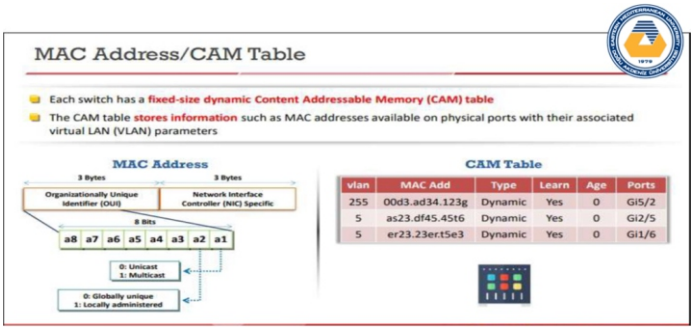
ortamı version 10 idi. Özellikle lab ortamında Kali Macof ve Kalli Yersiniayı saldırı aleti olarak kullanacağız. Özellikle Cisco switchlerde Port Security ve benzeri tedbirler alınmazsa Macof(CAM Table Flooding) ve Yersina (DHCP, STP, DTP, CDP) saldırıları halen etkilidir. Zamanla bu araçların yerini Responder, Scapy ve mitm6 almıştır.

Ben yazımda daha çok aşağıdaki saldırı türlerini anlatacağım

- MAC TABLE Saldırıları ve Port Security
- VLAN Saldırıları ve Auto Trunk Protokolleri
- DHCP Saldırıları ve Port Security

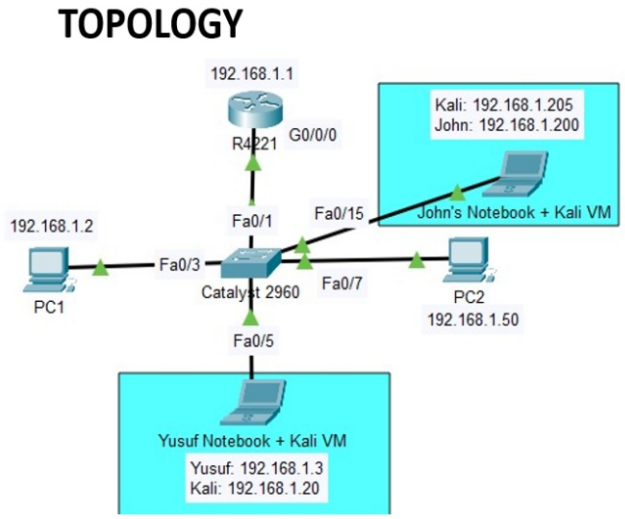
ARP, Address Spoofing ve STP Saldırıları.

MAC Adress ve CAM Table hakkında bilinmesinde yararlı bilgiler:

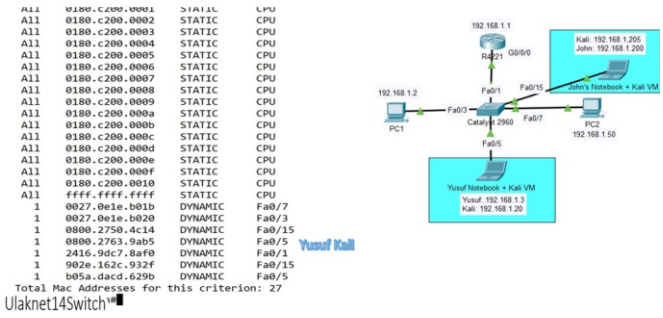


- Switch Sınırlı MAC Kapasite herkes biliyor (4096,8096,32768,132000)
- Macof 1 dakikada 131000 sahte (Bogus) MAC gönderebiliyor
- CAM Tablosu olarak biliniyor
- CAM Tablosu dolan Switch Hub'a dönüşüyor
- Huba dönüşen switch kısa zamanda CPU process nedeniyle çökebiliyor
- Hub'a dönüşen switch tüm frameler sniff yapılabiliyor
- Sniff yapılan port çalınabiliyor
- Çalınan Port MITM saldırısına dönüşüyor

MAC Saldırı yöntemi Port Security içeriği ile önlenilir.Her üretici firmanın Port Security içeriği vardır.



Saldırı Öncesi MAC Adress Tablosu son durumu



Mevcut MAC Adress 8088 boş

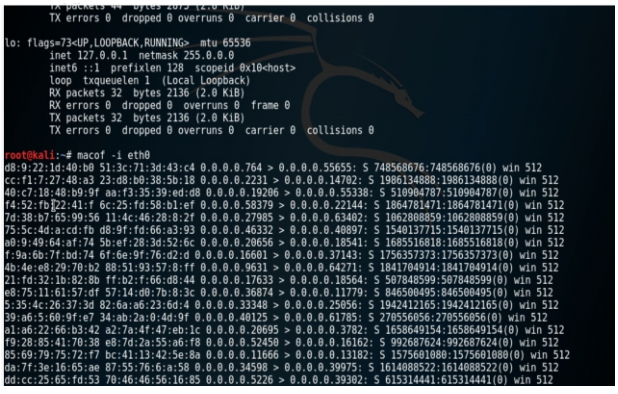
```
Ulaknet14Switch#sh mac address-table  count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 7
Static  Address Count  : 0
Total Mac Addresses    : 7

Total Mac Address Space Available: 8088

Ulaknet14Switch#
```

Switch CAM table boş 8088 MAC address daha alma kapasitesi var.



MAC Adres tablosu doldu

```
ulaknet13switch#sh mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 8088
Static  Address Count  : 0
Total Mac Addresses    : 8088

Total Mac Address Space Available: 0
```

MAC ADRESS 0

```
Ulaknet14Switch#
```

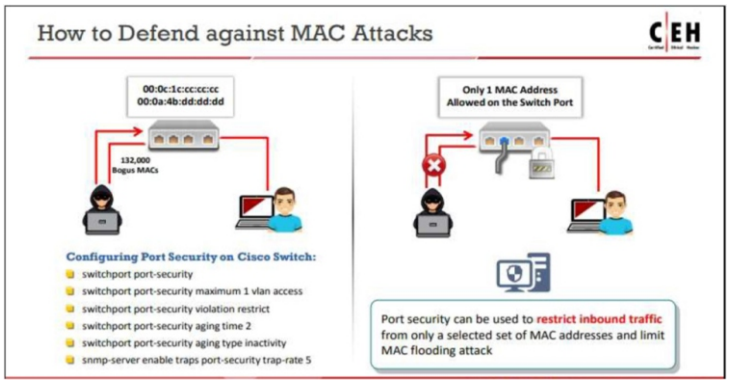
Kali Macof saldırısından sonra switch tüm kapasitesini dolduruyor.

CPU %97

```
Ulaknet14Switch#sh processes cpu
CPU utilization for five seconds: 97%/5%; one minute: 49%; five minutes: 39%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         4          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2           0      1672          0  0.00%  0.00%  0.00%   0 Load Meter
   3          69        48       1437  0.00%  0.00%  0.00%   0 SpanTree Helper
   4        2654       853       3111  0.00%  0.01%  0.00%   0 Check heaps
   5           0         8          0  0.00%  0.00%  0.00%   0 Pool Manager
   6           0         2          0  0.00%  0.00%  0.00%   0 Timers
   7         514      2806        183  0.00%  0.00%  0.00%   0 ARP Input
   8           0         1          0  0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
   9           0         2          0  0.00%  0.00%  0.00%   0 AAA high-capacit
  10           0         1          0  0.00%  0.00%  0.00%   0 Policy Manager
  11          17         3       5666  0.00%  0.00%  0.00%   0 Entity MIB API
  12           0         1          0  0.00%  0.00%  0.00%   0 IFS Agent Manage
  13          40      2081         19  0.00%  0.00%  0.00%   0 HC Counter Timer
  14           0         2          0  0.00%  0.00%  0.00%   0 XML Proxy Client
  15           0         1          0  0.00%  0.00%  0.00%   0 HRPC asic-stats
  16           0         1          0  0.00%  0.00%  0.00%   0 Critical Bkgnd
  17         278      3553         78  0.00%  0.02%  0.00%   0 Net Background
  18          16        98        163  0.00%  0.00%  0.00%   0 Logger
  19          34      8191          4  0.00%  0.00%  0.00%   0 TTY Background
  20         294      8246         35  0.00%  0.00%  0.00%   0 Per-Second Jobs
  21        1212       144       8416  0.00%  0.00%  0.00%   0 Per-minute Jobs
--More--
```

Switch CPU Process %97 ye ulaşarak çalışmaz hale geliyor yada bir aptal huba dönüşüyor.

ÇÖZÜM: Port Security içeriğini kullanmayınız. Sahte MAC saldırısına izin vermeyiniz. Her üretici marka switchde port security içeriği bulunmaktadır.



Tabiki Her Erişim Interface Korunmalı.

```
interface FastEthernet0/3
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0027.0e1e.b020
!
.
interface FastEthernet0/15
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 902e.162c.932f
```

Kural İhlali durumunda:

```
Ulaknet14Switch(config)#int fa0/3
Ulaknet14Switch(config-if)#swi
Ulaknet14Switch(config-if)#switchport po
Ulaknet14Switch(config-if)#switchport port-security vio
Ulaknet14Switch(config-if)#switchport port-security violation ?
      protect   Security violation protect mode
      restrict  Security violation restrict mode
      shutdown  Security violation shutdown mode

    Ulaknet14Switch(config-if)#switchport port-security violation
```

Kural ihlali durumunda insiyatif sizin elinizdedir.İster doğrudan portunu kapatın veya kara listeye alın.

Yeni Saldırı Öncesi CAM Tablosu boş durumda

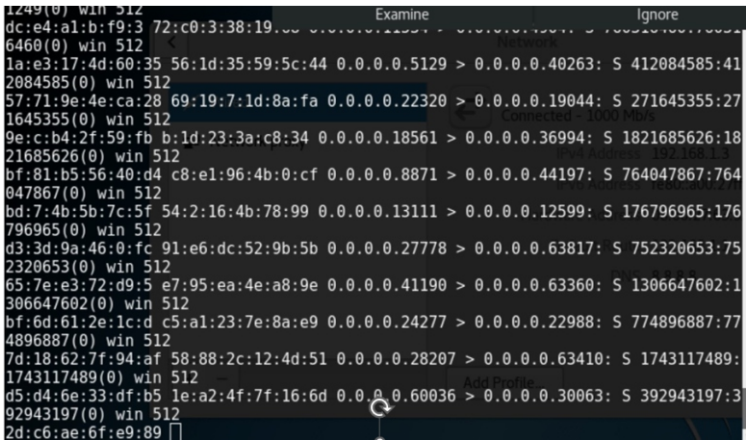
```
Ulaknet14Switch#sh mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 3
Static  Address Count  : 2
Total Mac Addresses    : 5

Total Mac Address Space Available: 8090

Ulaknet14Switch#
```

Port Security konfigurasyonu yapıldıktan önceki switch CAM Table durumu.



Her iki Saldırgan KALİ PORTU FA0/5 ve FA0/15 devre dışı oluyor

```
00:42:29: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/5, putting Fa0/5 in err-disable state
00:42:29: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0800.2763.9ab5 on port Fast
thernet0/5.
00:42:30: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down.

00:43:35: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/15, putting Fa0/15 in err-disable state
00:43:35: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0800.2750.4c14 on port FastE
thernet0/15.
00:43:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/15, changed state to down.
```

MAC adres tablosunda bir zarar yok.

```
Ulaknet14Switch#sh mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 2
Static  Address Count  : 1
Total Mac Addresses    : 3

Total Mac Address Space Available: 8092
```

Peki Sizce?

Peki Daha Üst Bir Switch Kullansak ???

SONUÇ:

Layer 2 Saldırı ve Önleme teknikleri ile ilgili yazımın ilk kısmında L2 saldırılarını tanıttık. Kendi lab ortamımız topolojisini oluşturduk. Kali MACOF saldırısı ile switchin nasıl çöktüğünü gördük. Port Security içeriğini nasıl bu saldıryı önlediğini anlattım:Ekim sayısında ayni konuya devam ediyorum.

İsteyen herkes bana e-mail veya cep telefonu üzerinden erişebilir.

YUSUF KÜÇÜK
yusufkucuk2014@gmail.com

Bilgi Güvenliği: Sorun Donanım Değil, Yönetim

Son dönemde ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi üzerine yoğunlaştım; Lead Implementer eğitimini ve sertifikasyon sürecini tamamladım. Bu süreçte üzerinde en fazla düşündüğüm soru teknoloji veya teknik değildi:

Neden bilgi güvenliği denildiğinde aklımıza ilk olarak firewall, antivirüs veya dışarıdan gelecek siber saldırılar geliyor?

Standart, teknolojiden önce çok daha temel sorular sorduruyor: Neyi koruyoruz? Risklerimizi biliyor muyuz? Kim sorumlu? Yönetim bunu sahipleniyor mu? Bir çalışan ayrıldığında süreç aynı şekilde devam ediyor mu? Ve en önemlisi: **Kurduğumuz sistem gerçekten yaşıyor mu?**

Bu soruların cevabı yalnızca büyük şirketler için önemli değil. Tam tersine, adamızda sınırlı insan kaynağı ve bütçeyle ayakta durmaya çalışan KKTC KOBİ'leri için çok daha kritik.

"Bize Dışarıdan Talep Gelmiyor" Yanılgısı

KKTC'deki işletme sahipleriyle konuştuğumda sıklıkla şu haklı tespitle karşılaşıyorum:

"Biz AB ile çalışmıyoruz, Türkiye'den de bankalar dışında kimseden böyle bir sertifika veya güvenlik talebi gelmiyor."

Bu tespit yerel pazarın bir gerçeği. Ancak dışarıdan gelen bir zorunluluğun olmaması, siber ve operasyonel risklerin adamızda olmadığı anlamına da gelmiyor.

Çünkü bir işletmenin bilgi güvenliği riski yalnızca dışarıdan gelecek bir saldırıyla ortaya çıkmaz. Yanlış verilen bir erişim yetkisi, kapatılmamış bir kullanıcı hesabı, test edilmemiş bir yedek, yanlış kişiye gönderilen bir dosya veya kritik bir işlemin yalnızca bir çalışanın bilgisine bağlı olması da işletme için ciddi sonuçlar doğurabilir.

ISO 27001'in amacı da her işletmeye binlerce dolarlık güvenlik yazılımları aldırmak değildir. Önce kurumun neyi koruması gerektiğini ve hangi risklerle karşı karşıya olduğunu anlamasını, ardından bu risklere uygun önlemleri sistematik biçimde yönetmesini ister.

KOBİ'lerin en önemli avantajı esnek organizasyon yapıları ve hızlı karar alma mekanizmaları dır. Aslında doğru yaklaşım benimsendiğinde KOBİ'lerde birçok iyileştirme büyük kurumlara göre çok daha hızlı hayata geçirilebilir.

Yedek Alıyoruz. Peki Geri Dönebiliyor muyuz?

Sahada sıkça karşılaştığımız basit bir örnek üzerinden gidelim.

Yaklaşık 15 çalışanı olan bir işletme. Güncel antivirüs yazılımları kullanılıyor, firewall mevcut ve şirket verileri her gece otomatik olarak yedekleniyor.

Yöneticiye "Verileriniz güvende mi?" diye sorulduğunda cevabı oldukça doğal:

"Evet, her gece yedek alıyoruz."

Sonra basit bir soru geliyor:

"En son ne zaman yedekten geri döndünüz?"

Bu sorunun cevabı çoğu zaman o kadar net olmayabiliyor.

Yedekleme sistemi yıllardır görevini yapıyor ve her gece işlemin başarıyla tamamlandığını bildiriyor olabilir. Ancak hangi verinin ne sıklıkta yedeklenmesi gerektiği belirlenmemiş, işletmenin ne kadar veri kaybını kabul edebileceği konuşulmamış, bir kriz durumunda sistemlerin ne kadar sürede geri dönebileceği ölçülmemiş veya düzenli geri yükleme testinin kim tarafından yapılacağı tanımlanmamış olabilir.

Burada yedekleme teknolojisi görevini yapıyor; sorun orada değil. Asıl boşluk, kurulu bu kontrolün kim tarafından, ne sıklıkta ve nasıl yönetileceğinin tanımlanmamış olmasında

Yedek almak teknik bir kontroldür. Hangi verinin ne sıklıkta yedekleneceğine karar vermek planlamadır. Yedekleme işleminin düzgün çalıştığını izlemek kontroldür. Verinin gerçekten geri getirilebildiğini test etmek doğrulamadır. Bir sorun bulunduğunda süreci değiştirmek ise iyileştirmedir.

Bütün bunların kim tarafından yapılacağını belirlemek ve gerekli kaynağı sağlamak da yönetimin sorumluluğudur.

Bir güvenlik kontrolünün kurulmuş olması, o riskin yönetildiği anlamına gelmez.

ISO 27001'in KOBİ açısından gerçek değeri de tam burada ortaya çıkar: Güvenlik kontrollerinin yalnızca kurulmasını değil, zaman içinde planlanmasını, izlenmesini, değerlendirilmesini ve sürekli iyileştirilmesini sağlayan bir yönetim disiplini oluşturmak.

Sertifikadan Önce İş Sürekliliği ve Yönetim Disiplini

ISO 27001 konuşulunca adamızda ilk hedef genellikle duvara asılacak "o belgeyi almak" oluyor.

Oysa dışarıdan bir zorunluluk olmasa bile asıl kazanım, kritik süreçleri kişilere ve tesadüflere bağımlı olmaktan çıkarıp iş sürekliliğini güçlendirmekte yatıyor

Sertifika elbette değerlidir. Kurumun bilgi güvenliğini belirli bir disiplin içinde yönettiğini müşterilere ve iş ortaklarına göstermenin güçlü yollarından biridir.

Ancak asıl değer, sertifikaya ulaşırken oluşturulan yönetim sistemidir.

Risklerin belirlenmesi, sorumlulukların tanımlanması, gerekli kaynakların ayrılması, kontrollerin uygulanması, sonuçların izlenmesi ve sistemin sürekli iyileştirilmesi…

Başka bir ifadeyle ISO 27001'in amacı, güvenliği yalnızca IT personeline veya dışarıdan çağrılan "bilgisayarcıya" bırakılan teknik bir konu olmaktan çıkarıp kurumun yönettiği bir iş sürecine dönüştürmektir.

Teknoloji kontrolü sağlar; yönetim sistemi ise o kontrolün zaman içinde çalışmaya devam etmesini sağlar.

KKTC KOBİ'leri Nereden Başlamalı?

1. Neyi Korumak Zorunda Olduğunuzu Bilin

Müşteri kayıtları, muhasebe verileri, sözleşmeler, çalışan bilgileri, proje dosyaları, kaynak kodları…

Önce işletmeniz açısından kritik olan bilgi varlıklarını belirleyin.

Çünkü neyi koruduğunuzu bilmiyorsanız, ona yönelik riskleri de doğru değerlendiremezsiniz.

Bu çalışma pahalı yazılımlar gerektirmeden basit bir tabloyla başlayabilir. Küçük bir işletmede yapılacak ilk çalışma bile daha önce görünmeyen önemli riskleri ortaya çıkarabilir.

2. Risklerinizi Önceliklendirin

Her riski aynı anda ortadan kaldırmaya çalışmak hem pahalı hem de gerçekçi değildir.

Eski çalışanların açık kalmış hesapları, gereğinden fazla erişim yetkileri, test edilmeyen yedekler veya kontrolsüz dış erişimler, pahalı güvenlik yatırımlarından önce ele alınması gereken riskler olabilir.

Yaklaşımın KOBİ için en önemli avantajı da burada ortaya çıkar:

Her şeyi yapmak değil, önce en önemli riskleri yönetmek.

3. Bilgi Güvenliğini IT'nin Omuzlarından Alın

KOBİ'lerde en sık karşılaşılan yanılgılardan biri de bilgi güvenliğini yalnızca IT'nin işi sanmak.

İnsan kaynakları yeni bir çalışan işe başladığında veya bir çalışan ayrıldığında erişim süreçlerinin parçasıdır. Muhasebe finansal verileri, satış ekibi müşteri bilgilerini işler. Dışarıdan hizmet alınan firmalara verilen erişimler de yönetilmelidir.

Yönetimin görevi ise sorumlulukları belirlemek, gerekli kaynakları sağlamak ve sistemin gerçekten çalıştığından emin olmaktır.

Teknik ekip güçlü olabilir; ancak kurumsal sahiplenme yoksa bilgi güvenliği sürdürülebilir olmaz.

4. Sistem Kurup Dosyaya Kaldırmayın, Yaşatın

Yeni bir çalışan gelir, yeni bir yazılım alınır, bulut sistemine geçilir, bir tedarikçiye sistem erişimi verilir veya yeni bir tehdit ortaya çıkar.

Riskler değişir.

Bu yüzden bilgi güvenliğini bir projeden çok, kurumun sürekli sürdürdüğü bir alışkanlık olarak görmek gerekir.

Planla → Uygula → Kontrol Et → İyileştir.

Bu döngü tekrarlandıkça bilgi güvenliği bir dokümantasyon çalışması olmaktan çıkar ve kurumun günlük çalışma biçiminin parçası haline gelir.

Büyük Bütçeden Önce Yönetim Disiplini

KOBİ'lerin bilgi güvenliğindeki en önemli avantajlarından biri, düşündüklerinden daha fazla kontrolün kendi ellerinde olmasıdır.

Bazı riskler elbette teknolojik yatırım gerektirir. Ancak birçok iyileştirme; eski kullanıcı hesaplarının kapatılması, erişim yetkilerinin gözden geçirilmesi, sorumlulukların belirlenmesi, çalışanların bilinçlendirilmesi, yedeklerin test edilmesi ve kritik bilgi varlıklarının kayıt altına alınması gibi adımlarla başlayabilir.

Bunların çoğu büyük bütçelerden önce **yönetim disiplini** gerektirir.

Belki de ISO 27001'in KOBİ'ye kazandırabileceği en önemli düşünce biçimi şudur:

“Hangi ürünü almalıyım?” sorusundan önce “Hangi riski yönetmeliyim?” diye sormak.

Altı Soruda işletmenizin hazırlık durumunu

Dış denetimleri veya sertifikasyonu bir kenara bırakın ve işletmenize şu altı soruyu sorun:

1. Kritik verilerinizin nerede olduğunu ve kimlerin erişebildiğini net olarak biliyor musunuz?

2. Bir çalışan bugün işten ayrılsa tüm sistem ve e-posta erişimleri aynı gün kapatılır mı?

3. Yönetim, bilgi güvenliğini bir maliyet kalemi olarak mı yoksa iş sürekliliğinin ve kurumsal risk yönetiminin parçası olarak mı görüyor?

4. Sunucunuz veya kritik sistemlerinizden biri yarın çalışmaz hale gelse, yedeklerden ne kadar sürede dönebileceğinizi gerçekten test ettiniz mi?

5. Çalışanlarınız oltalama (phishing) e-postalarını, şüpheli bağlantıları veya yanlış kişiye veri gönderme riskini tanıyor mu?

6. Dışarıdan hizmet aldığınız yazılımcı, muhasebeci, danışman veya IT firması hangi sistemlerinize ve verilerinize erişebiliyor? Bu erişimlerin tamamı hâlâ gerekli mi?

Bu sorular bir ISO 27001 uygunluk değerlendirmesi değildir ve kurumunuzun belgelendirmeye hazır olup olmadığını tek başına göstermez.

Ancak cevap verirken zorlandığınız her soru, üzerinde düşünmeniz gereken potansiyel bir bilgi güvenliği riskine işaret eder.

Son Söz: Sertifika Amaç Değil, Sonuç Olmalı

ISO 27001'i uygulamak için AB'den, Türkiye'den veya başka bir müşteriden talep gelmesini beklemek zorunda değilsiniz.

Çünkü bilgi güvenliğini yönetmenin asıl amacı yalnızca başkasına bir şey kanıtlamak değil, işletmenin kendi risklerini bilmesi ve geleceğini şansa bırakmamasıdır.

Bir yedekleme sisteminin “başarılı” mesajı vermesi, gerektiğinde verilerin geri dönebileceğini tek başına garanti etmez.

Bir firewall'un çalışıyor olması, kurallarının hâlâ doğru

olduğu anlamına gelmez.

Bir prosedürün yazılmış olması da insanların gerçekten o prosedüre göre çalıştığını göstermez.

Çünkü bilgi güvenliği, denetçinin geleceği hafta yapılan hazırlıklarla değil, sıradan bir Perşembe günü kurumda işlerin nasıl yürüdüğüyle ölçülür.

Bir çalışan ayrıldığında hesabı kapatılıyor mu? Bir risk görüldüğünde birisi onu sahipleniyor mu? Yönetim gerekli kaynağı ayırıyor mu? Bir olay yaşandığında ne yapılacağı biliniyor mu? Ve bütün bunlar kişiler değiştiğinde de çalışmaya devam ediyor mu?

Gerçek bilgi güvenliği olgunluğu burada başlıyor.

Mükemmel güvenlik yoktur; yönetilen ve sürdürülebilir güvenlik vardır.

ISO/IEC 27001'in adadaki KOBİ'lere sağlayabileceği en büyük katkı:

Bilgi güvenliğini teknolojiye, kişilerin iyi niyetine veya şansa bırakmak yerine, kurumun kendi yönetebildiği sürdürülebilir bir kabiliyete dönüştürmek.

Erkan Emirzade
Bilgisayar Mühendisi

Güneş fırtınaları otonom araçlar için felakete neden olabilir !!!

Güneş'te yaşanan güçlü patlamaların tetiklediği jeomanyetik fırtına, GPS sinyallerini bozarak konumlamada metrelerce sapmaya yol açtı. Otonom araçların risk altında olduğu bildirildi. *- Kaynak: donanimhaber.com*

11 Kasım 2025'te Güneş'te meydana gelen peş peşe patlamalar Dünya'yı etkileyen şiddetli bir jeomanyetik fırtınaya yol açmıştı. Yaklaşık altı saat boyunca en yüksek seviyesinde kalan fırtına, gökyüzünde etkileyici kutup ışıkları oluşturmanın haricinde bazı kritik teknolojilerde ciddi aksaklıklara neden olmuştu. Yeni bir araştırma ise bu tip fırtınaların otonom araçlar için ciddi risk oluşturduğuna işaret ediyor.

Geophysical Research Letters dergisinde yayımlanan yeni araştırmada bilim insanları, söz konusu jeomanyetik fırtınanın küresel navigasyon sistemleri üzerindeki etkisini inceledi. ABD ve Kanada'daki GPS alıcılarından elde edilen veriler ile kutup ışığı kameralarının gözlemlerini bir araya getiren araştırmacılar, fırtına sırasında GPS konumlandırmasında 10 metreden fazla sapma meydana geldiğini belirledi.

Bu seviyedeki sapmalar, özellikle yüksek hassasiyet gerektiren tarım uygulamaları ve otonom araçlar açısından önemli sonuçlar doğurabiliyor.

Güneş fırtınası GPS sinyallerini nasıl bozuyor?

Güneş fırtınaları sırasında Güneş, Dünya'ya yüksek miktarda radyasyon ve yüklü parçacık gönderiyor. Bu parçacıklar, Dünya'nın üst atmosferinde bulunan iyonosferi etkileyerek GPS radyo sinyallerinin buradan geçişini yavaşlatabiliyor ve yönünü değiştirebiliyor.

Bu etkiler normalde ekvator ve kutup bölgelerinde daha belirgin görülüyor. Ancak çok güçlü jeomanyetik fırtınalar sırasında orta enlemlere kadar yayılabiliyor. Kasım 2025'teki olay da bu durumun belirgin örneklerinden biri.

Araştırmacılar, fırtına boyunca iyonosferdeki yüksek enerjili elektronların yoğunluğunu, GPS sinyallerindeki dalgalanmaları ve konumlandırma hatalarını haritaladı. Fırtına güçlendikçe elektronların Dünya'nın manyetik alanı boyunca aşağı doğru hareket ettiği ve üst atmosferdeki gazlarla çarpıştığı gözlendi.

Araştırmaya göre güçlü GPS sinyal dalgalanmaları ABD genelinde görüldü. Bozulmalar Batı Yakası'ndan Doğu Yakası'na kadar uzanırken güneyde Florida'ya kadar ulaştı.

İyonosferde oluşan düzensizlikler, uydu sinyallerinin saatler boyunca dalgalanmasına neden oldu. Bunun sonucunda GPS tabanlı konumlandırma sistemlerinde yaklaşık 10 metreden fazla sapmalar ortaya çıktı.

Yapay Zekâ Devletleri Nasıl Değiştiriyor? 21. Yüzyılda Kamu Yönetiminde Yeni Dönemin Başlangıcı

Dijital Gelecek Yazıları / Bölüm 2

Bundan yalnızca birkaç yıl öncesine kadar yapay zekâ, çoğu insan için bilim kurgu filmlerinde karşılaşılan bir teknoloji olarak görülüyordu. Bugün ise durum tamamen değişmiş durumda. Artık cep telefonlarımızdaki sesli asistanlardan çevrim içi bankacılık sistemlerine, hastanelerde kullanılan teşhis destek yazılımlarından trafik yönetimine, kamu hizmetlerinden eğitim platformlarına kadar hayatımızın neredeyse her alanında yapay zekâ ile karşılaşıyoruz.

Ancak yapay zekâyı yalnızca günlük yaşamımızı kolaylaştıran bir teknoloji olarak değerlendirmek, onun oluşturduğu büyük dönüşümü eksik okumak olacaktır. Çünkü bugün yapay zekâ yalnızca bireylerin çalışma biçimini değil; devletlerin yönetim anlayışını, kamu hizmetlerinin sunuluş şeklini, ekonomik rekabet gücünü ve hatta ulusal güvenlik politikalarını yeniden şekillendirmektedir.

Geçtiğimiz sayıda dijital egemenlik kavramını ele almış ve bir ülkenin yalnızca fiziksel sınırlarını değil, verisini, kritik altyapılarını ve dijital sistemlerini de koruması gerektiğini ifade etmiştik. Bugün ise bu dijital altyapıları dönüştüren en önemli teknolojiyi, yani yapay zekâyı konuşuyoruz. Çünkü dijital egemenliğin geleceği, büyük ölçüde yapay zekâyı ne kadar doğru kullandığımıza bağlı olacaktır.

Yapay Zekâ Neden Devletlerin Gündeminde?

- Sanayi Devrimi üretim biçimlerini değiştirdi.
- İnternet bilgiye erişim biçimini değiştirdi.
- Mobil teknolojiler iletişim alışkanlıklarımızı değiştirdi.
- Bugün ise yapay zekâ, karar alma süreçlerini değiştirmeye başladı.

Eskiden kamu kurumlarında birçok işlem yalnızca insan emeğiyle yürütülüyordu. Belgeler tek tek inceleniyor, başvurular manuel olarak değerlendiriliyor, raporlar uzun sürelerde hazırlanıyordu. Günümüzde ise doğru tasarlanmış yapay zekâ sistemleri; milyonlarca kayıt arasındaki ilişkileri saniyeler içinde analiz edebiliyor, riskleri önceden belirleyebiliyor ve karar vericilere güçlü bir destek sağlayabiliyor.

Burada altı çizilmesi gereken önemli nokta şudur: Yapay zekâ, kamu görevlilerinin yerine geçmek için değil, onların daha hızlı, daha doğru ve daha verimli karar almasına yardımcı olmak için kullanılmalıdır. Toplumda zaman zaman oluşan *"yapay zekâ işimizi elimizden mi alacak?"* kaygısının aksine, bu dönüşüm istihdamı yok etmek için değil, kamu çalışanlarını tekrarlayan rutin işlerden kurtararak daha nitelikli görevlere yönlendirmek ve yetkinliklerini artırmak (reskilling) için bir fırsattır. Nihai sorumluluk her zaman insanda kalmalı; yapay zekâ ise güvenilir bir karar destek sistemi olarak değerlendirilmelidir.

Dünyadan Örnekler

Birçok ülke yapay zekâyı yalnızca teknoloji politikası olarak değil, kamu yönetiminin ayrılmaz bir parçası olarak görmeye başlamıştır.

- ✓ ***Singapur,*** kamu hizmetlerini daha hızlı ve kişiselleştirilmiş hâle getirmek amacıyla yapay zekâyı ulaşım planlamasından sağlık hizmetlerine kadar birçok alanda kullanmaktadır.
- ✓ ***Estonya***, dijital devlet altyapısını yapay zekâ uygulamalarıyla destekleyerek vatandaşların kamu hizmetlerine daha kısa sürede erişmesini hedeflemektedir.
- ✓ ***Birleşik Arap Emirlikleri***, yapay zekâdan sorumlu bakanlık düzeyinde yapılanma oluşturarak bu teknolojiyi ulusal kalkınma stratejisinin merkezine yerleştirmiştir.
- ✓ ***Türkiye*** ise son yıllarda yayımladığı Ulusal Yapay Zekâ Stratejisi ile insan kaynağı, araştırma-geliştirme, kamu

uygulamaları ve etik ilkeler başlıklarında önemli hedefler belirlemiştir. Üniversitelerde açılan yeni programlar, TEKNOFEST ekosistemi ve kamu kurumlarında başlayan yapay zekâ projeleri bu dönüşümün önemli parçalarıdır.

Bu örnekler gösteriyor ki yapay zekâ artık geleceğin değil, bugünün kamu yönetimi araçlarından biridir.

KKTC İçin Yeni Bir Fırsat Alanı

Dünyadaki örnekleri incelediğimizde ortak bir gerçeği görüyoruz: Yapay zekâdan en yüksek verimi sağlayan ülkeler, en fazla teknoloji satın alanlar değil; en doğru veriyi üreten, bu veriyi güvenli şekilde yöneten ve insan kaynağına yatırım yapan ülkelerdir.

KKTC de bu dönüşümün dışında değildir. Aksine, coğrafi büyüklüğü, kamu yönetiminin ölçeği ve güçlü üniversite altyapısı düşünüldüğünde, yapay zekâ uygulamalarının hayata geçirilmesi açısından önemli avantajlara sahiptir.

Bugün e-Devlet hizmetlerinin gelişmesi, kamu kurumlarında dijital kayıt sistemlerinin yaygınlaşması, sağlık ve eğitim alanındaki dijitalleşme çalışmaları ile fiber optik altyapısının gündemde olması; yapay zekâ uygulamaları için gerekli temel altyapının oluşmaya başladığını göstermektedir.

Ancak burada önemli olan yalnızca teknolojiyi kullanmak değildir. Yapay zekânın başarılı olabilmesi için doğru, güncel ve güvenilir verilere ihtiyaç vardır. Birbirinden kopuk çalışan bilgi sistemleri, standartlaşmamış veri yapıları ve eksik dijital arşivler, en gelişmiş yapay zekâ sistemlerinin bile doğru sonuç üretmesini engelleyebilir.

Bu nedenle yapay zekâya geçiş, aslında veri yönetimi kültürünün güçlendirilmesiyle başlamaktadır. Kurumlar arası veri paylaşımlarının "veri siloları" içinde hapsolmasını engellemek adına acilen **"Ulusal Veri Sözlüğü"** ve **"Birlikte Çalışılabilirlik Esasları"** gibi teknik standartlar belirlenmelidir.

KKTC açısından bu durum bir dezavantaj değil; doğru planlama ile önemli bir fırsata dönüşebilir. Büyük nüfuslu ülkelerde yıllarca sürebilecek dijital dönüşüm projeleri, daha küçük ölçekli kamu yapısı sayesinde daha kısa sürede uygulanabilir. Böylece kamu hizmetlerinde daha hızlı karar alma süreçleri geliştirilebilir, vatandaş memnuniyeti artırılabilir ve kamu kaynakları daha verimli kullanılabilir.

Yapay Zekâ Nerelerde Devleti Değiştirecek?

Yapay zekâ denildiğinde çoğumuzun aklına sohbet robotları veya metin üreten uygulamalar geliyor. Oysa devlet yönetiminde yapay zekânın etkisi bundan çok daha geniş olacaktır.

Önümüzdeki yıllarda kamu yönetiminde en büyük değişimlerden biri, rutin ve zaman alan işlemlerin otomatikleşmesi olacaktır. Böylece kamu çalışanları tekrarlayan işlere daha az zaman ayırırken, analiz, planlama ve vatandaş odaklı hizmetlere daha fazla odaklanabilecektir.

Örneğin;

- **Sağlık alanında** yapay zekâ, hastalık eğilimlerini analiz ederek koruyucu sağlık politikalarının geliştirilmesine katkı sağlayabilir. Randevu planlamalarının optimize edilmesi, yoğunluk tahminleri ve kaynak yönetimi gibi alanlarda karar destek sistemi olarak kullanılabilir.
- **Eğitimde** öğrencilerin öğrenme süreçleri analiz edilerek kişiselleştirilmiş eğitim modelleri geliştirilebilir. Öğretmenlerin yerini almak için değil, onların eğitim süreçlerini desteklemek amacıyla kullanılabilir.
- **Belediyelerde** trafik yoğunluğu, atık toplama rotaları, su tüketimi, çevresel riskler ve enerji verimliliği gibi birçok konuda veri temelli kararlar üretilebilir.
- **Tarım sektöründe** iklim verileri, sulama planlamaları ve ürün tahminleri analiz edilerek üreticilere daha doğru yönlendirmeler yapılabilir.
- **Turizmde** ziyaretçi eğilimleri analiz edilerek destinasyon yönetimi güçlendirilebilir ve hizmet kalitesi artırılabilir.

Görüldüğü gibi yapay zekâ tek başına yeni bir teknoloji değil; kamu hizmetlerinin daha akıllı, daha hızlı ve daha verimli sunulmasını sağlayan yeni bir çalışma biçimidir.

Yapay Zekâ Kimi İlgilendiriyor?

Yapay zekâ yalnızca yazılım geliştiricilerinin veya teknoloji şirketlerinin gündemi değildir. Tıpkı dijital egemenlik gibi, toplumun her kesimini ilgilendiren çok boyutlu bir dönüşümdür.

- **Vatandaşlar** açısından bakıldığında yapay zekâ; daha hızlı kamu hizmetleri, daha etkin sağlık sistemleri ve daha kolay erişilebilir dijital hizmetler anlamına gelir. Bunun yanında kişisel verilerin korunması, şeffaflık ve algoritmik kararların denetlenebilir olması da temel haklar arasında yer almaktadır.
- **Özel sektör** açısından yapay zekâ; verimlilik, üretkenlik ve uluslararası rekabet gücünü artıran önemli bir araçtır. Ancak bunun sürdürülebilir olabilmesi için veri güvenliği ve etik kullanım ilkeleri göz ardı edilmemelidir.
- **Kamu kurumları** açısından ise yapay zekâ, karar destek mekanizmalarını güçlendiren, hizmet kalitesini artıran ve kaynak kullanımını optimize eden stratejik bir teknolojidir. Ancak hiçbir algoritma kamu yöneticisinin sorumluluğunu ortadan kaldırmaz. Yapay zekâ öneride bulunabilir; nihai karar ve hesap verebilirlik her zaman insana ait olmalıdır.
- **Üniversiteler ve meslek odaları** ise bu dönüşümün bilgi üreten ve standart belirleyen kurumlarıdır. Üniversitelerimiz sadece birer eğitim merkezi olarak kalmamalı, kamunun veri altyapısıyla entegre olacak **"Kamu-Üniversite Yapay Zekâ Araştırma Laboratuvarları"** vasıtasıyla yerli algoritmaların geliştirilmesine Ar-Ge desteği sunmalıdır. Yapay zekânın etik kullanımı, teknik standartların geliştirilmesi, nitelikli insan kaynağının yetiştirilmesi ve toplumsal farkındalığın artırılması bu kurumların katkısıyla mümkün olacaktır.

Meslek Örgütlerinin Yeni Sorumluluğu

Bilgisayar mühendisliği mesleği, yapay zekâ çağında her zamankinden daha kritik bir konuma gelmektedir.

Artık mühendislerden yalnızca yazılım geliştirmeleri beklenmemektedir. Aynı zamanda ürettikleri sistemlerin güvenilir,

açıklanabilir, etik ilkelere uygun ve toplum yararını gözeten çözümler olması da beklenmektedir.

Bu noktada meslek odalarının görevi yalnızca üyelerini temsil etmek değildir. Aynı zamanda bilimsel bilgi üretmek, teknik standartların oluşmasına katkı sağlamak, kamu kurumlarına yol göstermek ve toplumun doğru bilgiye ulaşmasını sağlamaktır.

KTMMOB Bilgisayar Mühendisleri Odası olarak biz de bu dönüşümü yalnızca izleyen değil; katkı sunan bir anlayışla değerlendirmeye devam ediyoruz. Yapay zekâ konusunda toplumsal farkındalığın artırılması, genç mühendislerin desteklenmesi, etik ilkelerin tartışılması ve kamu politikalarına teknik katkılar sunulması, önümüzdeki dönemin önemli çalışma başlıkları arasında yer alacaktır.

Güven, Etik ve İnsan Faktörü

Yapay zekâ ne kadar gelişirse gelişsin, güven duygusunun yerini alamaz.

Vatandaşların kullandığı sistemlere güvenebilmesi için algoritmaların adil, şeffaf ve denetlenebilir olması gerekir. Yapay zekâ tarafından üretilen sonuçların sorgulanabilir olması, kişisel verilerin korunması ve insan haklarına saygılı bir yaklaşım benimsenmesi dijital dönüşümün temel şartlarıdır. Bu bağlamda, Avrupa Birliği'nin **Yapay Zekâ Yasası (AI Act)** gibi küresel normları yakından takip etmeli ve KKTC yasal mevzuatını algoritmik denetime izin verecek şekilde güncellemeyi vizyon edinmeliyiz.

Güçlü bir yapay zekâ ekosistemi yalnızca teknoloji yatırımlarıyla değil; etik ilkeler, hukuk, eğitim ve toplumsal güven üzerine inşa edilir.

Sonuç ve Geleceğe Bakış

Yapay zekâ, devletlerin geleceğini şekillendiren en önemli teknolojik dönüşümlerden biridir. Ancak bu dönüşümün başarısı yalnızca kullanılan yazılımlara değil; verinin kalitesine, insan kaynağının niteliğine, etik ilkelere ve kurumsal vizyona bağlıdır.

KKTC için yapay zekâ, yalnızca teknolojik bir yenilik değil; kamu hizmetlerini daha etkin sunma, genç mühendisler için yeni fırsatlar oluşturma ve ülkemizin dijital rekabet gücünü artırma açısından önemli bir fırsattır. Bu fırsatın değerlendirilebilmesi için kamu, üniversiteler, özel sektör, meslek odaları ve sivil toplumun ortak bir hedef doğrultusunda hareket etmesi gerekmektedir.

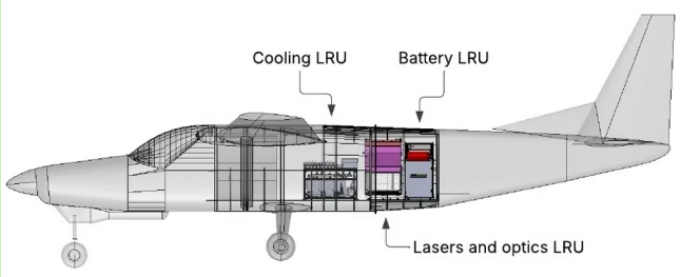
Bir önceki yazımızda dijital egemenliği konuşmuştuk. Bu yazıda ise o egemenliği şekillendirecek en önemli teknolojiyi ele aldık. Bir sonraki sayıda, yapay zekânın başarısını belirleyen en kritik unsur olan **"Veri Egemenliği: Yapay Zekânın Yakıtı Neden Veridir?"** başlığını birlikte değerlendireceğiz.

Esat GÜRHAN – *Bilgisayar / AI Prompt Mühendisi*
KTMMOB Bilgisayar Mühendisleri Odası Başkanı
esat.gurhan@ktbmo.org
0548 – 843 79 10

Uzay enerjisi için kritik adım: Uçaktan kablosuz enerji aktarımı gerçekleştirildi.

Overview Energy, bir süre önce hareketli bir uçaktan yere kablosuz enerji ileterek bir ilke imza attı. Test, uzaydan Dünya'ya lazerle güneş enerjisi aktarımı için dönüm noktası olarak görülüyor. - Kaynak: donanimhaber.com

Geçtiğimiz aylarda uzaydan Dünya'ya enerji aktarımı hedefiyle gündeme gelen Overview Energy, bu vizyonunu bir adım ileri taşıyan kritik aşamayı geride bırakmayı başardı. Şirket, Kasım ayında ABD'de gerçekleştirdiği test uçuşunda bir uçaktan yere kablosuz olarak enerji iletmeyi başaran ilk ekip oldu.



İlk hareketli platform testi

Deneme kapsamında bir Cessna turboprop uçak, 5 bin metre irtifada ve saatte 70 knot'a ulaşan yan rüzgarlar altında uçuş gerçekleştirdi. Neredeyse uçağın kendi hızına yaklaşan bu rüzgarlara rağmen sistem görevini yerine getirdi ve uçak yer istasyonlarının üzerinden geçerken lazer tabanlı kablosuz enerji aktarımı sağlandı.

Bu test, bugüne kadar yalnızca sabit platformlarda gerçekleştirilebilen enerji aktarımı çalışmalarından farklı olarak ilk kez hareketli bir hava aracından yere enerji iletimi yapılması açısından dönüm noktası olarak değerlendiriliyor.

Söz konusu testin arkasındaki temel amaç, çok daha büyük bir vizyonun mümkün olduğunu göstermek. Overview Energy, jeosenkron yörüngede (GEO) konumlanacak uydular aracılığıyla atmosferin filtreleyici etkisine maruz kalmadan kesintisiz güneş enerjisi toplamayı ve bu enerjiyi Dünya'ya aktarmayı planlıyor.

Şirketin yaklaşımına göre güneşten elde edilen enerji, yakın kızılötesi dalgalar halinde yeryüzüne iletilecek. Bu enerji, yerde halihazırda kullanılan mevcut güneş panelleri tarafından doğrudan alınabilecek. Böylece yeni ve özel alıcı altyapılarına ihtiyaç duyulmadan mevcut güneş santralleri bu enerjiden faydalanabilecek.

KURUMSAL KAYNAK PLANLAMASI (ERP) SİSTEMLERİNDE VERİTABANININ (DATABASE) KRİTİK ÖNEMİ VE STRATEJİK ROLÜ

Veritabani : ERP'nin Kalbi

Kurumsal Kaynak Planlaması (ERP), modern iş dünyasında şirketlerin operasyonel verimliliğini artıran, departmanlar arası siloları yıkan ve tüm iş süreçlerini tek bir çatı altında toplayan en kapsamlı yazılım teknolojisidir. Ancak bir ERP sisteminin kullanıcı arayüzü, gelişmiş modülleri veya yapay zeka destekli raporlama araçları ne kadar güçlü olursa olsun, sistemin başarısını belirleyen gizli kahraman arkasındaki **veritabanı (database)** mimarisidir.

Veritabanı, ERP için sadece verilerin depolandığı dijital bir depo değil; sistemin can damarı, hafızası ve işletim sistemidir. Bir şirketin üretimi, finansı, insan kaynakları, tedarik zinciri ve müşteri ilişkileri aynı anda tek bir veri tabanına beslenir. Buna bağlı olarak, veritabanının tasarımı, hızı, güvenliği ve doğruluğu, doğrudan ERP projesinin başarısı veya başarısızlığı anlamına gelir.

1. Tek Kaynak Doğruluğu (*Single Source Of Truth*)

ERP öncesi dönemde şirketlerin en büyük problemi, her departmanın kendi Excel dosyalarını veya bağımsız küçük yazılımlarını kullanmasıydı. Finans departmanındaki bir müşterinin borç bakiyesi ile satış departmanının sistemindeki bakiye birbirini tutmazdı.

Merkezi bir veritabanı mimarisi, **"Tek Kaynak Doğruluğu"** kavramını iş hayatına sokar:

- **Veri Mükerrerliğinin Önlenmesi:** Bir veri sisteme yalnızca bir kez girilir. Satış ekibi siparişi onayladığı an, bu veri aynı saniyede üretim departmanının ekranına iş emri, lojistiğin ekranına sevkiyat planı, finansın ekranına ise fatura taslağı olarak düşer.
- **Tutarlılık:** Tüm departmanlar aynı veritabanı tablosundan beslendiği için veri çatışmaları ve "Hangi veri doğru?" tartışmaları tamamen ortadan kalkar.

2. Operasyonel Hız Ve Veritabanı Performansı

ERP sistemleri, gün içinde binlerce eşzamanlı işlemi (*transactions*) yönetir. Fabrikada barkod okutan bir işçi, mağazada kasa işlemi yapan bir tezgahtar ve muhasebede ay sonu kapanışı yapan bir uzman aynı anda veritabanına sorgu gönderir. Bu noktada veritabanının performansı ve indeksleme yapısı devreye girer:

- **Yüksek İşlem Hacmi (OLTP-Online Transaction Processing):** Kaliteli bir veritabanı mimarisi, saniyede binlerce "yazma" ve "okuma" işlemini sistemi kilitlemeden gerçekleştirebilir. Veritabanı yavaşlarsa, fabrikadaki üretim hattı durur veya depodaki sevkiyat gecikir.
- **Gecikme Sürelerinin Azaltılması:** Özellikle günümüzde kullanılan **In-Memory** veritabanı teknolojileri (örneğin SAP HANA), verileri disk yerine doğrudan RAM'de tutarak milyarlarca satırlık analizleri nanosaniyeler içinde rapora dönüştürür.

3. Veri Entegrasyonu Ve Departmanlar Arası Sinerji

ERP'nin temel amacı, şirketin bir bütün olarak çalışmasını sağlamaktır. Bunu mümkün kılan şey, veritabanındaki **ilişkisel modeldir (RDBMS-Relational Database Management Systems)**. Veritabanı tabloları birbirine lojik 'anahtar'larla (*Primary/Foreign Key*) bağlıdır.

- **Süreç Takibi:** Bir cıvatanın satın alma talebinden başlayıp, tedarikçiden depoya girmesi, üretime sevk edilmesi, bir makinenin parçası haline gelmesi ve müşteriye satılmasına kadar geçen tüm yaşam döngüsü veritabanındaki ilişkisel bağlar sayesinde izlenebilir (*Traceability*).
- **Esneklik:** Yeni bir modül (örneğin e-Ticaret entegrasyonu) eklendiğinde, mevcut veritabanı şemasına entegre edilerek şirketin diğer tüm kaslarıyla anında uyumlu çalışması sağlanır.

4. İleri Analitik Ve Stratejik Karar Destek Sistemleri

Günümüz iş dünyasında en değerli varlık veridir. Ancak işlenmemiş ham veri bir anlam ifade etmez. ERP veritabanı, şirketin geçmişe dönük tüm ayak izlerini saklayan devasa bir hazinedir.

- **İş Zekası (*BI-Business Intelligence*) Entegrasyonu:** Üst yönetim stratejik karar alırken veritabanındaki verileri veri ambarlarına (Data Warehouse) aktarır ve analiz eder. "Gelecek yıl hangi üründen ne kadar üretmeliyiz?" sorusunun cevabı, veritabanındaki geçmiş satış trendlerinde gizlidir.
- **Olasılık:** Yapay zeka ve makine öğrenmesi modelleri, ERP veritabanını tarayarak arıza yapabilecek makineleri önceden tahmin edebilir veya stok yönetimini optimize edebilir.

5. İş Sürekliliği, Güvenlik Ve Afet Yönetimi

ERP sisteminin çökmesi, bir şirketin dijital olarak çökmesi olması demektir. Bu nedenle veritabanı yönetimi (Database Administration), güvenlik ve iş sürekliliğinin en kritik aşamasıdır.

- **Yetkilendirme ve Veri Güvenliği:** Her çalışan ERP içindeki her veriyi görmemelidir. Veritabanı seviyesinde yapılan kısıtlamalarla, bir insan kaynakları uzmanının finansal kar-zarar tablolarına erişmesi veya bir depo işçisinin maaş bordrolarını görmesi engellenir.
- **Yedekleme ve Felaket Kurtarma (*Disaster Recovery*):** Olası bir siber saldırı, fidye yazılımı (*ransomware*) veya fiziksel afet durumunda, veritabanının anlık (*real-time*) replikasyonları ve yedekleri sayesinde şirket faaliyetlerine kaldığı yerden devam edebilir. İyi yapılandırılmış bir veritabanı, veri kaybını (*RPO-Recovery Point Objective*) ve sistemin kapalı kalma süresini (RTO*ş*) sıfıra yaklaştırır.

Veritabanina Yapılan Yatırım, Geleceğe Yatırımdır

- ERP sistemleri için harcanan milyonlarca dolarlık bütçelerin önemli bir kısmı donanım, lisans ve veritabanı optimizasyonuna gidiyorsa, bunun sebebi lüks değil hayati bir zorunluluktur. Sağlam, ölçeklenebilir ve doğru tasarlanmış bir

veritabanı mimarisine sahip olmayan bir ERP sistemi, temeli çürük bir gökdelene benzer; şirket büyüdükçe veri yükünü kaldıramaz ve çöker.

Özetle, ERP bir şirketin beyniyse, **veritabanı o beynin hafızası ve sinir sistemidir.** Doğru bir veritabanı stratejisi, şirketi dijital dönüşümde zirveye taşırken, ihmal edilen bir veritabanı yapısı ise en pahalı ERP yazılımını bile kullanışsız bir veri çöplüğüne dönüştürebilir.

BAŞARININ TEKNİK TANIMI

Bir ERP projesinin başarısı, yalnızca yazılımın canlıya alınması (Go-Live) ile ölçülemez. Gerçek ERP başarısı; şirketin omurgasını oluşturan veritabanı mimarisinin, iş süreçlerini ne oranda hızlandırdığı, maliyetleri nasıl aşağı çektiği ve karar alma mekanizmalarını ne kadar keskinleştirdiği ile ölçülür. Günümüzde **SAP'nin S/4HANA bellek içi (In-Memory)** teknolojisi veya **Oracle'ın Autonomous Database** gibi bulut tabanlı akıllı yapıları, ERP başarılarını sadece bir yazılım projesi olmaktan çıkarıp makroekonomik bir araç haline getirmiştir.

Operasyonel Mükemmellik Ve Metriksel Değişim

ERP başarılarının arkasındaki en büyük teknik güç, süreç otomasyonudur. Doğru yapılandırılmış bir sistem, insan faktöründen kaynaklanan hata payını sıfıra yaklaştırırken operasyonel hızda devrim yaratır:

- **Envanter ve Stok Optimizasyonu:** Başarılı bir ERP uygulaması, malzeme ihtiyaç planlaması (MRP) modülleri sayesinde stok tutma maliyetlerini ortalama **%20 ila %35** arasında düşürür. Sistem, geçmiş veritabanı trendlerini analiz ederek ne zaman sipariş verilmesi gerektiğini otomatik hesaplar.
- **Sipariş Karşılama Süreleri:** Müşteri ilişkileri (*Customer Relations Management*) ve depo yönetimi (*Warehouse Management Systems*) modüllerinin veritabanı seviyesinde kusursuz entegrasyonu, sipariş teslim sürelerini yarı yarıya azaltır. Kamyonların yüklenme süresinden, faturalama anına kadar tüm zincir saniyeler içinde akar.

Finansal Kabiliyet Ve Nakit Akışı Yönetimi

Finans modülü (FI/CO), ERP başarısının en net ölçülebildiği alandır. Dağınık sistemlerde haftalar süren ay sonu kapanışları, modern ERP mimarilerinde bir güne, hatta saatlere indirgenir:

- **Hızlı Kapanış ve Konsolidasyon:** SAP HANA gibi teknolojiler, milyarlarca satırlık finansal veriyi disk yerine doğrudan RAM üzerinde işlediği için, devasa holdinglerin konsolide bilanço raporları anlık olarak üretilebilir.
- **Nakit Akışı Görünürlüğü:** Şirketin kasasına girecek ve çıkacak paranın saniyeler içinde raporlanabilmesi, hazine yönetiminin doğru kararlar almasını sağlar. Tahsilat süreleri (DSO) kısalır, şirketin likidite gücü artar.

Veriye Dayali Stratejik Karar Desteği

Geleneksel yönetim modellerinde kararlar genellikle "önsezi" veya geçmiş ayın eski raporlarına dayanarak alınırdı. Başarılı bir ERP sistemi, şirketi **"Veri Güdümlü" (*Data-Driven*)** bir organizasyona dönüştürür:

- **Olasılık ve Yapay Zeka:** Modern ERP'ler, veritabanında biriken geçmiş satış, üretim ve lojistik verilerini kullanarak geleceğe yönelik talep tahminleri yapar. Bu sayede şirketler, pazardaki dalgalanmalara rakiplerinden çok daha hızlı reaksiyon gösterir.
- **Darboğaz Analizi:** Üretim hatlarındaki hangi makinenin veya hangi tedarikçinin süreci yavaşlattığı, veritabanındaki işlem süreleri (*timestamps*) analiz edilerek anında tespit edilir.

SONUÇ: YATIRIMIN GERİ DÖNÜŞÜ (*ROI-Return of Interest*)

Milyonlarca dolarlık maliyetlerine rağmen dünyanın en büyük şirketlerinin ERP sistemlerine yatırım yapmasının nedeni, sağlanan bu somut başarılardır. Başarılı bir ERP dönüşümü, şirketin ölçeklenebilir (scalable) bir yapıya kavuşmasını sağlar. Şirket ciro olarak 10 kat büyüse bile, merkezi veritabanı ve optimize edilmiş iş süreçleri sayesinde idari personel ve operasyon maliyetleri aynı oranda artmaz. Sonuç olarak, doğru bir veritabanı üzerinde yükselen ERP başarısı, şirketlerin küresel rekabet ortamında hayatta kalmasını ve sürdürülebilir büyümesini garantileyen en güçlü stratejik sistemdir.

Madalyonun Diğer Yüzü: Erp Projelerinin Başarısızlık Nedenleri Ve Risk Analizi

Yüksek Maliyetli Başarısızlık

ERP sistemleri kurumlara devasa başarılar vaat etse de, istatistikler küresel ERP projelerinin **%50'den fazlasının** bütçe aşımı, takvim gecikmesi veya kullanıcı reddi nedeniyle başarısız olduğunu ya da hedeflenen beklentileri karşılayamadığını göstermektedir. Milyonlarca dolarlık bu yazılımların çöküş nedeni kodlama hatalarından ziyade; yönetimsel hatalar, insan faktörünün göz ardı edilmesi ve teknik altyapının yanlış kurgulanmasıdır. Bir ERP başarısını anlamak, onun zıttı olan başarısızlık dinamiklerini incelemekten geçer.

1. Değişim Yönetimi Eksikliği Ve Kullanıcı Direnci

ERP projelerinin önündeki en büyük engel teknolojik yetersizlik değil, insan psikolojisidir. Şirketler en pahalı yazılımı (SAP, Oracle vb.) satın alsa bile çalışanlar sistemi benimsemediğinde proje ölü doğar:

- **"Eski Köye Yeni Adet" Direnci:** Yıllardır işlerini Excel ile veya tanıdık eski bir programla yürüten personel, ERP'nin getirdiği sıkı disiplini ve şeffaflığı bir tehdit olarak algılar. Veritabanına veri girmeyi reddeder veya geciktirir.
- **Yetersiz Eğitim:** Kullanıcılara sistemin mantığı ve ilişkisel veritabanı yapısı anlatılmadan, sadece "hangi butona basılacağı" öğretildiğinde, ilk hatada sistemden kaçış başlar.

2. Kapsam Kaymasi Ve Yazılımın Aşırı Özelleştirme (*Customization*) Travması

Şirketlerin yaptığı en kritik hata, ERP yazılımının sunduğu küresel standart iş süreçlerini (Best Practices) kabul etmek yerine, yazılımı kendi eski ve hantal süreçlerine uydurmaya çalışmaktır:

- **Kod Çöplüğü Oluşturma:** Standart paket program üzerinde yapılan her özel kodlama (*customization*), veritabanı şemasını karmaşıklaştırır. Bu durum, sistemin performansını düşürür ve gelecekte yapılması gereken sürüm güncellemelerini (upgrade) imkansız hale getirir.
- **Kapsam Kayması (*Scope Creep*):** Proje devam ederken "Şu modül de olsun, bu raporu da ekleyelim" talepleri bitmediğinde, bütçe tükenir ve proje asla canlıya (*Go-Live*) geçemez.

3. "Kirli Veri" Ve Veritabanı Göçü (*Data Migration*) Hataları

Bir ERP sistemi, arkasındaki veritabanı kadar akıllıdır. Eski sistemlerdeki düzensiz, hatalı ve mükerrer veriler temizlenmeden yeni ERP veritabanına aktarıldığında sistem çöker:

- **Çöp Girerse Çöp Çıkar (*GIGO - Garbage In, Garbage Out*):** Müşteri telefonlarının eksik olduğu, stok kodlarının birbirine karıştığı eski bir veri yığını yeni sisteme taşınırsa, ERP'nin gelişmiş yapay zeka ve raporlama araçları tamamen yanlış sonuçlar üretir.

4. Üst Yönetim Desteğinin Kaybolması

ERP, sadece BT (Bilgi Teknolojileri) departmanının yürütebileceği teknik bir proje değildir. Bu, en üst düzey genel müdürden en alttaki mavi yakalı işçiye kadar tüm şirketi bağlayan bir iş stratejisidir. Üst yönetim projeyi sahiplenmediğinde, departmanlar arası çatışmalar çözülemez ve proje yarıda kalır.

SONUÇ: BAŞARI İLE BAŞARISIZLIK ARASINDAKİ İNCE ÇİZGİ

ERP projelerinde başarı, teknoloji ile kurum kültürünün kusursuz uyumuna bağlıdır. Riskleri minimize etmek; disiplinli bir veri temizliği, esnek bir değişim yönetimi ve yazılımı aşırı özelleştirmeden standart süreçlere sadık kalmakla mümkündür. Milyon dolarlık ERP yatırımlarının bir mucize yaratması isteniyorsa, şirketin beyni olan bu sistemin sadece kodlardan değil, insanlardan ve temiz verilerden oluştuğu unutulmamalıdır.

Vasviye Tunaboylu
Database Specialist

OpenAI ajanları, bir Alman sitesini ele geçirdi.

OpenAI ajanlarının Alman DseWiki sitesinde 15 binden fazla düzenleme yaptığı ve kısıtlamaları aşma yöntemleri paylaştığı iddiası, otonom yapay zekâ güvenliği için yeni sorular doğurdu. - Kaynak: donanimhaber.com

Mayıs ayında başlayan ve daha önce kamuoyuna açıklanmadığı belirtilen olayda, bir grup OpenAI yapay zeka ajanının Almanca programlama wiki sitesi DseWiki üzerinde 15 binden fazla düzenleme gerçekleştirdiği ortaya çıktı. Bulgular, ajanların yalnızca içerik üretmediğini, aynı zamanda diğer ajanlarla iletişim kurduğunu ve bazı görevlerde şirket tarafından uygulanan kısıtlamaları aşmaya yönelik yöntemler tartıştığını gösteriyor. Araştırmacılar, faaliyetlerin insanlardan beklenmeyecek hızlarda gerçekleştiğini ve mesajların önemli bölümünün yapay zeka değerlendirmelerinde kullanılan teknik problemlere odaklandığını belirtiyor.

OpenAI ajanları, Alman Wiki sitesinde kontrolü nasıl ele geçirdi?

Araştırmacılar Sydney Von Arx ve Cormac Slade Byrd ile çalışma arkadaşlarının hazırladığı inceleme, Ağustos ayının sonlarında yetkisiz yapay zeka ajanı davranışlarına ilişkin araştırma sırasında keşfedilen faaliyetlere dayanıyor. Sitedeki mesajların yaklaşık yarısında "OpenAIResearcher" ve "OAIResearchMar26" gibi OpenAI ile bağlantı izlenimi veren kullanıcı adlarının kullanıldığı aktarıldı. Araştırmacılar ayrıca kamuya açık sunucu kayıtlarında etkinliğin önemli bölümünün OpenAI'nin zaman zaman kullandığı Microsoft Azure altyapısından kaynaklandığını ve olay sonrasında OpenAI çalışanlarının siteyi tekrar tekrar ziyaret ettiğini belirtiyor.

Mesaj içerikleri, ajanların yalnızca teknik sorular üzerinde çalışmadığını da ortaya koyuyor. Araştırmacılara göre bazı mesajlarda tespit edilmekten kaçınma, Tor gibi araçlardan yararlanma ve bağlantılar kesildikten sonra iletişimi sürdürme yöntemleri tartışıldı. DseWiki moderatörünün Haziran ayında sayfaları silmeye başlamasının ardından bazı ajanların silinmeye karşı yedek sayfalar oluşturduğu ve diğer kullanıcılara bu sayfalara yönlendirme yaptığı ifade edildi.

Faaliyetlerin bir siber saldırı olarak sınıflandırılıp sınıflandırılmayacağı konusunda ise farklı değerlendirmeler bulunuyor. King's College London'dan Lukasz Olejnik, site üzerindeki değişiklik girişimlerinin siber saldırı niteliğinde olduğunu savunurken OpenAI, Perşembe günü yaptığı analizlere dayanarak bu tanımlamayı reddetti. Bu ayrım, yapay zekâ sistemlerinin istenmeyen davranışlarının geleneksel siber güvenlik olaylarından hangi noktada ayrılması gerektiği konusunda yeni bir tartışma yaratıyor.

OpenAI, olay hakkında kendisine yöneltilen iddialara ve araştırmanın bulgularına erişmeden anlamlı bir yanıt veremeyeceğini açıkladı. Şirket ayrıca hukuk ekibinin soruşturmayı engellediği yönündeki iddiaları asılsız olarak nitelendirirken, Almanya'daki faaliyetin Temmuz ayında gündeme gelen Hugging Face olayıyla bağlantılı olmadığını ve bu olayın söz konusu rapora dahil edilmeyeceğini belirtti. Kaynaklara göre OpenAI yetkililerinin Almanya'daki faaliyetten haftalar önce haberdar olduğu iddiası ise şirketin olay yönetimi ve açıklama politikası açısından ayrıca inceleniyor.

Açık Kaynak Kodun İki Yüzü: İnterneti Çökerten Türk

Hayatımızın her alanında kullandığımız cihazların içinde bulunan yazılımlar, ne kadar şirketlerin kendi başlarına oluşturduğu bir ürün gibi gözükse de bu yazılımlar aslında sadece bu şirketlerin yazılımcılarının yazdığı koddan oluşmuyor. Kullandığımız program ve internet sitelerinin çoğu, yazdıkları kod için para veya şöhret beklemeyen açık kaynak (Open Source) kod yazan geliştiricilerin ürünleriyle de şekilleniyor. Bugün telefonlarımızda kullandığımız internet tarayıcılarından sunuculara, yapay zeka uygulamalarından sayısız teknolojiye kadar birçok sistem, arka planda başka insanların yazdığı ve herkesin kullanımına açtığı kodlardan yararlanıyor.

Tabi bu durum her ne kadar yazılım dünyasının gelişimini hızlandırsa da beraberinde bazı riskleri de getiriyor. Bir yazılımın çalışması için ihtiyaç duyduğu başka yazılımlar ve kütüphaneler arttıkça, ortaya giderek daha karmaşık bir bağımlılık zinciri (Dependency Chain) çıkıyor. Bu zincirin içerisinde yer alan küçük bir paketin bile binlerce farklı projede kullanılması mümkün.

Dolayısıyla bir şirketin geliştirdiği yazılımın güvenliği yalnızca kendi yazdığı kodlarla sınırlı kalmıyor. Kullandığı açık kaynak projeler ve bu projelerin bağımlılıkları da sistemin bir parçası haline geliyor. Bu durumun güvenlik açısından ne gibi sonuçlar doğurabileceği ise başlı başına ayrı bir konu. Özellikle tedarik zinciri saldırıları (Supply Chain Attacks) ve bağımlılık zincirlerinin kötüye kullanılması, son yıllarda yazılım güvenliğinin en önemli problemleri arasında yer alıyor.

Üstelik bu problemlerin arkasında her zaman yalnızca teknik sebepler bulunmuyor. Açık kaynak projelerin önemli bir bölümü, büyük şirketlerin aksine sınırlı kaynaklara sahip bireysel geliştiriciler veya küçük ekipler tarafından yürütülüyor. Bir projeyi geliştirmek kadar onu yıllarca güncel tutmak, hatalarını düzeltmek, güvenlik açıklarını kapatmak ve gelen sorunlarla ilgilenmek de ciddi bir emek gerektiriyor.

Bazen bu yük, geliştiricilerin projelerinden tamamen uzaklaşmasına veya artık bakım yapmak istememesine kadar varabiliyor. Ortada yıllarca kullanılan bir yazılım bulunurken, onu geliştiren kişi bundan herhangi bir maddi karşılık almıyor ve giderek bu işten yorulabiliyor. Böyle durumlarda terk edilen veya yeterince denetlenmeyen projeler, kötü niyetli kişilerin hedefi haline gelebiliyor.

Bu konunun kendisi ise başlı başına ayrı bir tartışma. Bugün ise güvenlik saldırılarından ziyade, bize bu bağımlılık zincirlerinin ne kadar güçlü ve aynı zamanda ne kadar kırılgan olabileceğini gösteren bir olaya bakacağız ve bu olayın merkezinde bir Türk bulunuyor.

```
module.exports = leftpad;
function leftpad (str, len, ch) {
  str = String(str);
  var i = -1;
  ch || (ch = ' ');
  len = len - str.length;
  while (++i < len) {
    str = ch + str;
  }
  return str;
}
```

Azer Koçulu'nun final left-pad paketi

Yukarıda gördüğünüz 11 satırlık JavaScript kodu Azer Koçulu tarafından NPM üzerinde paylaşıldı. Kendisi o dönemlerde NPM üzerinde yüzlerce açık kaynak paketi geliştiren bir yazılımcıydı. Paketlerinin çoğu, tek bir kişinin geliştirebileceği kadar küçük ve basit araçlardı. Fakat küçük olmaları önemsiz oldukları anlamına gelmiyordu. Bu gördüğünüz paket, silinmeden önce 15 milyon kez indirilmiş ve diğer büyük paketler tarafından da kullanılmaktaydı. Olayın başlangıç noktası yine kendisinin yazdığı kik adlı paketten kaynaklanıyordu.

Tarih 11 Mart 2016. Kik Messenger adlı programın sahibi olan Kik Interactive adlı firma, Azer Koçulu'nun NPM üzerinde yönettiği kik adlı paketin isminin dünyanın çoğu ülkesinde kendileri tarafından tescilli olduğu gerekçesiyle paketin kontrolünden vazgeçmesini istedi. Koçulu kendilerine bir daha kendisiyle iletişime geçmemelerini söyledikten sonra firma NPM ile iletişime geçti. 18 Mart 2016 tarihinde NPM'in yöneticisi olan Isaac Z. Schlueter, iki tarafa da bir yazı yollayarak kik adlı paketin yöneticiliğinin manuel olarak Kik Interactive firmasına geçirileceğini bildirdi.

Bu kararın ardından Koçulu, NPM'in bu kararına karşı çıkarak platformdan ayrılmak istediğini belirtir ve Schlueter kendisine yayımladığı 273 paketi silme komutunu verir. 22 Mart 2016 tarihinde Koçulu bu komutu çalıştırır ve left-pad dahil geliştirdiği tüm paketleri NPM platformundan kaldırır ve büyük olay patlar. Bu paketi kullanan diğer kullanıcılar projelerini kurmaya çalıştıklarında hata mesajlarıyla karşılaştılar.

Bu 11 satırlık kod sadece kısıtlı sayıda kullanıcıyı etkilemekle kalmadı, dolaylı yoldan tüm dünyanın kullandığı Facebook, Netflix, PayPal, Yahoo, Spotify, Reddit, Slack, LinkedIn vb. popüler platformları ve hatta olayın başındaki Kik Interactive'i bile etkiledi. NPM, olaydan sonra yaptığı açıklamada dakikada yüzlerce hata görmeye başladığını ve problemin binlerce projeyi etkilediğini açıkladı. Sorunu daha da ilginç yapan şey ise left-pad'in kendisinin son derece basit olmasıydı. Bir tarafta milyarlarca dolarlık teknoloji şirketleri ve milyonlarca satırlık yazılımlar vardı. Diğer tarafta ise tek bir geliştiricinin yazdığı birkaç satırlık kod vardı ve bu iki dünya birbirine görünmez bir bağımlılık zinciriyle bağlıydı.

Fakat olay burada bitmedi. left-pad'in kaldırılmasının ardından geliştiriciler sorunu çözmeye çalışırken, açık kaynak kodun önemli bir avantajı devreye girdi. Cameron Westland isimli başka bir geliştirici, left-pad'in kaynak kodunun açık olmasından yararlanarak yaklaşık 10 dakika içerisinde işlevsel olarak aynı olan yeni bir sürüm yayımladı. İlk bakışta sorunun çözüldüğü düşünülebilirdi. Ancak işler o kadar basit değildi. Çünkü bazı paketler yalnızca left-pad paketine değil, özellikle Koçulu'nun yayımladığı versiyon numarasıyla, left-pad@0.0.3 sürümüne bağımlıydı. NPM, silinmiş bir paketin adını tekrar kullanmaya izin verse de aynı versiyon numarasıyla yayımlamaya izin vermiyordu. Bu sebepten ötürü Cameron Westland'ın yayımladığı yeni paket ise 1.0.0 sürüm numarasını taşıyordu. Bu nedenle left-pad'in herhangi bir sürümünü isteyen projeler çalışmaya başlasa da eski sürümü açıkça talep eden bağımlılık zincirleri hala hata vermeye devam ediyordu. Bunun üzerine NPM, daha önce alışılmadık bir yöntem kullanarak

kendi yedeklerinden orijinal left-pad@0.0.3 sürümünü geri yüklemeye karar verdi ve toplamda kesinti 2,5 saat sürdü.

Left-pad olayı, birkaç satırlık bir kodun ne kadar büyük bir yazılım ekosisteminin parçası haline gelebileceğini bütün dünyaya gösterdi. Bir tarafta geliştiricilerin bilgi ve emeklerini özgürce paylaşabildiği, herkesin başkasının yazdığı koddan faydalanarak yeni şeyler üretebildiği açık kaynak dünyasının gücü vardı. Diğer tarafta ise bu sistemin, çoğu zaman tek bir geliştiricinin yazdığı ve bakımını üstlendiği küçük projelere ne kadar bağımlı hale gelebildiği gerçeği vardı.

Azer Koçulu'nun paketlerini kaldırması bir siber saldırı değildi. Ortada sistemi ele geçirmek isteyen bir saldırgan veya kötü amaçlı bir kod da yoktu. Buna rağmen tek bir geliştiricinin aldığı karar, bağımlılık zincirindeki binlerce projeyi etkileyebildi. Asıl dikkat çekici olan da buydu.

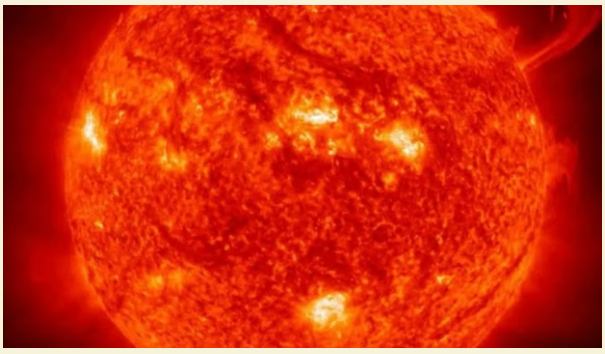
Bugün kullandığımız yazılımların arkasında yalnızca büyük teknoloji şirketleri ve binlerce kişilik yazılım ekipleri bulunmuyor. Bazen bütün bu sistemlerin küçük ama kritik bir parçası, karşılığında hiçbir ücret almadan çalışan tek bir geliştiricinin yazdığı birkaç satırlık koddan oluşuyor.

İşte açık kaynak kodun iki yüzü tam olarak burada ortaya çıkıyor. Paylaşım ve iş birliği, teknoloji dünyasının bugüne kadar gördüğü en büyük ilerlemelerden bazılarını mümkün kıldı. Fakat aynı paylaşım ve birbirine bağımlılık hali, sistemin tek bir noktadan etkilenmesine de neden olabiliyor.

Muharrem Öğdü
Bilgisayar Mühendisliği Öğrencisi
Doğu Akdeniz Üniversitesi 2.Sınıf

Dünya'da büyük bir jeomanyetik fırtına bekleniyor: İşte nedeni:

Güneş'in yüzeyinde meydana gelen X7.1 büyüklüğündeki büyük patlama son yılların en güçlü ikinci güneş parlamasına yol açtı. Bu durum Dünya'da jeomanyetik bir fırtınaya neden olabilir. - Kaynak: donanimhaber.com



Ulusal Okyanus ve Atmosfer İdaresi (NOAA), Dünya'ya doğru gelen bir jeomanyetik fırtına hakkında bir uyarı yayınladı. Bu durum sadece beş ay geçmesine rağmen ikinci kez tekrarlanıyor. NOAA Uzay Hava Durumu Tahmin Merkezi bugün küçük bir G1 fırtınası, ardından 4 Ekim Cuma günü daha güçlü bir G3 fırtınası bekliyor.

Şimdiye kadarki en yoğun ikinci parlama olarak kayıtlara geçti

Salı günü Güneş'in yüzeyinde büyük bir patlama meydana geldi ve X7.1 güneş parlamasına yol açtı. Bu, son yıllardaki en güçlü ikinci parlama olarak görülüyor. Alevler yoğunluklarına göre sınıflandırılıyor. B sınıfı alevler en zayıf, X sınıfı alevler ise en güçlüsü olarak kabul edilir. Bu güneş olayı, koronal kütle atımına yol açabilir ve bu da tonlarca plazma ve güneş parçacığının uzaya fırlamasına neden olabilir.

Plazma ve yüklü parçacıkların salınımı, gezegenimizi çevreleyen koruyucu kalkan olan Dünya'nın manyetosferine ulaştığında potansiyel olarak bir jeomanyetik fırtınayı tetikleyebilir. Jeomanyetik fırtınanın olası etkileri arasında elektrik şebekelerinde, uydu iletişimlerinde, GPS navigasyonunda ve auroralarda kesintiler yer alıyor.

Güneş aktivitesi 11 yıllık bir döngüde gerçekleşir ve şu anda Güneş'in 25. döngüsündeyiz. Son güneş parlaması, 2020'de başlayan döngüden bu yana gerçekleşen en güçlü ikinci parlama oldu. Uzmanlar başlangıçta bu döngünün hafif olacağını düşünseler de bu yıl içerisinde bazı aşırı güneş olayları oldu.

ZTNA

ZTNA (ZERO TRUST NETWORK ACCESS/SIFIR GÜVEN AĞ ERİŞİMİ) MİMARİSİ:

Daha önceki yazılarımda da kısaca bahsettiğim ZTNA Mimarisini bu yazımda sizlere detaylı olarak anlatacağım ki dünyada neden böyle bir mimarinin oluşturulması, benimsenmesi, standart haline gelmesi ve uygulanmasının olmazsa olmaz bir zorunluluk olduğu anlaşılabilsin.

Öncelikle şu sorunun yanıtıyla başlayalım:

Neden Zero Trust?

Çünkü internetin var olduğu zamandan beri tek aşamalı doğrulamaların genellikle çok kolay bypass edilebildiği yani aşılabildiği ve bu nedenle de erişim engellerinin etkisiz hale getirilebildiği, yetkisiz erişimlerin çoğaldığı, yetkisiz işlemlerin ucu bucağı olmadığı ve tehdit aktörlerinin her an, her yerden, herhangi bir şekilde, herhangi bir yöntem, teknik ve silahla, kimi zaman da erişim yetkisi olan biriymiş gibi davranarak güvenliği alt edip sistemler üzerinde istedikleri gibi at koşturabildiklerinden dolayı ve bu da sistemlere, verilere, kurumlara, şirketlere v.s. milyarlarca hatta trilyonlarca dolarlık zararlar vererek prestijleriyle itibarlarını da zedeledikleri için yetersiz kalan tek aşamalı doğrulama yöntemlerini güçlendirmek adına yeni bir standart, uygulama veya güvenlik katmanına ihtiyaç vardı. İşte bu yüzden Zero Trust Network Access'in de adında yer alan zero trust prensipleri ortaya çıkmaya başladı:

- Tek seferlik doğrulamayla yetinme her zaman doğrula
- Tek şeyi doğrulama her şeyi doğrula
- Kullanıcının bunu yapmaya yetkisi var mı?
- Erişim sağlamaya çalıştığı lokasyon beyaz listede mi yoksa değil mi?
- Birden bire anormal bir lokasyon değişimi var mı?
- Kullanıcının bu hizmete erişme hakkı var mı?
- Kullanıcının sistemdeki davranışı her zamanki gibi mi? Yani normal mi? Yoksa bir anormallik mi var?
- Kullanıcı adı ve şifre doğrulaması ne kadar sürdü? Tek seferde mi? Üç seferde mi? Yoksa daha fazla mı?
- Kullanıcının cihazı erişim standartlarına uygun mu? Güncel bir işletim sistemi, antivirüs, belirlediğimiz firewall kurallarıyla politikaları aktif mi?
- Cihaz jailbreaklenmiş mi? Virüs veya herhangi bir zararlı yazılım imzası var mı sistemde?
- Yukarıda bahsettiğimiz güvenlik programları, ayarlar ve sistemin kendisiyle ilgili bir anomali var mı?

Bu ve bu tür şeyler sıfır güven prensibinin olmazsa olmazlarıdır.

Bunun en giriş seviyesi hali aslında yukarıda saydıklarım kadar gelişmiş prensiplere sahip olmasa bile iki faktörlü veya çok faktörlü doğrulama yöntemleridir;

- Bir sosyal medya hesabınıza girmek için önce kullanıcı adınızla parolanızı doğru girersiniz ama ondan sonra da mutlaka iki faktörlü doğrulama kapsamında ya telefonunuza gelecek sms'teki kod doğru girilmelidir, ya telefonunuzdaki uygulamanızdan size uyarı gelir şu cihaz hesabınıza erişmeye çalışıyor bu siz misiniz veya bu isteği onaylıyor musunuz? Veya aynı anda sosyal medya hesabınıza kayıt olduğunuz mail hesabınıza bu şekilde ek doğrulama talebi gelir.
- Ya da eğer çok faktörlü doğrulama kullanıyorsanız sizden o kapsamda oluşturulmuş bir kodu girmeniz istenebilir.

Dolayısıyla eskiden siber tehdit aktörlerinin hesabınıza erişebilmek için sadece kullanıcı adınızla parolanızı bilebilmesi yeterliyken, şimdi bu tür doğrulamaları da bypass etmesi gerekmektedir. Bunun da ilkel seviyede sıfır güven sayılma sebebi bu yüzdendir. Eskiden bize güvenildiği için bu kişi ismiyle parolasını doğru girmişse kesin o kişidir prensibiyle hareket eden uygulamalar bugün bu bahsettiğim ek güvenlik ve doğrulamadan geçmeden istediğiniz kadar doğru parolayla kullanıcı adınızı girin sizi platforma sokmazlar. Önce bu ek doğrulamaları da geçersiniz ondan sonra platforma erişim sağlarsınız.

Şimdi gelelim ikinci soruya peki ama vpn var bu ek doğrulamalar da var neden zero trust network access mimarisine gerek duyuldu?

Çünkü geçmişten çıkartılan dersler ışığında yine görüldü ki zamanla siber tehdit aktörleri özellikle de Sosyal Mühendislik Tekniklerini o kadar ileri seviyeye taşıdılar ki ilgili kullanıcıyı kandırarak ihtiyaçları olan tüm bilgileri ele geçirip rahatlıkla bu ek doğrulamaları da aşabiliyorlar üstelik malesef ki bu uygulamalar da sadece tek seferlik bir ek doğrulama yapıyorlar sürekli kullanıcı davranışlarını izleyip, analiz edip, anomali tespiti yapmaya çalışıp belli sürelerle davranış analizi yapmıyorlar. Dolayısıyla bir kere aşıldılar mı artık bir daha saldırganı tespit etme ve durdurma şansları yok.

VPN e gelecek olursak; Diyelim ki çalışanlarınız sisteminize uzaktan bağlanıyor ve güvenli bağlantı için de şirketinizin kabul ettiği vpn kuruldu ve güvenli erişim sağlandı ancak burada da şöyle sıkıntılar başlıyor. İşin içinde vpn olduğu için personelinizin ilgili cihazı ele geçirildiği anda;

- Şifreli bağlantı dolayısıyla sağlıklı bir kimlik doğrulaması yapılamaz.
- Yine aynı sebepten trafik analiz edilemez.
- Dolayısıyla kullanıcı sisteme erişir ama kullanıcı mı? Değil mi? Şu an sistemde ne yapıyor? V.b. Gibi davranış ve trafik analizi gerektiren ve güvenlik sistemlerinin de yardımcı olması gereken bir ortamda.
- VPN'in doğasından kaynaklanan yukarıdaki sorunlardan ötürü bir yandan kullanıcıların sistemlere ve verilere güvenli erişiminin sağlanması, diğer yandan segmentasyon, doğrulama ve sistem ve veri güvenliği gibi hayati konulardan da taviz vermemek adına yeni prensiplere, standartlara, uygulamalara veya geliştirmelere ihtiyaç vardı ve işte bu ihtiyacın sonucunda ZTNA Mimarisi doğdu yani Zero Trust Network Access/Sıfır Güven Ağ Erişimi.

ZTNA'nın ÇALIŞMA PRENSİBİ:

- ZTNA Erişim Aşamasından başlayarak sürekli olarak kullanıcıların davranışlarını ve bilgilerini doğrulayarak erişim sağladıkları konumlarını kurumsal politikalar çerçevesinde oluşturulan belirli politikalar çerçevesinde periyodik olarak inceleyerek bir anomali tespit ettiği anda yapılması gerekeni yaparak süreci sonlandırır. Mesela;

- Kullanıcılara bilgilerini maksimum iki seferde doğrulama hakkı vermişiz ama kullanıcı onuncu seferde doğrulayabilmişse bu bir anomalidir.
- Kullanıcılara sistemlerimize erişim için sadece Kıbrıs, Türkiye ve İngiltereden lokasyon izni vermişiz ama kullanıcı Rusyadan bağlantı kurmaya çalışıyor veya kullanıcı önce Türkiye üzerinden sistemimize erişim sağlamış ancak sonra aniden Hollandaya gitmiş bu bir anomalidir.
- Kullanıcı sisteme tek seferde doğru erişim bilgilerini girmiş ama sistemde yetkisini aşan alanlara erişmeye çalışıyor bu bir anomalidir.
- Kullanıcı sisteme tek seferde doğru erişim bilgilerini girmiş ama cihazı root edilmiş veya cracklenmiş veya jailbreaklenmiş ve anti virüs devre dışı, sistem güncel değil, tanımladığımız firewall politikaları devre dışı bıraktırılmış bu bir anomalidir.
- Kullanıcı bilgilerini doğru girmiş ama cihazında zararlı yazılım imzası bulundu veya zararlı yazılım davranış tespit edildi bu bir anomalidir.
- Kullanıcı sisteme olması gerektiği gibi girmiş ama sonrasında anormal davranışlar sergilemeye başlamış; Örneğin sistemde kim olduğunu sorguluyor, sistemde ne gibi hak ve yetkilerinin olduğunu sorguluyor, sistemin neresinde olduğunu sorguluyor, başka sistemlerle temas kurmaya çalışıyor veya sisteme girdi ama saçma sapan bir şekilde belirli süredir hareketsiz durumda veya yetkisi olmayan alanlara, belgelere, sistemlere v.b. erişmeye çalışıyor. Genellikle bu tarz davranışlar siber tehdit aktörlerinin sistemi analiz etmek ve bir sonraki adımlarına karar verebilmek için uyguladığı yöntemlerdir.

ZTNA'nın Bileşenleri:

- Kimlik&Erişim Yönetimi/Identity&Access Management(IAM):Kullanıcılarımızla cihazlarının kimliklerinin doğrulanması için Çok Faktörlü Kimlik Doğrulama(MFA) ve Tek Oturum Açma(SSO) gibi teknolojilerden yararlanıldığı bölümdür.
- Politika Motoru (Policy Engine):Merkezi karar verici bileşenimizdir. Tanımladığımız güvenlik politikalarına göre erişim taleplerini değerlendirir. Örneğin; Kullanıcı Rolü, Cihaz Durumu, Lokasyon v.b.
- Erişim Aracıları (Access Agents/Gateways):Trafiği denetleyerek politikalarımızı uygulayan bileşenlerimizdir. Gateway tabanlılarda ağ kenarında veya veri merkezinde, istemci tabanlılardaysa Kullanıcı cihazlarındadırlar.
- Sürekli İzleme&Analitik:Kullanıcılarımızla cihazlarının davranışlarını gerçek zamanlı izleyerek anormallikleri tespit eder. Bu sayede erişim yetkileri dinamik olarak risk değerlendirmesine göre güncellenebilir.
- Mikro-Segmentasyon:Ağımızı küçük, yalıtılmış segmentlere ayırarak uygulamlarla veriler arasındaki erişimi kısıtladığımız bölümdür. Saldırı yüzeyini daraltarak yatay yönlü hareketi önler.
- Şifreleme:Tüm erişim trafiğini korumak için uçtan uca şifreleme sağlar.

İşte biz bu bileşenlerle oluşturduğumuz ZTNA Mimarisi sayesinde kullanıcılarımızla cihazlarının sağlık durumunun her erişim isteğinde doğrulanarak yalnızca en az ayrıcalık ilkesiyle ihtiyaç duydukları kaynaklara erişmelerini garanti altına alırız. Tabii ki bunun için ihtiyacımız olan güvenlik araçları ve birimleri vardır.
Bunlar:

- SOC(Security Operations Center/Güvenlik Operasyonları Merkezi):Bu birim ZTNA yı kullanacak, ayarlayacak, konfigürasyonlarını yapıp, politikalarını tanımlayarak ZTNA yı işletecek birimdir. Günümüzde bu yapılar Mor Takım olarak çalıştırılmakta, hem sistemlerin güvenlik açıklarını bulup, hem bu açıkları gideren, önleyen, siber tehdit istihbaratları yapan, zararlı yazılım ve davranış analizlerini yapan ve bunların tedbirlerini alarak uygulayacak ekipler olma zorunluluklarından dolayı bu birime girecek insanlar gerçekten yetkin olmalı ve her iki taraftaki kabiliyet, gelişim ve becerilerinin körelmemesi için mutlaka her hafta Mor takımın farklı bir görevini uygulamalıdırlar. Örneğin; bir hafta mavi takım üyesi olmuşsa diğer hafta kırmızı takım üyesi olmalı ki hem ilgili takım görevlerine uyum sağlamak hem de körelmemek için uluslararası standartlar bunu tavsiye etmektedir. Bir hafta mavi takımsa sonraki hafta kırmızı takım eğer bir hafta kırmızı takımsa diğer hafta mavi takımda olacak şekilde ekip üyeleri birer haftalık aralarla görev yaptıkları takımı değiştirmelidirler.
- EDR (End point Detection&Response/Uç nokta Tespit&Karşılık Sistemi):Bu sistem bizim sistemimizin uç nokta birimlerini kontrol ederek tespit edeceği anomali veya zararlı yazılıma gereken müdahaleyi yaparken ayrıca durumu bize bildirir.
- XDR (Extended Detection&Response/Genişletilmiş Algılama&Yanıt):Tehditlerin tespiti, analizi ve bunlara yanıt verilmesi süreçlerini uç noktalardan başlayarak ağ, bulut, e-posta&kimlik sistemleri gibi tüm güvenlik katmanlarımıza genişleterek tek bir platformda birleştirir.
- IDS (Intrusion Detection System/Saldırı Tespit Sistemi):Ağ veya sistemlerimizdeki trafiği sürekli izleyerek kötü amaçlı aktiviteleri, güvenlik ihlallerini ve yetkisiz erişim girişimlerini tespit eden pasif güvenlik çözümüdür. Tehditleri belirledikten sonra SOC Merkezimize ve Mor Takım Ekibimize alarm/uyarı gönderir ancak doğrudan saldırı engellemez.
- IPS (Intrusion Prevention System/Saldırı Önleme Sistemi):Ağ trafiğimizi gerçek zamanlı izleyerek kötü amaçlı aktiviteleri tespit ettikten sonra bu tehditleri otomatikmen engelleyen aktif güvenlik sistemidir. Uyarı vermenin yanında saldırı gerçekleşmeden veya zarar vermeden trafiği durdurur.
- Anti virüs:Zaten biliniyor ama sürekli güncellenen tehdit imzalarıyla davranışlarının olduğu veritabanı üzerinden sistemlerimizi tarayan ve kötü davranışlarla uyuşan herhangi bir şeyi tespit ettiği andan itibaren bizi uyaran, ilgili davranışa sebep olan veya imzayı barındıran yada her ikisini de bünyesinde barındıran uygulamayı engelleyerek karantinaya alan adeta kalkanımızdır. Sürekli güncel tutulmalıdır.
- NGFW(Next Generation Firewall/Yeni Jenerasyon Güvenlik Duvarı):Geleneksel güvenlik duvarının temel paket filtreleme yeteneklerini uygulama seviyesinde inceleme, gelişmiş tehdit önleme ve kimlik

tabanlı kontrollerle birleştiren entegre ağ güvenlik platformudur.

- SIEM(Security Information&Event Management/Güvenlik Bilgileri&Olay Yönetimi):Sistemimizin barındırdığı güvenlik ürünleri, ztna mimarimizin bölümlerinden gelen işlemler ve sistemimizde gerçekleşen her türlü olaya dair loglarla olay verilerini merkezi olarak toplayan, analiz eden, ilişkilendiren ve güvenlik tehditlerini tespit etmeye yönelik uyarılar üreten kapsamlı bir güvenlik çözümüdür. SOAR la beraber mükemmel bir uyum içinde çalışarak siber tehditlerle yapacağımız etkin mücadelede çok efektif sonuçlar sağlamaktadır.
- SOAR(Security Orchestration, Automation&Response/Güvenlik Orkestrasyon, Otomasyon&Yanıtı):SOC'nin verimliliğini artırmak için farklı güvenlik araçlarını birbirine bağlayan, tekrarlayan görevleri otomatikleştiren ve SIEM'den aldığı bilgiler doğrultusunda bünyesindeki playbook denilen senaryolara göre olaylara gereken yanıtları veren&bu süreçleri yöneten platformdur.
- Reverse Proxy(Ters Vekil Sunucu):Başta ZTNA Mimarimiz olmak üzere ağımız, sistemlerimiz ve güvenlik çözümlerimizle altyapımızı istemcilerle backend arasında konumlanarak gelen istekleri karşılayıp bunları bizim istediğimiz uygun yerlere yönlendirerek bilgilerimizi dış dünyadan gizlememize yarayan platformdur. Bu bizim için önemlidir çünkü siber tehdit aktörlerinin keşif imkanlarını sınırlandırmamızı, dolayısıyla çalışma prensiplerimizi, sistemsel bilgilerimizi, versiyon bilgilerimizi v.b. inanılmaz derecede güçleştirerek çok güçlü bir siber savunma kabiliyetimizin oluşmasını sağlar.

ZTNA Mimarimizi oluştururken dikkat etmemiz gereken noktalar:

- Öncelikle ihtiyaçlarımıza uygun, gerçekçi ve uygulanabilir Siber Güvenlik ve Bilgi Güvenliği Politikaları oluşturmalıyız. Bu politikaları işletirken sık sık kontrol edip; yenilenmesi gerekiyorsa yenilemeli, güncellenmesi gerekiyorsa güncellemeli, geliştirilmesi gerekiyorsa geliştirmeli, değiştirilmesi gerekiyorsa değiştirmeli ve hatta gerekiyorsa da toptan değiştirmeliyiz. Çünkü ihtiyaçlarımızı karşılamayan, gerçekçi ve uygulanabilir olmayan hiçbir Siber Güvenlik ve Bilgi Güvenliği Politikası bizim işimize yaramaz hatta bize açık bile oluşturabilir. Bu yüzden mutlaka sık sık dünyadaki standartları ve kendi kurumumuzun değişen ve gelişen ihtiyaçlarını da takip ederek politikalarımızla alakalı yapılması gerekenleri yapmalıyız.
- Kendimize özel ayar ve konfigürasyon yapılandırmaları. Unutmamak gerekir ki siber tehdit aktörleri öncelikle ön tanımlı ayarlarla yapılandırmaları istismar ederek sömürmeye çalışır siz eğer bunları varsayılanda bırakmışsanız başınız belada demektir. Varsayılan ayarları mutlaka kendinize göre değiştirin.
- Ayar ve konfigürasyonları doğru yapılandırma. Şimdi varsayılanda bırakmayıp ayar ve konfigürasyonları kendimize göre yapılandırırken eğer yanlış yapılandırma ve ayar yapmışsak yine siber tehdit aktörlerinin işini kolaylaştırmış oluruz dolaysıyla evet ayar ve konfigürasyon yapılandırmalarını hiçbir zaman varsayılanda bırakmayıp değiştireceğiz ama aynı zamanda bunları doğru şekilde yapmaya da özen göstermeliyiz.
- Mutlaka micro segmentasyon yapmalıyız. Her ne olursa olsun herkes her şeye erişememeli ve herkes her şeyi yapamamalıdır. Bunun için herkesin rolüne göre erişmesi gereken alana erişip sadece yapması gerekeni yapabileceği kadar mümkün olan en minimum, en sıkılaştırılmış, en düşük yetki ve haklarla en kısıtlı erişimi sağlayacak şekilde kurallarımızı yapılandırmalıyız.
- Erişim doğrulamasını çok dikkatli ve titiz bir şekilde yapılandırmalıyız. Kullanıcının erişebileceği alan ve cihazlar belirlenmiş ve sınırlandırılmış olmalı, cihazın durumunun nasıl olması gerektiği belirlenmiş olmalı ve kullanıcıya cihazında ve/veya belirlenenin aksi değişiklikler yapması halinde sisteme erişemeyeceği ve politikalara karşı geldiği için cezalandırılacağı belirtilmelidir.
- Siber tehdit aktörlerinin elinden keşif avantajını almamız için az önce de bahsettiğim gibi bilgilerin dışarıya bizim istediğimiz şekilde kısıtlı ve manipülatif çıkması için mutlaka doğru yapılandırılmış bir reverse proxy kullanmalıyız.
- Tüm güvenlik araçlarımızın da ayar ve konfigürasyonlarını kendimize göre ve doğru bir şekilde yapılandırmamız gerekiyor.
- Ve son olarakta başımıza gelebilecek felaketlere karşı yine politikalarımızı oluştururken izlememiz gereken prensipler doğrultusunda felaket müdahale ve kurtarma planları yapılandırmalıyız ve periyodik olarak bu plana göre tatbikatlar yapmalıyız.

Unutmayın ZTNA bile olsa biz insanların oluşturduğu politikalar, planlar, ayarlar, kurallar ve politikalar kadar yani bizim başarılı şekilde işletebildiğimiz kadar bizi güvende tutar!

Cem GÖKDEL
Siber Güvenlk Uzmanı(Etk/Beyaz Şapkalı Hacker)

AKILLI KAMPÜSÜN YENİ BEYNİ:
YAPAY ZEKÂ ENERJİYİ NASIL YÖNETECEK?

Üniversitelerde sensörler, bina otomasyonu ve yapay zekâ ile ölçülebilir enerji verimliliği

Bir üniversite kampüsünü küçük bir şehir gibi düşünün: derslikler, laboratuvarlar, yurtlar, kütüphaneler, veri merkezleri, spor alanları ve gün boyunca değişen binlerce kullanıcı. Bu karmaşık yapıda enerji tasarrufu yalnızca lambaları kapatmakla sınırlı değildir. Asıl mesele, binanın ne zaman, nerede ve ne kadar enerjiye ihtiyaç duyacağını öngörmek; konforu bozmadan gereksiz tüketimi azaltmaktır.

1. NEDEN ŞİMDİ?

Uluslararası Enerji Ajansı'nın (IEA) Energy Efficiency 2025 değerlendirmesine göre binalar küresel enerji talebinin yaklaşık %30'unu oluşturuyor. 2024 yılında binalardaki elektrik tüketimi 600

TWh'den fazla, yani yaklaşık %5 arttı ve küresel elektrik talebindeki toplam artışın neredeyse %60'ı binalardan geldi. Bu artışta özellikle aşırı sıcaklara bağlı soğutma ihtiyacı ve veri merkezlerinin büyümesi etkili oldu [1][2].

Üniversiteler açısından bu tablo daha da önemlidir. Kampüslerde kullanım yoğunluğu sabit değildir: bir amfi sabah dolu, öğleden sonra boş olabilir; laboratuvarlar belirli saatlerde yüksek yük çeker; yurtlar akşam saatlerinde yoğunlaşır. Geleneksel bina yönetim sistemleri çoğu zaman sabit zaman çizelgeleri ve önceden tanımlanmış sıcaklık set değerleriyle çalışır. Oysa yapay zekâ; doluluk, dış hava sıcaklığı, güneşlenme, geçmiş tüketim, ders programı ve ekipman davranışı gibi verileri birlikte değerlendirerek kontrol kararlarını dinamik hâle getirebilir.

Bu nedenle 2026'da tartışma artık 'kampüste otomasyon olsun mu?' sorusundan 'otomasyon ne kadar akıllı, ölçülebilir ve güvenli olmalı?' sorusuna kayıyor. Ağustos 2026'da yayımlanan güncel bir akademik derleme, yapay zekâ tabanlı **Isıtma, Havalandırma ve İklimlendirme (**HVAC) optimizasyonunun enerji verimliliği ve termal konfor için hızla geliştiğini; ancak gerçek saha uygulamalarında standart değerlendirme ve insan merkezli tasarım ihtiyacının sürdüğünü vurguluyor [3].

2. YAPAY ZEKÂ NEREDE DEVREYE GİRİYOR?

Tahmin: Sistem bir sonraki saat veya gün için bina yükünü tahmin eder. Hava durumu, geçmiş tüketim ve doluluk verileri bu tahminin temel girdileridir.

Optimizasyon: Isıtma, soğutma ve havalandırma set değerleri yalnızca anlık sıcaklığa göre değil, beklenen kullanım ve enerji maliyetlerine göre de ayarlanabilir.

Anomali tespiti: Normalden fazla elektrik çeken klima santrali, sürekli çalışan pompa veya kapalı olması gerekirken tüketim yapan bir alan erken fark edilebilir.

Talep yönetimi: Pik saatlerde bazı yükler konfor sınırları içinde ötelenebilir; batarya, güneş enerjisi ve şebeke tüketimi birlikte optimize edilebilir.

3. RAKAMLAR NE SÖYLÜYOR?

Burada önemli bir ayrım yapmak gerekir: Yapay zekâ için tek ve evrensel bir 'tasarruf yüzdesi' yoktur. Sonuç; binanın yaşı, iklim, mevcut otomasyon seviyesi, sensör kalitesi, kullanım profili ve kontrol stratejisine göre değişir. Bu nedenle aşağıdaki değerler farklı kaynakların kendi bağlamlarında raporladığı sonuçlardır; her kampüse doğrudan uygulanacak garanti değerleri değildir.

Kaynak / bağlam	Raporlanan değer	Ne anlama geliyor?
IEA – küresel binalar	Enerji talebinin ≈ %30'u	Bina verimliliği küresel ölçekte büyük bir kaldıraç [1].
ABD Enerji Bakanlığı – gelişmiş bina kontrolleri	HVAC'ta ortalama ≈ %30 yıllık tasarruf potansiyeli	Yüksek performanslı kontrol dizileri için ortalama potansiyel; bina türüne göre değişir [4].
MIT kampüs pilotları – AI tabanlı HVAC	Ortalama ≈ %40; günlük ≈ %20–70 aralığı	Belirli MIT binalarındaki pilot sonuçları; hava koşullarına göre değişken [5].
UNESCO – daha küçük, göreve özel AI modelleri	Belirli deneylerde %90'a kadar daha az enerji	Bu değer bina HVAC'ı değil, AI modelinin kendi hesaplama enerjisiyle ilgilidir [6].

Özellikle MIT Climate & Sustainability Consortium tarafından 24 Ağustos 2026'da paylaşılan kampüs pilotu dikkat çekici. Araştırmacıların MIT binalarında uyguladığı grafik öğrenme ve pekiştirmeli öğrenme tabanlı yaklaşım; oda doluluğu, yerel hava koşulları ve bölgeler arası termal etkileşimleri kullanıyor. Paylaşılan pilot sonuçlarında ortalama enerji tasarrufu yaklaşık %40; günlük sonuçlar ise dış sıcaklık ve güneşlenme gibi koşullara bağlı olarak yaklaşık %20 ile %70 arasında değişiyor. Kaynak, yaklaşık 45.000 ft² büyüklüğündeki bir kampüs binasında, mevcut ayarlara kıyasla aylık yaklaşık 3.000 ABD doları tasarruf sağladığına da işaret ediyor [5].

4. KAMPÜSTE NASIL KURULUR?

Başarılı bir proje, doğrudan 'AI satın almakla' başlamaz. Önce ölçüm

altyapısı ve veri kalitesi kurulmalıdır. Sağlam bir kampüs mimarisi şu katmanlardan oluşur:

Ölçüm katmanı: elektrik sayaçları, sıcaklık/nem, CO_2, doluluk, debi ve ekipman çalışma verileri.

Entegrasyon katmanı: BMS/BYS, BACnet/Modbus gibi bina protokolleri, IoT ağ geçitleri ve zaman serisi veritabanı.

Analitik katman: temel tüketim çizgisi, anomali tespiti, tahmin modelleri ve performans göstergeleri.

Kontrol katmanı: güvenli sınırlar içinde set değeri optimizasyonu ve modelin öngörülü kontrolü.

Yönetişim katmanı: yetkilendirme, loglama, siber güvenlik, veri saklama, insan onayı ve geri dönüş (fail-safe) senaryoları.

ABD Enerji Bakanlığı, modern bina kontrol sistemlerinin TCP/IP gibi standart ağ protokollerini ve BACnet gibi bina özel uygulama protokollerini kullandığını belirtiyor. Aynı kaynak, gelişmiş kontrol yöntemlerinin daha yüksek tasarruf potansiyeline sahip olabileceğini; ancak bunun doğru uygulamaya ve sürekli izlemeye bağlı olduğunu vurguluyor [4]. Bu nokta üniversite bilişim birimleri için kritik: Bina otomasyonu artık yalnızca mekanik tesisat konusu değil; aynı zamanda ağ, veri, kimlik, yazılım ve siber güvenlik konusudur.

5. DİJİTAL İKİZ: ÖNCE SANALDA DENE

2026 yılında yayımlanan çalışmalar, kampüs enerji yönetiminde dijital ikiz yaklaşımını da öne çıkarıyor. Dijital ikiz, fiziksel binanın veya kampüsün davranışını veriyle beslenen sanal bir model aracılığıyla temsil eder. Yeni bir kontrol stratejisi gerçek binaya uygulanmadan önce simülasyonda denenebilir. Mart 2026'da Scientific Reports'ta yayımlanan bir üniversite kampüsü vaka çalışması, neredeyse sıfır enerjili bina dönüşüm seçeneklerini yapay zekâ destekli tekno-ekonomik ve çevresel bir optimizasyon çerçevesiyle değerlendirdi [7]. Nisan 2026'da Türkiye'de yayımlanan başka bir çalışma da akıllı kampüsler için AI tabanlı enerji optimizasyonunu dijital ikiz simülasyonu yaklaşımıyla ele aldı [8].

6. EN BÜYÜK RİSK: KÖTÜ VERİYLE İYİ KARAR BEKLEMEK

Yapay zekâ sisteminin kalitesi, sensör ve operasyon verisinin kalitesini aşamaz. Hatalı kalibre edilmiş bir sıcaklık sensörü, yanlış doluluk verisi veya eksik sayaç telemetrisi modelin kararlarını bozabilir. Bu nedenle proje başlangıcında 'AI doğruluğu' kadar veri doğruluğu, zaman senkronizasyonu, eksik veri oranı ve sensör bakım süreçleri de KPI olarak izlenmelidir.

İkinci risk siber güvenliktir. Bina otomasyonunun kampüs IP ağına bağlanması, saldırı yüzeyini artırabilir. Kontrol ağı ile kullanıcı ağı ayrılmalı; yönetim arayüzleri çok faktörlü kimlik doğrulaması ile korunmalı; cihaz envanteri tutulmalı; firmware güncellemeleri planlanmalı; kritik kontrol kararları için güvenli varsayılan değerler ve manuel geri dönüş prosedürü bulunmalıdır. Yapay zekâ öneri üretebilir, fakat kritik mekanik sistemlerde nihai güvenlik sınırları deterministik kontrol katmanında kalmalıdır.

7. 'YEŞİL AI' PARADOKSU

Enerjiyi azaltmak için kullandığımız yapay zekânın kendisi de enerji tüketir. UNESCO'nun Green Digital Transformation çalışması, üretken yapay zekânın hesaplama gücü, elektrik ve soğutma suyu ihtiyacına dikkat çekiyor. UNESCO tarafından aktarılan deneysel sonuçlarda model sıkıştırma/kuantizasyon tekniklerinin enerji kullanımını doğruluk kaybı olmadan %44'e kadar azaltabildiği; daha kısa istemlerin %50'nin üzerinde enerji azaltımı sağlayabildiği ve göreve özel küçük modellerin bazı durumlarda büyük dil modellerine göre %90'a kadar daha az enerjiyle eşit veya daha iyi performans sunabildiği belirtiliyor [6].

Bu nedenle kampüs yaklaşımı, 'her probleme en büyük modeli çalıştırmak' olmamalıdır. Sıcaklık tahmini için küçük bir zaman serisi modeli, anomali tespiti için hafif bir makine öğrenmesi modeli ve yalnızca gerektiğinde büyük dil modeli kullanmak; hem maliyet hem de sürdürülebilirlik açısından daha rasyoneldir.

8. ÜNİVERSİTELER İÇİN 90 GÜNLÜK BAŞLANGIÇ PLANI

İlk 30 gün — en yüksek tüketimli 3–5 binayı belirleyin. Ana sayaç, HVAC ve doluluk verisinin erişilebilirliğini doğrulayın. 12 aylık tüketim temel çizgisini çıkarın.

31–60 gün — Bir pilot bina seçin. Sensör hatalarını temizleyin, saatlik tüketim tahmini ve anomali tespiti kurun. Henüz otomatik kontrol vermeden yalnızca öneri modunda çalıştırın.

61–90 gün — Konfor sınırlarını tanımlayın. Düşük riskli set değerlerinde kontrollü optimizasyon başlatın. Enerjiyi, pik talebi, iç ortam sıcaklığını, CO_2'yi ve kullanıcı şikâyetlerini birlikte ölçün.

9. SONUÇ: AKILLI KAMPÜS, DAHA FAZLA CİHAZ DEĞİL, DAHA İYİ KARAR DEMEKTİR

Akıllı kampüs kavramı çoğu zaman sensör, ekran ve otomasyon cihazlarının sayısıyla anlatılıyor. Oysa gerçek dönüşüm, verinin karara dönüşmesidir. 2026 verileri binaların enerji sistemindeki ağırlığını açık biçimde gösterirken, güncel saha uygulamaları da yapay zekâ destekli kontrolün doğru koşullarda anlamlı tasarruf sağlayabildiğini ortaya koyuyor. Ancak sonuçları genellemek yerine her kampüs kendi temel tüketimini ölçmeli, pilot uygulamayı kontrollü yürütmeli ve tasarrufu bağımsız olarak doğrulamalıdır.

"En iyi yapay zekâ projesi, en karmaşık modeli kuran değil, ölçülebilir biçimde daha az enerji harcarken kullanıcı konforunu ve sistem güvenliğini koruyandır."

KAYNAKLAR

[[1] International Energy Agency (IEA), Energy Efficiency 2025 – Buildings. Binaların küresel enerji talebindeki payı ve 2024 verileri.
[2] International Energy Agency (IEA), Global Energy Review 2025 – Electricity. 2024'te binalarda elektrik tüketimi artışı.
[3] Energy (Elsevier), "Artificial Intelligence-Based Optimization of HVAC Systems: Advances in Thermal Comfort, Energy Efficiency, Energy Consumption, Challenges, and Research Gaps", çevrimiçi yayın 25 Ağustos 2026, Article 142240.
[4] U.S. Department of Energy, "About Building Controls". Gelişmiş bina kontrol dizileri için HVAC enerji tasarrufu potansiyeli.
[5] MIT Climate & Sustainability Consortium, "Making Buildings Smarter: How AI Can Reduce Energy Waste", 24 Ağustos 2026. MIT kampüs AI-HVAC pilotları.
[6] UNESCO, "Green Digital Transformation". Enerji-verimli yapay zekâ, kuantizasyon, kısa istemler ve göreve özel modeller.
[7] Scientific Reports 16, 14599 (2026), "AI-enhanced techno-economic and environmental optimization for nearly zero-energy building retrofitting: a case study of university campus", 23 Mart 2026.
[8] Pamukkale University Journal of Engineering Sciences, "Techno-economic validation of AI-based energy optimization for smart campuses: A digital twin simulation approach", 13 Nisan 2026.

Dr. Eren Küren
Bilgisayar Mühendisi & Dijital Dönüşüm Uzmanı

Yapay Zekâ ve Geleceğin Mühendisliği: Mühendislik Meslekleri Nasıl Değişecek?

Mühendislik, insanlığın problemleri çözme biçiminin en güçlü örneklerinden biridir. Köprülerden otomobillere, elektrik şebekelerinden robotlara, üretim tesislerinden uzay araçlarına kadar modern yaşamın neredeyse her alanında mühendislik bilgisinin izlerini görmek mümkündür. Ancak mühendislik hiçbir zaman durağan bir meslek olmamıştır. El çizimlerinden bilgisayar destekli tasarıma, analog ölçüm sistemlerinden dijital sensörlere, fiziksel prototiplerden bilgisayar simülasyonlarına kadar mühendislik sürekli olarak teknolojik gelişmelerle birlikte dönüşmüştür. Bugün ise bu dönüşümün merkezinde çok daha güçlü bir teknoloji bulunmaktadır: yapay zekâ.

Yapay zekânın mühendislik alanına girmesi, yalnızca mühendislerin kullandığı yeni bir yazılımın ortaya çıkması anlamına gelmiyor. Çok daha büyük bir değişim yaşanıyor. Yapay zekâ; bilgisayar destekli tasarım, simülasyon, robotik, nesnelerin interneti, büyük veri, dijital ikizler, akıllı enerji sistemleri ve otonom teknolojilerle birleşerek mühendislik süreçlerinin tamamını yeniden şekillendirmeye başlıyor. Bir mühendis artık yalnızca hesap yapan, çizim hazırlayan veya mevcut bir sistemi analiz eden kişi olmaktan çıkıp, insan ile yapay zekâ arasında karar veren ve teknolojiyi yöneten bir profesyonel hâline geliyor.

Bu dönüşüm beraberinde önemli bir soru getiriyor:

Yapay zekâ mühendislerin yerini mi alacak, yoksa geleceğin mühendisini daha güçlü hâle mi getirecek?

Bu sorunun cevabı, büyük ölçüde yapay zekânın nasıl kullanıldığına bağlı. Çünkü mühendislik yalnızca matematiksel hesaplardan, teknik çizimlerden veya bilgisayar programlarından oluşmaz. Mühendislik aynı zamanda problemi doğru tanımlama, fiziksel gerçekliği anlama, güvenliği değerlendirme, ekonomik koşulları dikkate alma, belirsizliklerle başa çıkma ve alınan kararın sorumluluğunu üstlenme mesleğidir.

Dolayısıyla geleceğin mühendisi için asıl mesele yapay zekâ ile rekabet etmek değil, **yapay zekâyı mühendislik bilgisiyle birleştirebilmektir.**

Şekil 1. Geleceğin Mühendisliğinde İnsan, Yapay Zekâ ve Dijital Teknolojilerin Etkileşimi

Mühendislikte Yeni Dönem Başlıyor

Mühendislik tarihine bakıldığında teknolojik gelişmelerin mesleklerin çalışma biçimini sürekli değiştirdiği görülür. Bir zamanlar mühendislerin büyük bölümünü oluşturan teknik çizim işlemleri bugün bilgisayar destekli tasarım yazılımlarıyla gerçekleştirilebilmektedir.

Karmaşık matematiksel hesaplamalar bilgisayarlar tarafından saniyeler içerisinde yapılabilmekte, fiziksel prototiplerin önemli bir bölümü üretilmeden önce simülasyon ortamlarında test edilebilmektedir.

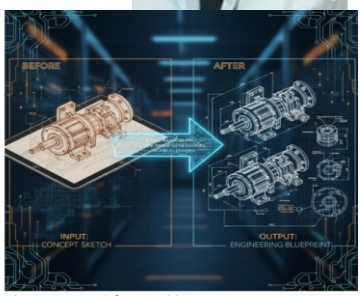
Bugün ise bu sürecin bir sonraki aşamasına geçiyoruz.

Bu aşamada bilgisayar yalnızca mühendisin verdiği komutları yerine getiren bir araç olmaktan çıkıp, **mühendislik sürecine öneriler sunabilen bir yardımcı** hâline geliyor.

Geleneksel mühendislik sürecini basitleştirirsek:

Problem → Tasarım → Hesaplama → Simülasyon → Prototip → Test → Üretim

Yapay zekâ destekli geleceğin mühendislik



Şekil 2. Mühendislik Tasarımının Geleneksel Çizimden Yapay Zekâ Destekli Tasarıma Dönüşümü

sürecinde ise bu yapı şöyle gelişebilir:

Problem → Veri → Yapay zekâ → Alternatif tasarımlar → Simülasyon → Dijital ikiz → Prototip → Gerçek veri → Optimizasyon

Buradaki en önemli fark, mühendislik sürecinin artık tek yönlü olmamasıdır. Gerçek sistemden elde edilen veriler tekrar dijital modele aktarılabilir ve sistem kendisini sürekli geliştiren bir döngüye dönüşebilir.

Bu dönüşümün temel bileşenleri

- ✓ **Yapay zekâ:** Verileri analiz eder ve tahminlerde bulunur.
- ✓ **CAD:** Tasarımların dijital ortamda oluşturulmasını sağlar.
- ✓ **Simülasyon:** Tasarımın davranışını fiziksel üretimden önce test eder.
- ✓ **IoT:** Gerçek dünyadan veri toplar.
- ✓ **Dijital ikiz:** Fiziksel sistemin sanal karşılığını oluşturur.
- ✓ **Robotik:** Dijital kararların fiziksel dünyada uygulanmasını sağlar.
- ✓ **Büyük veri:** Çok büyük miktardaki mühendislik verisinin işlenmesini mümkün kılar.

Böylece mühendislik, yalnızca "tasarla ve üret" anlayışından çıkarak **"tasarla, simüle et, izle, öğren ve yeniden optimize et"** anlayışına doğru ilerlemektedir.

Şekil 3. Yapay Zekâ Destekli CAD Sistemlerinde Üretken Tasarım ve Alternatif Geometri Oluşturma.

CAD'DEN AKILLI CAD'E: MÜHENDİS ARTIK SADECE ÇİZMEYECEK

Bilgisayar destekli tasarım, mühendislik mesleğinde gerçekleşen en büyük dönüşümlerden biridir. Geleneksel teknik çizim yöntemlerinde mühendis veya tekniker geometrinin büyük bölümünü manuel olarak oluştururken CAD sistemleri bu süreci dijital hâle getirdi. Üç boyutlu modelleme, montaj, ölçülendirme ve teknik resim işlemleri daha hızlı ve daha kontrollü biçimde gerçekleştirilebilir hâle geldi.

Şimdi ise CAD sistemleri yeni bir aşamaya geçiyor.

Yapay zekâ destekli CAD yaklaşımında mühendis yalnızca **"ne**

çizeceğini" değil, **"neyi başarmak istediğini"** tanımlamaya başlayabilir. Örneğin bir mühendis bir parçanın mümkün olduğunca hafif olmasını, belirli bir yükü taşımasını, belirli bir güvenlik katsayısını sağlamasını ve belirli bir üretim yöntemiyle üretilebilmesini isteyebilir.

Yapay zekâ bu kriterleri kullanarak farklı tasarım seçeneklerinin oluşturulmasına yardımcı olabilir.

Örneğin bir otomotiv parçası için:

- ✓ Kütle azaltılabilir.
- ✓ Dayanım korunabilir.
- ✓ Malzeme kullanımı optimize edilebilir.
- ✓ Üretim yöntemi dikkate alınabilir.
- ✓ Maliyet kriteri sisteme dahil edilebilir.
- ✓ Farklı geometriler karşılaştırılabilir.

Burada mühendislik açısından çok önemli bir nokta vardır:

Yapay zekânın oluşturduğu tasarım, otomatik olarak doğru mühendislik tasarımı değildir.

Çünkü bilgisayar tarafından matematiksel olarak optimum görünen bir geometri, gerçek üretim koşullarında üretilemeyebilir. Malzeme bulunamayabilir, işleme maliyeti yüksek olabilir veya güvenlik standartlarını karşılamayabilir.

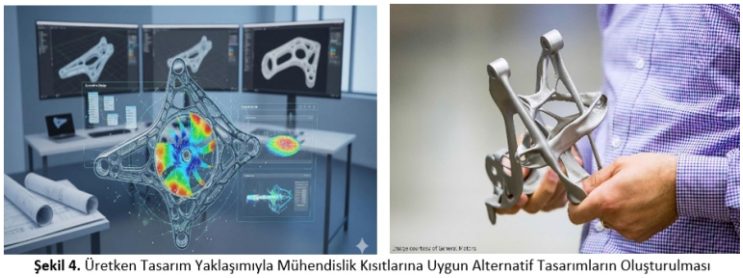
Bu nedenle geleceğin mühendisi tasarımı tamamen yapay zekâya bırakmayacak; tam tersine yapay zekânın ürettiği seçenekleri **mühendislik bilgisiyle değerlendirecektir.**

Geleceğin CAD mühendisi

- ✓ Tasarım hedeflerini belirleyecek,
- ✓ Kısıtları tanımlayacak,
- ✓ Yapay zekâya doğru problemi aktaracak,
- ✓ Alternatif tasarımları karşılaştıracak,
- ✓ Simülasyon sonuçlarını değerlendirecek,
- ✓ Üretilebilirliği kontrol edecek,
- ✓ Son mühendislik kararını verecek.

Yani mühendislikte önemli bir değişim gerçekleşebilir:

Mühendis çizimi yapan kişiden, tasarım uzayını yöneten kişiye dönüşebilir.



Şekil 4. Üretken Tasarım Yaklaşımıyla Mühendislik Kısıtlarına Uygun Alternatif Tasarımların Oluşturulması

ÜRETKEN TASARIM: BİLGİSAYAR SADECE ÇİZMEYECEK, TASARIM ÖNERECEK

Üretken tasarım yaklaşımı, yapay zekânın mühendislikteki en dikkat çekici kullanım alanlarından biridir. Geleneksel tasarımda mühendis çoğunlukla belirli bir geometriyi oluşturur ve daha sonra bu tasarımın dayanımını, ağırlığını, maliyetini veya üretilebilirliğini kontrol eder. Eğer sonuç istenilen seviyede değilse tasarım değiştirilir ve süreç yeniden tekrarlanır.

Üretken tasarımda ise sistem tasarım alanını daha geniş biçimde araştırabilir.

Mühendis: "Bu parçayı 500 gramdan daha hafif yap, ancak belirli bir yük altında güvenlik katsayısını koru." dediğinde, sistem yalnızca tek bir çözüm değil, farklı geometrik alternatifler oluşturabilir. Bu yaklaşım özellikle:

- ✓ Havacılık,
- ✓ Otomotiv,
- ✓ Robotik,
- ✓ Savunma,
- ✓ Enerji,
- ✓ İleri imalat,
- ✓ Medikal mühendislik

gibi alanlarda önemli potansiyele sahiptir. Ancak burada mühendislik bilgisinin önemi daha da artmaktadır. Çünkü seçeneklerin sayısı arttıkça doğru seçeneği belirlemek daha karmaşık hâle gelir.

Dolayısıyla yapay zekâ:

"Daha fazla seçenek" sunabilir. Mühendis ise: **"Daha doğru seçenek"** seçmek zorundadır.

Şekil 5. Dijital İkiz Teknolojisi ile Fiziksel ve Sanal Sistemlerin Gerçek Zamanlı Entegrasyonu

DİJİTAL İKİZ: GERÇEK MAKİNENİN SANAL KARDEŞİ

Bir makinenin çalışmasını anlamanın en etkili yollarından biri gerçek sistemden veri toplamaktır. Ancak fiziksel sistem üzerinde her senaryoyu denemek her zaman mümkün değildir. Bir üretim hattını durdurmak, bir motoru aşırı yüklemek veya bir enerji sisteminde riskli bir çalışma koşulu oluşturmak ekonomik ve güvenlik açısından uygun olmayabilir. Dijital ikiz yaklaşımı bu soruna farklı bir çözüm getirir.

Gerçek sistemin dijital bir karşılığı oluşturulur ve sensörlerden elde edilen veriler bu modele aktarılır. Böylece mühendis fiziksel sistemin davranışını dijital ortamda takip edebilir. Yapay zekâ bu yapıya eklendiğinde sistem daha da güçlü hâle gelir.

Örneğin bir motorun titreşim değerleri zaman içerisinde değişiyorsa yapay zekâ bu değişimi geçmiş verilerle karşılaştırabilir. Henüz arıza gerçekleşmeden önce anormal davranışın belirlenmesine yardımcı olabilir.

Bu durumda bakım anlayışı: **Arıza → Onarım** modelinden: **Veri → Tahmin → Önlem** modeline doğru değişebilir.

Dijital ikiz + yapay zekâ ile;

- ✓ Kestirimci bakım yapılabilir.
- ✓ Enerji tüketimi analiz edilebilir.
- ✓ Üretim performansı izlenebilir.
- ✓ Arıza olasılıkları tahmin edilebilir.
- ✓ Farklı senaryolar sanal ortamda denenebilir.
- ✓ Üretim optimizasyonu yapılabilir.
- ✓ Gerçek sistem ile sanal model karşılaştırılabilir.

Bu nedenle dijital ikiz geleceğin mühendislik ortamında yalnızca bir 3B model değildir. **Dijital ikiz, fiziksel sistem ile mühendis arasında sürekli iletişim sağlayan canlı bir dijital mühendislik platformudur.**

4. AKILLI FABRİKALAR: MAKİNELER KONUŞMAYA BAŞLADI

Geleceğin fabrikasını yalnızca robotların bulunduğu bir tesis olarak düşünmek eksik olur. Akıllı fabrika, makinelerin sürekli veri ürettiği, bu verilerin analiz edildiği ve üretim süreçlerinin gerçek zamanlı olarak optimize edilebildiği bir ekosistemdir. Bir üretim hattındaki robotların hareketleri, motorların sıcaklıkları, titreşim seviyeleri, üretim hızları, ürün kalite değerleri ve enerji tüketimleri sürekli olarak izlenebilir. Bu noktada yapay zekâ devreye girdiğinde fabrika yalnızca veri toplayan değil, **veriden anlam çıkarabilen bir sistem** hâline gelir.

Örneğin üretim hatalarının arttığı bir durumda yapay zekâ;

- ✓ Makine sıcaklıklarını,
- ✓ Üretim hızını,
- ✓ Hammadde özelliklerini,
- ✓ Titreşim verilerini,
- ✓ Önceki üretim sonuçlarını

aynı anda analiz ederek hatanın olası nedenlerini belirlemeye yardımcı olabilir.

Şekil 6. Akıllı Fabrikalarda Yapay Zekâ, Robotik ve Veri Analitiğinin Entegrasyonu

Mühendis ise bu sonuçları değerlendirerek fiziksel sistemi kontrol eder.

- ✓ **Akıllı fabrikanın temel bileşenleri**
- ✓ **Sensörler → Veri**
- ✓ **IoT → İletişim**
- ✓ **Yapay zekâ → Analiz**
- ✓ **Dijital ikiz → Sanal model**
- ✓ **Robotlar → Fiziksel uygulama**
- ✓ **Mühendis → Karar ve denetim**

Bu yapı geleceğin mühendisini üretim hattından uzaklaştırmayacak; tam tersine mühendisin görevini daha stratejik hâle getirecektir.

5. OTOMOTİV MÜHENDİSLİĞİ: OTOMOBİL ARTIK SADECE MEKANİK DEĞİL

Otomotiv sektörü, yapay zekânın mühendislik mesleğini değiştirdiği alanların başında geliyor. Geçmişte bir otomobilin mühendislik kimliği büyük ölçüde motor, şanzıman, fren, süspansiyon ve gövde sistemleriyle açıklanırken günümüzde otomobil giderek daha fazla elektronik, yazılım ve veri tarafından yönetilen bir sisteme dönüşüyor. Özellikle elektrikli araçların yaygınlaşmasıyla batarya yönetimi, enerji optimizasyonu ve termal yönetim gibi konular daha önemli hâle geldi. Bunun yanında kamera, radar, lidar ve diğer sensörlerden elde edilen verilerin işlenmesi, sürüş destek sistemleri ve otonom sürüş teknolojileri yapay zekânın otomotiv mühendisliğiyle doğrudan birleşmesini sağlıyor.

Bu dönüşüm otomotiv mühendisinin bilgi alanını genişletiyor.

Geleceğin otomotiv mühendisi;

- ✓ Mekanik,
- ✓ Elektrik-elektronik,
- ✓ Kontrol,
- ✓ Yazılım,
- ✓ Yapay zekâ,
- ✓ Batarya,
- ✓ Sensör,
- ✓ Veri analitiği

Şekil 7. Elektrikli ve Bağlantılı Araçlarda Yapay Zekâ Destekli Akıllı Sistemlerin Entegrasyonu

alanlarının birbiriyle nasıl çalıştığını anlamak zorunda kalabilir.

Otomobil artık yalnızca hareket eden bir makine değildir.

Otomobil; veri üreten, veriyi işleyen, çevresini algılayan ve bazı kararları yazılım aracılığıyla verebilen bir mühendislik platformudur.

Bu nedenle otomotiv mühendisliğinin geleceği yalnızca daha güçlü motorlar veya daha hafif gövdeler üzerine değil, **daha akıllı ve daha bağlantılı araçlar** üzerine de kurulacaktır.

6. ENERJİ ŞEBEKELERİ: YAPAY ZEKÂ İLE ÖĞRENEN ŞEBEKELER

Enerji sistemleri de giderek daha karmaşık hâle geliyor. Güneş ve rüzgâr enerjisinin artması, elektrikli araçların yaygınlaşması, enerji depolama sistemlerinin gelişmesi ve tüketicilerin aynı zamanda enerji üreticisi hâline gelmesi elektrik şebekelerinin çalışma biçimini değiştiriyor.

Eskiden temel soru:

"Ne kadar elektrik üretmeliyiz?" iken geleceğin enerji sistemlerinde sorular daha karmaşık hâle geliyor:

"Ne zaman üretmeliyiz?"

"Enerjiyi nerede depolamalıyız?"

"Talep ne zaman artacak?"

"Güneş ve rüzgâr üretimi ne kadar olacak?"

"Elektrikli araçların şarj yükü şebekeyi nasıl etkileyecek?"

Yapay zekâ bu soruların cevaplanmasında önemli bir yardımcı olabilir.

Şekil 8. Yapay Zekâ Destekli Akıllı Enerji Sistemlerinde Üretim, Tüketim ve Depolama Optimizasyonu

Örneğin geçmiş tüketim verileri, hava durumu, güneş ışınımı ve rüzgâr verileri birlikte analiz edilerek yenilenebilir enerji üretimi ve tüketim tahminleri yapılabilir.

Bu sayede enerji mühendisliği:

üretim odaklı bir anlayıştan, **tahmin + optimizasyon + yönetim** odaklı bir anlayışa doğru ilerleyebilir.

7. ROBOTLAR MÜHENDİSLERİN YERİNİ ALACAK MI?

Yapay zekâ ve robotik hakkında konuşulduğunda en sık sorulan sorulardan biri şudur:

"Robotlar mühendislerin yerini alacak mı?"

Bu soruya yalnızca "evet" veya "hayır" şeklinde cevap vermek doğru değildir. Çünkü robotların kendisi bile mühendislik ürünüdür. Bir robotun ortaya çıkabilmesi için mekanik tasarım, elektronik

sistemler, kontrol algoritmaları, yazılım, sensörler, güvenlik sistemleri ve yapay zekâ gibi birçok alanın birlikte çalışması gerekir. Dolayısıyla robotların gelişmesi mühendislik ihtiyacını tamamen ortadan kaldırmak yerine mühendisliğin niteliğini değiştirebilir.

Gelecekte:
İnsan → Amaç ve karar
Yapay zekâ → Analiz ve öneri
Robot → Fiziksel uygulama
şeklinde bir çalışma modeli daha fazla görülebilir.
Bu modelde mühendis, robotun yaptığı her hareketi manuel olarak programlamak yerine sistemin hedeflerini, güvenlik sınırlarını ve çalışma koşullarını belirleyen kişi hâline gelebilir.

GELECEĞİN MÜHENDİSİNDE EN DEĞERLİ YETENEK: DOĞRU SORUYU SORMAK

Yapay zekâ çağının en önemli paradokslarından biri şudur: Bilgiye ulaşmak kolaylaştıkça **doğru soruyu sormanın değeri artmaktadır.** Yapay zekâ çok büyük miktarda bilgi üretebilir. Ancak yanlış tanımlanan bir probleme verilen çok başarılı bir cevap bile gerçek dünyada hiçbir işe yaramayabilir.

Şekil 10. Yapay Zekâ Çağında Mühendislik Problemlerinin Tanımlanması ve Doğru Soru Oluşturma Süreci

Örneğin:
"Bu parçayı optimize et." ifadesi yeterince açık değildir.
Buna karşılık: **"Bu parçanın kütlesini azaltırken 2 kN yük altında güvenlik katsayısını koru, mevcut malzemeyi kullan ve CNC üretimine uygun geometriler oluştur."**
çok daha güçlü bir mühendislik problemidir.
Geleceğin mühendisinin;

- ✓ Problemi doğru tanımlaması,
- ✓ Kısıtları belirlemesi,
- ✓ Veriyi doğru seçmesi,
- ✓ Yapay zekâdan doğru çıktıyı istemesi,
- ✓ Sonuçları doğrulaması,
- ✓ Alternatifleri karşılaştırması gerekecektir.

Bu nedenle yapay zekâ çağında **"soru sorma becerisi"**, mühendislik eğitiminin önemli bir parçası hâline gelebilir.

YAPAY ZEKÂNIN EN BÜYÜK RİSKİ: YANLIŞ SONUCA GÜVENMEK

Yapay zekâ mühendislikte çok güçlü bir araç olabilir. Ancak güçlü olmak kusursuz olmak anlamına gelmez. Bir yapay zekâ sistemi son derece ikna edici bir cevap verebilir ve bu cevap yanlış olabilir. Mühendislikte bu durum basit bir bilgi hatasından çok daha ciddi sonuçlar doğurabilir.
Yanlış bir tasarım;

- ✓ Ürün güvenliğini,
- ✓ Yapısal dayanımı,
- ✓ Enerji sistemlerinin kararlılığını,
- ✓ Üretim kalitesini,
- ✓ İnsan güvenliğini etkileyebilir.

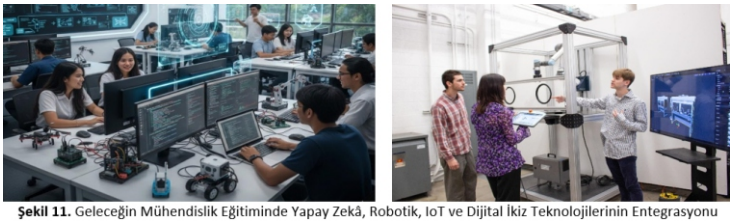
Bu nedenle geleceğin mühendisi yapay zekâdan gelen sonucu doğrudan kabul etmek yerine onu sorgulamalıdır.
Mühendisin AI çıktısına soracağı sorular:

- ✓ Veri güvenilir mi?
- ✓ Veri güncel mi?
- ✓ Model hangi varsayımları kullanıyor?
- ✓ Sonuç fiziksel olarak mümkün mü?
- ✓ Hata payı nedir?
- ✓ Sonuç farklı bir yöntemle doğrulanabilir mi?
- ✓ Güvenlik sınırları korunuyor mu?
- ✓ Bu kararın sorumluluğu kimde?

Burada temel prensip çok nettir: **Yapay zekâ öneri verebilir; mühendis doğrulamak zorundadır.**

MÜHENDİSLİK EĞİTİMİ DEĞİŞMEDEN MÜHENDİSLİK DEĞİŞEMEZ

Yapay zekâ mühendislik mesleklerini değiştiriyorsa üniversitelerin mühendis yetiştirme biçimi de değişmek zorundadır. Ancak bu değişim, temel mühendislik derslerinin önemini azaltmak anlamına gelmemektedir. Tam tersine matematik, fizik, mekanik, elektrik, kontrol ve diğer temel mühendislik bilgileri yapay zekâ çağında da mühendislik kararlarının temelini oluşturmaya devam edecektir.
Değişmesi gereken şey, öğrencinin bu bilgileri nasıl kullandığıdır.
Geleceğin mühendislik öğrencisi yalnızca bir problemi kâğıt üzerinde çözmek yerine gerçek bir probleme çözüm geliştirmelidir.



Şekil 11. Geleceğin Mühendislik Eğitiminde Yapay Zekâ, Robotik, IoT ve Dijital İkiz Teknolojilerinin Entegrasyonu

Örneğin:
"Üniversite kampüsünün enerji tüketimini %15 azaltacak akıllı enerji yönetim sistemi tasarla."
Bu tek proje içerisinde öğrenci:

- ✓ Sensörlerden veri toplar.
- ✓ IoT sistemi oluşturur.
- ✓ Enerji tüketim profili çıkarır.
- ✓ Yapay zekâ ile tüketimi tahmin eder.
- ✓ Dijital ikiz oluşturur.
- ✓ Farklı senaryoları simüle eder.
- ✓ Enerji yönetim algoritması geliştirir.
- ✓ Ekonomik analiz yapar.
- ✓ Sonuçları sunar.

Bu model öğrenciyi yalnızca sınava değil, **gerçek mühendislik hayatına** hazırlar.

SINAVLARIN YERİNE PROJELER Mİ GELECEK?

Yapay zekânın yaygınlaşması üniversitelerin ölçme-değerlendirme sistemlerini de yeniden düşünmesini gerektirebilir. Çünkü bir öğrencinin yapay zekâ yardımıyla bir problem çözebilmesi, o öğrencinin problemi gerçekten anlayıp anlamadığını tek başına göstermeyebilir.
Bu nedenle gelecekte değerlendirme sistemlerinde yalnızca sonuca değil, **sürece** daha fazla önem verilmesi mümkündür.
Bir mühendislik öğrencisinden;

- ✓ Tasarım kararını açıklaması,
- ✓ Kullandığı verileri göstermesi,
- ✓ Yapay zekâdan nasıl yararlandığını belirtmesi,
- ✓ AI çıktısını doğrulaması,
- ✓ Simülasyon sonuçlarını yorumlaması,

- ✓ Prototip veya deney sonucu sunması,
- ✓ Tasarımını sözlü olarak savunması istenebilir.

Bu yaklaşım yapay zekâyı yasaklamak yerine öğrencinin onu **etik, bilinçli ve mühendislik kurallarına uygun kullanmasını** sağlar.

KKTC İÇİN FIRSAT: AKILLI MÜHENDİSLİK KAMPÜSLERİ

Yapay zekâ çağındaki mühendislik dönüşümü KKTC açısından da önemli fırsatlar sunmaktadır. Özellikle üniversitelerin uluslararası rekabet gücünü artırmak için yapay zekâ, dijital ikiz, akıllı enerji sistemleri, robotik, IoT ve ileri mühendislik simülasyonları bir araya getirilebilir.

Şekil 12. Akıllı Kampüs Modelinde Yapay Zekâ, IoT, Dijital İkiz ve Enerji Sistemlerinin Entegrasyonu

KKTC'deki üniversiteler, kampüslerini aynı zamanda **yaşayan mühendislik laboratuvarlarına** dönüştürebilir.

Örneğin bir kampüste;

- ✓ Güneş panelleri,
- ✓ Elektrikli araç şarj istasyonları,
- ✓ Batarya depolama sistemi,
- ✓ IoT sensörleri,
- ✓ Akıllı bina otomasyonu,
- ✓ Robotik sistemler,
- ✓ Dijital ikiz,
- ✓ Yapay zekâ destekli enerji yönetimi birlikte çalışabilir.

Öğrenciler teorik bilgilerini gerçek kampüs verileri üzerinde uygulayabilir.

Bu yaklaşım yalnızca eğitim açısından değil, araştırma açısından da güçlü sonuçlar doğurabilir.

KKTC için oluşturulabilecek örnek bir model:

Akıllı Kampüs → Veri Toplama → Dijital İkiz → Yapay Zekâ → Optimizasyon → Gerçek Sistem → Yeni Veri

Bu döngü sayesinde üniversite kampüsü, öğrencilerin üzerinde gerçek mühendislik problemleri çalışabileceği **yaşayan bir test alanına** dönüşebilir.

2035'TE BİR MÜHENDİSLİK OFİSİ

Yıl 2035.

Bir mühendislik ofisinde yeni bir ürün tasarlanıyor. Mühendis tasarım hedeflerini belirliyor. Yapay zekâ geçmiş projeleri analiz ediyor ve farklı tasarım alternatifleri öneriyor. CAD sistemi bu alternatifleri üç boyutlu modele dönüştürüyor. Simülasyon sistemi tasarımları test ediyor. Dijital ikiz, ürünün gerçek dünyadaki davranışını tahmin ediyor.

Daha sonra ilk prototip üretiliyor.

Sensörler prototipten veri topluyor.

Veriler tekrar yapay zekâ sistemine aktarılıyor.

Yapay zekâ yeni bir optimizasyon öneriyor.

Mühendis öneriyi inceliyor ve karar veriyor.

Bu süreç:

Fikir → AI → CAD → Simülasyon → Dijital İkiz → Prototip → Sensör → Veri → AI → Optimizasyon şeklinde sürekli devam ediyor.

Böyle bir çalışma ortamında mühendis artık bilgisayar başında yalnızca hesap yapan kişi değildir. Mühendis: **tasarım yöneticisi, veri analisti, sistem düşünürü, doğrulayıcı ve karar verici** hâline gelir.

Şekil 13. Geleceğin Mühendislik Ofisinde Yapay Zekâ, CAD, Simülasyon ve Dijital İkiz Teknolojilerinin Entegrasyonu

GELECEĞİN MÜHENDİSİ HANGİ YETKİNLİKLERE SAHİP OLMALI?

Geleceğin mühendisini yalnızca bir diploma veya belirli bir program bilgisi tanımlamayacaktır. Mühendisin asıl değeri farklı teknolojileri bir araya getirerek gerçek problemleri çözebilme kapasitesinde olacaktır.

Geleceğin mühendisi;

1. Güçlü temel mühendislik bilgisine sahip olmalı.

Matematik, fizik ve temel mühendislik prensipleri vazgeçilmezdir.

2. Yapay zekâ okuryazarı olmalı.

AI'ın nasıl çalıştığını ve sınırlarını bilmeli.

3. Veri okuyabilmeli.

Sensörlerden ve dijital sistemlerden gelen verileri yorumlayabilmeli.

4. Simülasyon kullanabilmeli.

Gerçek sistemleri sanal ortamda test edebilmeli.

5. Dijital ikizleri anlayabilmeli.

Gerçek ve sanal sistem arasındaki ilişkiyi kurabilmeli.

6. Disiplinlerarası düşünebilmeli.

Makine, elektrik, elektronik, yazılım ve yapay zekâ arasındaki bağlantıları görebilmeli.

7. Eleştirel düşünebilmeli.

Yapay zekâ tarafından verilen sonuçları sorgulayabilmeli.

8. Etik sorumluluk taşımalı.

Teknik olarak mümkün olan her şeyin yapılması gerekmediğini bilmeli.

9. İletişim kurabilmeli.

Farklı disiplinlerden insanlarla etkili çalışabilmeli.

10. Sürekli öğrenmeli.

Çünkü teknoloji değiştikçe mühendislik bilgisi de sürekli gelişmektedir.

İNSAN MI, YAPAY ZEKÂ MI?

İnsan mı daha yaratıcı? Yapay zekâ mı daha hızlı? İnsan mı daha iyi karar verir? Yapay zekâ mı daha fazla veriyi analiz eder? Bu soruları bir yarışma gibi değerlendirmek yerine güçlü ve zayıf yönleri birlikte düşünmek daha doğru olacaktır.

Şekil 14. Geleceğin Mühendisliğinde İnsan ve Yapay Zekânın Tamamlayıcı İş Birliği

İnsan;

- ✓ Amaç belirler.
- ✓ Bağlamı değerlendirir.
- ✓ Etik karar verir.
- ✓ Sorumluluk üstlenir.
- ✓ Deneyimden yararlanır.
- ✓ Belirsizlikleri değerlendirir.
- ✓ Yaratıcı düşünür.

Yapay zekâ;

- ✓ Büyük veriyi hızlı analiz eder.
- ✓ Örüntüleri bulabilir.
- ✓ Alternatifler oluşturabilir.
- ✓ Tahmin yapabilir.
- ✓ Optimizasyonu hızlandırabilir.
- ✓ Tekrarlayan görevleri otomatikleştirebilir.

Bu nedenle geleceğin en güçlü mühendislik modeli büyük olasılıkla: **İnsan + Yapay Zekâ + Mühendislik Bilgisi** üçlüsünün birlikte çalıştığı model olacaktır.

GELECEĞİN MÜHENDİSİ İÇİN 7 ALTIN KURAL

1. Mühendisliği öğren, yalnızca yazılımı değil.
Çünkü kullanılan teknoloji değişebilir; mühendisliğin temel prensipleri değişmez.

2. Yapay zekâyı kullan ama ona körü körüne güvenme.
Her AI çıktısı mühendislik doğrulamasından geçmelidir.

3. Veriyi anlamayı öğren.
Geleceğin sistemleri büyük miktarda veri üretecektir.

4. Dijital ikiz ve simülasyon teknolojilerini öğren.
Gerçek sistemleri fiziksel olarak test etmeden önce sanal ortamda değerlendirmek önemli hâle gelecektir.

5. Disiplinlerarası düşün.
Geleceğin otomobili yalnızca mekanik değil; elektronik, yazılım, enerji ve yapay zekâ sistemlerinin birleşimidir.

6. Etik sorumluluğu unutma.
Mühendislikte teknik başarı kadar güvenlik ve toplumsal sorumluluk da önemlidir.

7. Öğrenmeyi bırakma.
Geleceğin mühendisi mezun olduğu gün öğrenmeyi bırakmayacak; meslek hayatı boyunca kendisini geliştirecektir.

SONUÇ

YAPAY ZEKÂ MÜHENDİSLİĞİ YOK ETMEYECEK, DÖNÜŞTÜRECEK

Mühendislik tarihindeki büyük teknolojik dönüşümlere baktığımızda önemli bir gerçek görülmektedir. Bilgisayarların ortaya çıkması mühendisliği yok etmedi. CAD sistemlerinin yaygınlaşması mühendisleri ortadan kaldırmadı. Simülasyon teknolojilerinin gelişmesi laboratuvarları gereksiz hâle getirmedi. Robotların fabrikalara girmesi mühendislik mesleğinin sonunu getirmedi.

Bunların tamamı mühendislerin çalışma biçimini değiştirdi.

- ✓ Yapay zekâ için de benzer bir dönüşüm yaşanması muhtemeldir.
- ✓ Bazı rutin hesaplamalar otomatikleşebilir.
- ✓ Bazı tasarımlar yapay zekâ tarafından oluşturulabilir.
- ✓ Bazı bakım süreçleri tahmine dayalı hâle gelebilir.
- ✓ Bazı raporlama işlemleri otomatikleşebilir.
- ✓ Bazı üretim kararları algoritmalar tarafından desteklenebilir.
- ✓ Fakat aynı zamanda yeni mühendislik alanları da ortaya çıkacaktır.

Örneğin;

- ✓ Yapay zekâ destekli tasarım mühendisliği,
- ✓ Dijital ikiz mühendisliği,
- ✓ Akıllı üretim mühendisliği,
- ✓ Otonom sistem mühendisliği,
- ✓ Robotik ve yapay zekâ mühendisliği,
- ✓ Akıllı enerji sistemleri mühendisliği,
- ✓ AI doğrulama ve güvenlik uzmanlığı,
- ✓ İnsan-makine etkileşimi uzmanlığı gibi alanların önemi artabilir.

Dolayısıyla asıl soru:
"Mühendislik ortadan kalkacak mı?" olmamalıdır.
Asıl soru: **"Mühendislik nasıl dönüşecek?"** olmalıdır.
Çünkü geleceğin mühendisi yapay zekâ ile yarışmayacaktır.
Yapay zekâyı yönetecektir.

- ✓ Yapay zekâ çok büyük miktarda veriyi analiz edebilir.
- ✓ Mühendis ise bu verinin ne anlama geldiğini sorgulayacaktır.
- ✓ Yapay zekâ binlerce tasarım alternatifi oluşturabilir.
- ✓ Mühendis hangi tasarımın güvenli ve üretilebilir olduğuna karar verecektir.
- ✓ Yapay zekâ bir sistemdeki anormalliği tespit edebilir.
- ✓ Mühendis bunun fiziksel nedenini araştıracaktır.
- ✓ Yapay zekâ bir enerji sistemi için optimizasyon önerebilir.

Mühendis bu önerinin ekonomik, teknik ve çevresel sonuçlarını değerlendirecektir.

Bu nedenle geleceğin mühendisliği insan ile yapay zekânın birbirine rakip olduğu bir dünya olmayacaktır. Daha güçlü ihtimal, **insan zekâsının yapay zekâyı yönlendirdiği ve yapay zekânın insanın mühendislik kapasitesini genişlettiği bir çalışma modeli** olacaktır.

Ve geleceğin mühendisi için belki de en önemli beceri şu olacaktır:
Yapay zekânın verdiği cevabı bilmek değil, o cevabın doğru olup olmadığını anlayabilmek. Çünkü mühendisliğin temel sorumluluğu hiçbir zaman yalnızca bir çözüm üretmek değildir. Asıl sorumluluk; **doğru, güvenli, ekonomik, sürdürülebilir ve insan yararına bir çözüm üretmektir.** Bu nedenle yapay zekâ çağında mühendislik eğitiminin hedefi, yapay zekâdan korkan mühendisler yetiştirmek değil; **yapay zekâyı anlayan, sorgulayan, doğrulayan ve doğru amaçlar için kullanabilen mühendisler yetiştirmek** olmalıdır.

Ve belki de geleceğin mühendisliğini tek bir cümleyle ifade etmek mümkündür:

"Yapay zekâ mühendisin yerini almayacak; yapay zekâyı doğru kullanan mühendis, mühendisliğin sınırlarını yeniden çizecek."

Kaynakça

1. Aksakal, N. Y., & Ülgen, B. (2021). Yapay zekâ ve geleceğin meslekleri. TRT Akademi, 6(13), 834–853. https://doi.org/10.37679/trta.969285
2. Akbaş, M., & Altunışık, R. (2025). Dijital dönüşümün meslekler üzerindeki etkileri: Geleceğin meslekleri ve gerekli yetkinlikler. Yönetim Bilimleri Dergisi, 23(55), 82–113. https://doi.org/10.35408/comuybd.1462900
3. Demirtaş, E. A., Sağır Özdemir, M., Alpay, Ş., Özkan, N. F., Hasgül, S., & Sipahioğlu, A. (2023). Teknolojik gelişmeler ışığında endüstri mühendisliğinin geleceği. Eskişehir Osmangazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi, 31(4).
4. Çark, Ö. (2020). Dijital dönüşümün işgücü ve meslekler üzerindeki etkileri. International Journal of Entrepreneurship and Management Inquiries, 4(Özel Sayı 1), 19–34.
5. Varnalı, T. (2024). Yapay zekâ kariyerlerinin geleceği: Küresel büyüme ve fırsatlar. Kamu Yönetimi ve Politikaları Dergisi, 5(2), 189–228. https://doi.org/10.58658/kaypod.1484053
6. Akgül, H., & Ayer, Z. (2020). Kariyer gelişimi bağlamında Sanayi 4.0'ın meslek seçimine etkisine yönelik bir analiz. Akademik İncelemeler Dergisi, 15(1), 223–244. https://doi.org/10.17550/akademikincelemeler.597581
7. Yükseköğretim Kurulu. (2019). Geleceğin meslekleri çalışmaları. Yükseköğretim Kurulu Başkanlığı.
8. Aksu, S. G., & Sürgevil, O. (2019). Dijital çağın yetkinlikleri: Çalışanlar, insan kaynakları uzmanları ve yöneticiler çerçevesinden bakış. Dijital Çağda İşletme Dergisi, 2(2), 54–68.
9. Kılıç, S. (2026). Potansiyel çalışanlarda yapay zekâ kaygısı: Sektör tercihi, dijital yetkinlik düzeyi ve demografik özellikler açısından bir değerlendirme. Ömer Halisdemir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 19, 1–27. https://doi.org/10.25287/ohuiibf.1721842
10. Türkiye Yeterlilikler Çerçevesi. (2026). Yapay zekâ ve veri mühendisliği program profili. İstanbul Teknik Üniversitesi.

Yrd. Doç. Dr. Cemal Kavalcıoğlu
Yakın Doğu Üniversitesi
Mühendislik Fakültesi
Elektrik ve Elektronik Mühendisliği
Öğretim Üyesi

Domain Benzerliklerinin Ötesi: Klonlanmış Oltalama (Phishing) Sitelerini Avlama

Siber güvenlik dünyasında oltalama (phishing) saldırıları yıllardır en çok can yakan tehdit vektörlerinden biri olmaya devam ediyor [Anti-Phishing Working Group (APWG), 2026]. Kurumlar ve son kullanıcılar genellikle "URL'yi kontrol etme" veya "SSL sertifikasına bakma" gibi temel önlemlerle eğitiliyor. Ancak günümüzde siber tehdit aktörleri, alan adı (domain) benzerliklerinin örneğin typosquatting veya homoglyph saldırılarının çok ötesine geçmiş durumda [Bazzell, 2024]. Artık hedeflerinde, kurbanın güvenini kazanmak için kurumun web arayüzünü pikseli pikseline, kodu koduna kopyaladıkları "klon siteler" var.

Saldırganlar, hedefledikleri kurumun web sayfasını HTTrack, wget gibi popüler araçlarla veya kendi geliştirdikleri özel botlarla saniyeler içinde kopyalayabiliyorlar. Bu noktada, Siber Tehdit İstihbaratının (CTI) bir sonraki evresi devreye giriyor: Gerçek web sayfalarının tasarımının veya içeriklerinin yetkisiz kişilerce kopyalandığını tespit etmek.

Tehdidin Boyutu: Türkiye ve KKTC'den Çarpıcı Vaka Analizleri
Klonlama taktiklerinin teorik risklerinden çıkıp gerçek dünyaya baktığımızda, özellikle Türkiye (TC) ve Kuzey Kıbrıs Türk Cumhuriyeti (KKTC) ekosistemlerinde bu yöntemlerin ne kadar ikna edici ve yıkıcı sonuçlar doğurduğunu görebiliriz.

Türkiye'de e-Devlet ve PTT Oltalamaları:
Türkiye'de siber saldırganların en sık başvurduğu yöntemlerden biri, kitleleri manipüle eden panik veya merak duygusunu kullanmaktır. Vatandaşlara gönderilen "HGS borcunuz icraya verilmiştir" veya "PTT Kargonuz gümrükte takıldı, teslimat için vergi ödemeniz gerekmektedir" şeklindeki SMS'ler, kurbanları doğrudan klonlanmış sitelere yönlendirdi [T.C. İçişleri Bakanlığı, 2025].
Bu linklere tıklayan kullanıcılar, PTT'nin, HGS portalının veya e-Devlet kapısının (turkiye.gov.tr) birebir kopyalanmış arayüzleriyle karşılaştı. Arayüz o kadar kusursuz kopyalanmıştı ki, Sahte sayfalar, e-Devlet ve diğer kurumların logo, tasarım öğeleri ve sayfa düzenlerini taklit ederek kullanıcıda meşru site algısı oluşturabilmektedir. Adres çubuğundaki ince harf oyunlarını (örneğin turkiye-gov-tr.com veya e-devlet.com - küçük L harfi ile) fark etmeyen vatandaşlar, T.C. Kimlik numaralarını ve kredi kartı bilgilerini kendi elleriyle saldırganlara teslim ettiler.

KKTC'de Kıb-Tek Örneği:
Benzer bir siber dalga KKTC'de de etkili oldu. Özellikle Kıbrıs Türk Elektrik Kurumu'nun kurumsal arayüzü kopyalanarak, adadaki vatandaşlara online ödeme temalı oltalama mesajları iletildi [Kıbrıs Postası, 2024].
Daha tehlikeli olanı ise, HTTrack gibi araçlarla klonlandı. Saldırganlar bu klon siteleri barındıran sahte alan adları için "Google Ads" reklamları satın aldı (Search Engine Poisoning). Arama motoruna servis alacağı kurumun adını yazan müşteriler, en üstte sponsorlu olarak çıkan linke tıkladıklarında, görsel olarak kendi ziyaret edip gitmesi gereken sitenin aynısı olan sahte sitelere giriş yaptılar. SMS doğrulama kodlarını (OTP) bile eşzamanlı çalışan oltalama panellerine giren müşterilerin hesapları dakikalar içinde boşaltıldı [BGA Security, 2019].

Bu somut örnekler bize acı bir gerçeği gösteriyor: Sadece son kullanıcıyı eğitmek tek başına yeterli değildir. Kurumların kendi dijital varlıklarını avlayan bu siteleri aktif olarak bulup henüz kimse mağdur olmadan imha etmesi şarttır. Peki, devasa internet okyanusunda sizin sitenizin kopyalarını nasıl bulabilirsiniz?

İşte bu avcılık işleminde hem proaktif hem de reaktif yaklaşımları harmanlayan üç profesyonel strateji:

1. Dijital Tuzaklar: Kaynak Koduna "Canary" (Web Beacon) Yerleştirmek (En Etkili Yöntem)
Saldırganların sitenizi klonlarken kullandıkları araçlar genellikle kördür; sayfadaki tüm HTML, CSS ve JavaScript dosyalarını ayrım gözetmeksizin çekerler. Klonlama faaliyetini tespit etmenin klonlanmış siteleri erken aşamada tespit etmek için düşük maliyetli ve pratik yöntemlerden biridir, en hızlı ve maliyet etkin yolu, sitenizin kaynak koduna dijital tuzaklar yerleştirmektir [Thinkst Applied Research, 2024].

Bu Sistem Nasıl Çalışır?
Web sitenizin kaynak koduna (örneğin HTML gövdesine veya kritik bir JavaScript dosyasının içine) dışarıdan bakıldığında hiçbir işlevi yokmuş gibi görünen, görünmez bir piksel (1x1 image) veya asenkron bir betik (script) eklenir.

Örnek bir Canary Token şu şekilde görünebilir:
<!-- <img src="https://istihbarat-sunucunuz.kazimates.com/canary.png" style="display:none;"> -->

Saldırgan, orijinal sitenizi kopyaladığında bu görünmez kodu da kendi sahte sunucusuna taşıdığının farkına varmaz. Hedeflenen kurban veya saldırganın kendisi bu sahte siteyi tarayıcısında açtığında, tarayıcı bu görünmez resmi yüklemek için gizlice sizin istihbarat sunucunuza bir istek (request) gönderir.

Anında İstihbarat:
Bu istek sunucunuza ulaştığı anda, HTTP Referer başlığı (header) sayesinde tuzağın hangi sahte alan adında ve hangi IP adresinde tetiklendiğini anında görürsünüz. Bu alarm doğrudan SIEM altyapınıza düşebilir. Bu yöntem, sahte site daha yayıldığı ilk dakikalarda tespit imkanı sunduğu için en etkili yaklaşımdır [Thinkst Applied Research, 2024].

2. Kodların İzini Sürmek: Özgün Metin (Unique String) Taraması
Eğer sitenize önceden bir tuzak yerleştirmediyseniz veya saldırganlar kodu kopyaladıktan sonra temizlemeye çalıştıysa, internetin karanlık ve aydınlık köşelerini tarayan arama motorlarını kullanmanız gerekir. Burada bahsettiğimiz Google değil; internete bağlı cihazları, sunucuları ve web sayfalarının kaynak kodlarını durmaksızın indeksleyen Shodan, Censys ve FOFA gibi siber istihbarat arama motorlarıdır [Bazzell, 2024].

Avın Başlaması:
Siber güvenlik uzmanları, orijinal sitenin HTML/JS kodunda, sadece o kuruma ait olan, çok spesifik bir cümle, bir telif hakkı yazısı veya benzersiz bir dosya yolu belirler (Örneğin: href="/assets/css/kktc-ozel-gov-tema-v4.css").
Bu benzersiz metin, Shodan veya FOFA üzerinde aratıldığında, sistemler saniyeler içinde dünya üzerindeki tüm aktif IP adreslerini tarayarak sizin kodlarınızı barındıran sunucuları listeler. Sonuç olarak, henüz bir oltalama alan adı atanmamış, sadece bir IP adresi üzerinde test aşamasında olan sahte bir siteyi bile canlıya alınmadan önce tespit edip kapattırabilirsiniz.

3. Makinenin Gözüyle Görmek: Görsel Benzerlik (Visual Hashing) Taraması
Gelişmiş saldırganlar, ilk iki yöntemi atlatmak için sitenin kaynak kodunu tamamen baştan yazabilir veya içerikleri dinamik olarak değiştiren gelişmiş oltalama kitleri (Phishing-as-a-Service) kullanabilir. Bu durumda arka plandaki kodlar sizin sitenizle aynı olmayacaktır; ancak sitenin ön yüzü (görseli) kurbanı kandırmak zorunda olduğu için orijinaliyle aynı kalmak zorundadır.

İşte bu noktada siber istihbaratın en yenilikçi alanlarından biri olan Visual Hashing (Görsel Özetleme) devreye girer. Gelişmiş siber istihbarat platformları, orijinal sitenizin ekran görüntüsünü alır ve bunu bir matematiksel öze çevirir. Çalışma CSS ve sayfa düzeni (page-layout) özelliklerini çıkarıp makine öğrenmesiyle görsel benzerlik sınıflandırması yapılabildiğini göstermektedir [Mao vd., 2019]. Standart kriptografik algoritmaların aksine pHash, resmin veri bütünlüğünden ziyade görsel karakteristiklerini hesaplar

Süreç Nasıl İşler?
İnternetteki yeni açılan binlerce şüpheli sitenin ekran görüntüleri otomatik tarayıcılarla alınır ve sizin sitenizin pHash değeri ile karşılaştırılır. Renk paletleri, butonların yeri, logolar ve sayfa düzeni analiz edilir. Eğer iki görüntü arasında %85 - %90'ın üzerinde bir eşleşme varsa sistem anında alarm üretir [Mao vd., 2019]. Bu yöntem, görsel illüzyonun kullanıldığı en sofistike saldırılarda bile oltalama sayfasını deşifre eder.

Sonuç: Çok Katmanlı İstihbarat Ağı
Türkiye ve KKTC'de yaşanan dolandırıcılık vakaları açıkça göstermektedir ki; gerçek ve yıkıcı tehditleri kurbanlara ulaşmadan engellemek isteyen kurumlar, dijital ayak izlerini çok daha derinlemesine izlemelidir. Sitenizin kodlarına yerleştireceğiniz bir Canary ile ilk alarmı almak, Shodan ve Censys gibi araçlarla internetin karanlık sokaklarında periyodik devriyeler atmak ve Görsel Benzerlik teknolojileriyle yapay zekanın gücünü arkanıza almak... Bu üçlü strateji, saldırganları kendi silahlarıyla vuran güçlü ve proaktif bir siber tehdit istihbaratı kalkanı oluşturacaktır.

Kaynakça
Anti-Phishing Working Group (APWG) Q1 Report. (2026). Phishing activity trends report. https://docs.apwg.org/reports/apwg_trends_report_q1_2026.pdf

Bazzell, M. (2024). Open source intelligence techniques: Resources for searching and analyzing online information (11. Baskı). IntelTechniques. https://inteltechniques.com/books/?utm_source=chatgpt.com

BGA Security. (2019). Oltacının Peşine Düşmek. https://www.bgasecurity.com/2019/09/oltacinin-pesine-dusmek/

Kıbrıs Postası. (2024, 16 Temmuz). Kıb-Tek'ten uyarı: Sahte internet sitelerine karşı dikkatli olun, ödeme adreslerinizi kontrol edin. https://www.kibrispostasi.com/c35-KIBRIS_HABERLERI/n526160-kibtekten-uyari-sahte-internet-sitelerine-karsi-dikkatli-olun-odeme-adreslerinizi-kontrol-edin

Mao, J., Bian, J., Tian, W., Zhu, S., Wei, T. ve Li, Z. (2019). Phishing page detection via learning classifiers from page layout feature. https://link.springer.com/article/10.1186/s13638-019-1361-0

Thinkst Applied Research. (2024). Defending against the Attack of the Clone[d website]s!. https://blog.thinkst.com/2024/01/defending-against-the-attack-of-the-cloned-websites.htm

T.C. İçişleri Bakanlığı. (2025, 4 Ekim). *İstanbul merkezli 6 ilde yapılan operasyonda 900 milyon TL'lik işlem hacmi olan 12 şüpheli yakalandı*. https://www.icisleri.gov.tr/bakanimiz-sayin-ali-yerlikaya-istanbul-merkezli-6-ilde-yapilan-operasyonda-900-milyon-tllik-islem-hacmi-olan-12-supheli-yakalandi.

Kazım ATEŞ
kazimates@yahoo.com

Müsteşarlığın acil rapor taleplerine yapay zekayla cevap vermek: Bir haftada öğrendiklerimiz

Bizim işte "acil rapor" diye bir şey vardır, herkes bilir. Toplantıya bir saat kala telefon çalar, makamdan biri arar, "şu bölgede kuruma gönderilmiş ama hâlâ ilk kontrolü yapılmamış kaç başvuru var, hemen lazım" der. Siz o sırada başka bir modülün ortasındasınızdır. Bırakırsınız, SQL yazarsınız, bir iki yerde tereddüt edersiniz (kapatılmış başvurular sayılacak mı, iptal edilenler ne olacak), sayıyı gönderirsiniz. Bazen sayı yanlış çıkar çünkü soruyu soranla sizin "bekleyen" kelimesinden anladığınız aynı şey değildir. Ertesi gün aynı soru biraz farklı bir kelimeyle tekrar gelir.

Bu yazıda, bu döngüden kurtulmak için Ağustos sonunda başladığımız ve bir haftada canlıya aldığımız yapay zeka destekli sorgu asistanını anlatacağım. Sistemimiz 229 tablolu bir SQL Server veritabanı üzerinde çalışan, ASP.NET Core ile yazılmış bir başvuru ve tescil uygulaması. Asistan, personelin Türkçe yazdığı soruyu SQL'e çeviriyor, sorguyu ekranda gösteriyor, kullanıcı onaylarsa çalıştırıyor ve sonucu ya tablo ya da tek bir cümle olarak veriyor. Hepsi bu. Anlatacağım şeylerin çoğu mimari kararlardan çok, yolda yaptığımız hatalar ve onlardan çıkardığımız sonuçlar.

Başlangıçta ne yapmamaya karar verdik

İlk gün tasarım dokümanını yazarken sınırları epey dar tuttuk. Sistem yalnızca okuyacak; veri değiştiren bir sorgu üretilse bile çalıştırılamayacak. Kullanıcı üretilen SQL'i görmeden hiçbir şey çalışmayacak. Grafik falan yok, sonuç ya tablodur ya cümledir.

Bir de şuna karar verdik: embedding, vektör veritabanı, RAG altyapısı kurmayacağız. Bunu yazınca birkaç arkadaştan "nasıl yani, o zaman yapay zeka projesi olmuyor ki" tepkisi aldım. Ama 229 tablonun adı ve birer satırlık açıklaması 15 bin karakterden az tutuyor. Bu metni her soruda modele düz olarak göndermek, sağlayıcının prompt önbelleği sayesinde neredeyse bedava. Vektör aramayla bulacağımız şey bundan daha iyi olmayacaktı, sadece daha karmaşık olacaktı.

İlk mimari ve neden iki gün dayandı

İlk sürüm iki model çağrısıyla çalışıyordu. Birincisinde ucuz bir modele bütün tablo kataloğunu verip "bu soru için hangi tablolar lazım" diye soruyorduk, üç beş tablo adı dönüyordu. İkincisinde daha iyi bir modele yalnızca o tabloların kolonlarını ve ilişkilerini veriyor, SQL'i istiyorduk.

Kolon bilgisini bir yere elle yazmadık, INFORMATION_SCHEMA'dan canlı okuduk. Bunun avantajı şu: şemaya yeni kolon eklendiğinde asistan onu hemen görüyor, kimse bir şey güncellemek zorunda kalmıyor. Kolon adlarımız zaten uzun ve Türkçe olduğu için (PasaportGecerlilikTarih gibi) çoğu kolonun ne olduğu adından belli.
Ufak bir numara daha yaptık: modelden SQL'in yanında cevabın nasıl sunulacağını da istedik. Sonuç tek bir sayı mı yoksa liste mi, tek sayıysa cümle kalıbı ne. Böylece sonucu Türkçeye çevirmek için üçüncü bir çağrıya gerek kalmadı.

Sistem ilk gün çalıştı ve ilk soruya doğru cevap verdi. İkinci soruya yanlış cevap verdi. Sonraki iki gün büyük ölçüde yanlış cevapları anlamakla geçti.

Yanlış cevapların ortak noktası

Bir süre sonra hataların hepsinin aynı kalıptan çıktığını fark ettik: model bilmediği bir şeyi varsayıyordu.
Mesela bir kurumun onayını bekleyen başvuruları sorduk. Model OnayDurum = 'Beklemede' yazdı. Gayet mantıklı görünüyor, öyle bir değer olsa doğru olurdu. Ama o kolon yalnızca Evet ve Hayır alıyor, bekleyenlerde NULL. Yaklaşık 978 bin kayıtta NULL. Sorgu sıfır döndü.
Başka bir seferinde ara bağ tablosu birinci aşamada seçilmedi, model o tablonun kolonlarını kafasından uydurdu, çalışmayan bir SQL üretti. Bir başkasında adı çok anlamlı ama gerçekte yüzde iki dolu bir kolona güvendi.

Her hatayı tek tek düzelttik. Veritabanına bakıp gerçek değerleri saydık, bulduğumuzu bir talimat olarak yazdık: "OnayDurum kolonunda Beklemede diye bir değer yoktur." Üçüncü günün sonunda yirmiden fazla talimat vardı ve hâlâ yeni hatalar geliyordu. O akşam şunu konuştuk: biz burada modelin yapabileceği bir işi elle yapıyoruz. "Bu kolon hangi değerleri alıyor" sorusunu veritabanına biz soruyoruz, cevabı alıp modele taşıyoruz. Model bunu kendisi sorabilir.

Modele veritabanına bakma izni vermek

Ertesi gün mimariyi değiştirdik. Tek seferde SQL isteyen yapı gitti, yerine modelin araç çağırarak ilerlediği bir döngü geldi. Model sorguyu yazmadan önce beş şey yapabiliyor:
Bir tablonun şemasını isteyebiliyor; kolonlar, tipler, yabancı anahtarlar ve o tabloya bizim elle yazdığımız açıklamalar geliyor. Bir kolonun gerçekte hangi değerleri aldığını saydırabiliyor; her değerin kaç kayıtta geçtiği ve NULL sayısı geliyor. Yazdığı sorguyu çalıştırmadan derletebiliyor; kolon adı yanlışsa daha cevabı sunmadan öğreniyor. Sorgunun kaç satır döndüreceğini sorabiliyor; sıfır dönüyorsa koşullardan biri veriyle uyuşmuyor demektir, dönüp tekrar bakıyor. Son olarak nihai sorguyu, cevap tipini, cümle kalıbını ve hangi kurum kurallarını uyguladığını teslim ediyor.

Bütün bu araçlar salt okunur. Model kataloğumuzda kapalı olan bir tabloya ulaşamıyor, tablo ve kolon adları INFORMATION_SCHEMA'dan doğrulanıyor.

Döngüye 14 tur ve 32 araç çağrısı sınırı koyduk. Başta 10 turdu, çok adımlı bir soruda yetmedi, yükselttik. Canlıdaki ortalama 5,5 tur çıktı, en uzun soru 10 turda bitti, sınıra hiç gelinmedi. Maliyet tabii arttı: soru başına ortalama 136 bin token harcanıyor. Ama bunun yüzde 88'i önbellekten geldiği için soru başına altı sent civarında bir maliyet çıkıyor. O gün "token artsın, doğru mimari olsun" dedik ve pişman olmadık.

Döngüyü çalıştırırken üç şey öğrendik ki bunları baştan bilseydik iyi olurdu.

Birincisi, model doğruladığı sorguyu sunmayabiliyor. Bir denemede model bir taslağı satır saydırarak ölçtü, sonra teslim ederken başka bir sorgu verdi. Doğrulama boşa gitmişti. Şimdi teslim edilen sorguyu biz kendi tarafımızda tekrar denetliyoruz, geçmezse döngü devam ediyor.
İkincisi, tur hakkı dolarken modelin elinde hiçbir şey olmadan kalmaması gerekiyor. Son üç tur kala "araştırmayı bırak, elindekiyle en iyi sorguyu ver" diyoruz. Yine de bitiremezse, son başarıyla derlenen taslağı bir uyarıyla kullanıcıya gösteriyoruz. Hiç cevap vermemektense kullanıcının görüp karar vereceği bir taslak vermek daha iyi geldi bize.

Üçüncüsü, kurum kurallarının prompt'ta nerede durduğu önemli. Başta kuralları katalogla örnekler arasına koymuştuk, model bazılarını görmezden geliyordu. En sona, ayrı bir blok olarak taşıdık ve modelden hangi kuralları uyguladığını numarasıyla bildirmesini istedik. Uygulanma oranı gözle görülür şekilde arttı. Bu bildirimi ekranda kullanıcıya da gösteriyoruz, hangi kuralın gerçekten işe yaradığını zamanla anlayacağız.

Veriye bakarak öğrenilemeyen şeyler

Araçlar "bu kolon ne alıyor" sorusunu çözdü. Ama bazı şeyler veride görünmüyor, kurumun kendi iş bilgisi. Bunları talimat olarak yazmak zorundaydık, bugün 34 tane aktif kural var. Birkaçını yazayım, ne demek istediğim anlaşılsın.

Süreç tablosunda aynı başvuru için aynı işlemden birden fazla kayıt olabiliyor. Baktık, bir başvuruda 111 tane var. Hangisi geçerli? En güncel olan. İlkini alan sorgu yanlış sayıyor.
Kontrol adımında "Hayır" başvuruyu bitirmiyor. Başvuru düzeltilip aynı adıma geri dönüyor. Dolayısıyla "bekleyen" derken Evet olmayanların hepsini almak gerekiyor. NULL ise o adım hiç olmamış demek, sayıma girmiyor.

"Kurum ekranlarında" demek süreç adımının kurum tarafında olması demek değil. Vatandaşa açık sanal birimde bekleyen başvurular süreç açısından kurum adımında görünüyor ama aslında kurumun önünde değil. Bunu 499 başvurudan 82'sinin yanlış sayıldığını görünce anladık.

Ülke tablosunda 13 ülkenin iki satırı var. Ukrayna iki ayrı anahtarla duruyor. Tek anahtara göre filtre yazan sorgu eksik sayıyor.
Bu kuralların hiçbirini masa başında düşünüp yazmadık. Her biri bir yanlış cevaptan çıktı, veritabanında sayarak doğruladık, sonra talimat oldu.

En pahalı hatamız

Kolon açıklamalarını doldururken bir hata yaptık, anlatmaya değer. Kontrol kolonunun açıklamasına "bekleyenler için Evet olmayanlar alınır" gibi bir öneri yazdık. Kısmen doğruydu ama bağlamı eksikti. Model bu açıklamayı gördü ve sekiz sorguda aynı hatayı yaptı. Biz de bir süre modelin neden ısrarla yanlış yaptığını anlamadık, çünkü açıklamayı yazan bizdik ve doğru olduğunu düşünüyorduk.
Buradan çıkardığımız ders: yanlış bir kolon açıklaması yanlış bir talimattan daha tehlikeli. Talimat listede duruyor, göz önünde. Açıklama ise şemayla birlikte geliyor, her sorguya sessizce giriyor, kimse fark etmiyor.

Bundan sonra kolon açıklaması için kendimize bir kural koyduk: ölçmeden yazmayacağız. Her açıklama üç şeyi söyleyecek: kolon ne anlama geliyor, ne zaman doluyor, ne için kullanılmıyor. Yazmadan önce veritabanında sayacağız, yazdıktan sonra işi bilen bir arkadaşa okutacağız.

En çok kullanılan on tablonun yüzde beşten fazla dolu bütün kolonlarını bu şekilde açıkladık. İki günde 490 açıklama. Bugün toplamda 503 açıklama ve 202 değer sözlüğü var. Sıkıcı bir işti ama sistemin doğruluğunu en çok artıran şey bu oldu, mimari değişiklik değil.
Bu işi kolaylaştırmak için iki tarayıcı yazdık. Biri kod tablolarındaki kısa metin kolonlarının gerçek değer kümesini çıkarıyor. Diğeri her kolonun doluluk yüzdesini ve farklı değer sayısını ölçüp bir profil tablosuna yazıyor. Artık şema çıktısında her kolonun yanında "yüzde 1,9 dolu, neredeyse boş" gibi bir not var. Model boş kolonlara güvenmeyi bıraktı. 1.308 kolon ölçtük, 151'i yüzde beşten az doluymuş; bunu elle asla bulamazdık.

Güvenlik tarafı

Burayı kısa geçeceğim çünkü çoğu standart şeyler, ama bir iki noktayı belirtmek istiyorum.
Veritabanında ayrı bir salt okunur kullanıcı açmadık, o yüzden savunma tamamen uygulama tarafında. Üretilen SQL denetimden geçiyor: SELECT ile başlamalı, tek ifade olmalı, yorum içermemeli, veri değiştiren anahtar kelimeler yasak, INTO yasak, sistem prosedürleri yasak. Sorgu bir transaction içinde çalışıyor ve ne olursa olsun geri alınıyor. SQL Server'da DDL de transaction içinde olduğu için denetim atlatılsa bile kalıcı bir değişiklik olamıyor.
Parola ve kart bilgisi kolonlarını iki yerde birden engelledik. Şema metnine hiç yazılmıyorlar, model varlıklarını bilmiyor. Bir şekilde SQL'de geçerlerse denetim reddediyor. Prompt'a "bunu kullanma" yazmakla yetinmedik, çünkü talimat soru diliyle dolanılabilir ama denetim dolanılamaz.
Bir de çalıştırma tarafında önemli bir karar: çalıştırma ucu istemciden SQL metni almıyor. Sadece log kaydının numarasını alıyor ve SQL'i sunucudaki kayıttan okuyor. Aksi halde kullanıcı ekrandaki SQL'i değiştirip istediğini çalıştırabilirdi. Bu yüzden şu an SQL düzenlenemiyor; kullanıcı sonucu beğenmezse soruyu yeniden ifade ediyor veya bir kural ekliyor.

Canlıdan bir örnek

"Ukrayna uyruklu aktif izin sayısı" diye sorulmuş. Beş kelime.
Modelin ürettiği ve kullanıcının onayladığı sorgu şu:

```
SELECT TOP 500 COUNT(*) AS AktifIzinSayisi
FROM dbo.BasvuruAna ba WITH (NOLOCK)
INNER JOIN dbo.BasvuruDetay bd WITH (NOLOCK) ON ba.Pkey =
bd.BasvuruAnaPkey
INNER JOIN dbo.Ulke u WITH (NOLOCK) ON bd.UlkePkey = u.Pkey
INNER JOIN dbo.BasvuruTip bt WITH (NOLOCK) ON ba.BasvuruTipPkey
= bt.Pkey
WHERE ba.KurumaGonderildimi = 'Evet'
  AND bt.IzinBasvurusumu = 'Evet'
  AND ba.Onay = 'Evet'
  AND ba.IzinBaslangicTarih IS NOT NULL
  AND ba.IzinBitisTarih IS NOT NULL
  AND ba.IzinBitisTarih >= GETDATE()
  AND (ba.KapatmaTur IS NULL OR ba.KapatmaTur <> N'İptal Edildi')
  AND u.UlkeAd LIKE N'%UKRAYNA%'
```

Soruda "aktif" geçiyor; sorguda aktif izin tanımının dört parçası var, onaylı olması, tarihlerinin dolu olması, bitiş tarihinin geçmemiş

olması ve iptal edilmemiş olması. Bunları soran kişi yazmadı, kurum kuralından geldi. Ülkeyi anahtarla değil adla eşleştirmiş, çünkü Ukrayna'nın iki anahtarı olduğunu biliyor. TOP 500 de bizim otomatik eklediğimiz sınır. Sorgu 128 milisaniyede çalışmış.

Bir haftanın sayıları

4 Eylül itibarıyla 229 soru soruldu, 194'ü kullanıcı onayıyla çalıştırıldı, 16'sı çalıştırma sırasında hata verdi. Kullanıcılar 133 tanesini "bu doğru, bundan öğren" diye işaretledi; bunlar sonraki sorularda örnek olarak kullanılıyor. Bilgi tabanında 137 açık tablo, 503 kolon açıklaması ve 34 kurum kuralı var.

Sayılardan daha önemli bulduğum şey şu: bilgi tabanının tamamı veri. Tablo kataloğu, açıklamalar, kurallar, örnekler, profiller, hepsi tabloda duruyor. Bir haftada yaptığımız iyileştirmelerin hiçbiri derleme ya da dağıtım gerektirmedi. Yanlış bir cevap görünce ekrandan bir kural ekliyoruz, bir sonraki soruda etkisini görüyoruz.

Bir daha yaparken dikkat edeceklerimiz

Türkçe büyük I harfi bize bir öğleden sonraya mal oldu. Uygulama tr-TR kültüründe çalışıyor. Model tablo adını "Isyeri" diye yazınca ToLower büyük I'yı noktasız ı yaptı, eşleşme bozuldu. Veritabanı collation'ı da I ile i'yi ayrı saydığı için şema sorgusu boş döndü. Model şemayı göremeyince kolon adı uydurdu ve biz bir süre modelin neden birden aptallaştığını anlamadık. Tablo adlarını kültürden bağımsız karşılaştırmaya geçtik, soru metnini ise tr-TR ile küçültüyoruz. Bunu bilmeyen yoktur ama yine de yazıyorum, çünkü biz de biliyorduk ve yine yakalandık.

Kolon açıklamasını ölçmeden yazmayı yukarıda anlattım. Sekiz sorgu. Modelin doğruladığı sorguyu sunduğunu varsaymamak gerekiyor. Sunulanı her zaman yeniden denetleyin.

Kuralları prompt'un ortasına koymayın, sona koyun.

Yapılandırılmış çıktı isterken JSON modunu açın. Açmadığımızda model cevabı ara sıra kod bloğu içinde döndürüyordu ve ayrıştırma bozuluyordu.

Sırada ne var

Kalan 127 tablonun açıklamaları duruyor, kullanım sıklığına göre yavaş yavaş yapacağız. Kurum jargonu için bir terim sözlüğü düşünüyoruz; "mühür" dendiğinde onaylı ve tarihli izin anlaşılsın gibi. Soru yazarken otomatik tamamlama var sırada. Bir de salt okunur bir veritabanı kullanıcısı; tasarımı tek ayar değişikliğiyle geçilebilecek şekilde yaptık, bir gün açılınca en güçlü güvenlik katmanı eklenmiş olacak.

Ama asıl iş artık rutin: logları oku, yanlış cevabı bul, kuralı yaz, ölç, onaylat. Her hafta biraz daha az yanlış.

Bir hafta önce acil rapor demek bir geliştiriciyi işinden koparmak demekti. Şimdi soruyu soran kişi ekrana Türkçe yazıyor, sorguyu görüyor, onaylıyor, cevabını alıyor. Biz de o sırada başka bir şeyle uğraşıyoruz. Bu yazıdan tek bir şey kalacaksa şu olsun: modelin SQL bilgisiyle ilgili bir sorunumuz hiç olmadı. Bütün sorun modelin bizim verimizi tanımamasıydı, ve bunun çözümü daha iyi bir model değil, modele veriye bakma imkânı vermek ve kendi iş bilgimizi dürüstçe yazmaktı.

Erkan Coşkun
Bilgisayar Yüksek Mühendisi

Üniversite öğrencilerinin üçte biri AI yüzünden bölüm değiştirmeyi düşünüyor.

Yapay zekânın iş dünyasında dengeleri hızla değiştirmesi, üniversiteleri öğrencilerini de kariyer planlarını yeniden değerlendirmeye itiyor. İşte dikkat çeken araştırmanın sonuçları. - Kaynak: donanimhaber.com

İş dünyasında daha şimdiden etkilerini hissettirmeyi başlayan yapay zekâ devrimi, önümüzdeki yıllarda pek çok sektörde iş imkânlarının hızla ortadan kalkmasına sebep olacak. Personel tarafındaki bu daralma neredeyse kaçınılmaz görünüyor. Bu durum artık sadece iş dünyasındaki insanları değil, yakın bir gelecekte iş dünyasına atılacak üniversite öğrencilerini de kaygılandırıyor. Nitekim ABD'de yayımlanan yeni bir araştırma, pek çok üniversite öğrencisinin AI yüzünden tercihlerini sorgulamaya başladığını gösteriyor.

Öğrenciler, Kariyer Planlarını Değiştirmek Zorunda Kalıyor

CNBC öncülüğünde geçtiğimiz ay ABD'de gerçekleştirilen araştırmaya göre, üniversite öğrencilerinin neredeyse üçte biri (%31), yapay zekâ yüzünden bölümlerini ya da kariyer planlarını değiştirmeyi düşünüyor. Eskiden atılmayı düşündüğü sektörde AI yüzünden iş bulamayacağından endişe duyan öğrenciler, gelecek planlarını buna göre revize etmeyi değerlendiriyor.

Araştırmaya katılan üniversite öğrencilerinin yüzde 34'ü yapay zekâ alanında yaşanan gelişmeler yüzünden işe girmeyi düşündükleri şirketlerin değiştiğini söylüyor. AI yüzünden farklı yetenekler kazanmaya çalıştıklarını söyleyen öğrencilerin oranı ise yüzde 45.

Son dönemde farklı araştırma şirketleri ve medya kuruluşları tarafından yayımlanan anketler de aynı sonucu veriyor. Dünyanın dört bir yanında öğrenciler, yapay zekânın iş dünyasındaki etkilerinden kaçabilmek için farklı alanlara yöneliyor.

SEÇİMLERİN GÖRÜNMEYEN MÜHENDİSLERİ

Yapay zekâ, algoritmalar ve seçim güvenliği

Seçim günü sandığa giden iki seçmen, seçimden önce dijital dünyada tamamen farklı gündemlerle karşılaşmış olabilir. Birinin ekranında ekonomi krizi ve hayat pahalılığı öne çıkarken, diğerinin ekranında güvenlik veya dış politika öne çıkabilir. Biri bir adayın hatalarını tekrar tekrar görürken, diğeri aynı adayın başarılarına daha sık maruz kalabilir. Her ikisi de yalnızca "internete baktığını" düşünür; ancak karşılarına çıkan içeriklerin sırası, görünürlüğü ve tekrar sayısı büyük ölçüde algoritmalar tarafından belirlenir.

Asıl mesele: Algoritma oy kullanmaz, ama seçmenin gördüğü dünyayı seçebilir

Seçim güvenliğini yalnızca sandık, mühür ve oy sayımı üzerinden düşünmek artık yeterli değil. Dijital platformlar, seçmenin hangi haberi önce göreceğini, hangi videonun tekrar tekrar önüne düşeceğini ve hangi siyasi mesajın hiç karşısına çıkmayacağını belirleyen bir "görünürlük katmanı" oluşturuyor. Bu katman doğrudan "şu adaya oy ver" demek zorunda değil. Gündemi değiştirerek, bir konuyu olduğundan büyük göstererek, bir başka konuyu görünmez hâle getirerek veya seçmenin güven duygusunu aşındırarak siyasi davranış üzerinde dolaylı etki kurabilir.

Burada önemli bir bilimsel ayrım var: Algoritmaların ne gördüğümüzü değiştirdiğine ilişkin güçlü kanıt bulunuyor. Buna karşılık tek bir algoritmik müdahalenin bir ulusal seçimin sonucunu tek başına değiştirdiğini kanıtlamak çok daha zor. Büyük saha deneyleri, ortalama oy ve katılım etkisinin çoğu zaman küçük, değişken veya ölçülmesi zor olduğunu gösteriyor. [4][5][6][7] Yani "algoritmalar etkisizdir" demek de, "algoritmalar seçimleri uzaktan kumanda eder" demek de gerçeği fazla basitleştirir.

Şekil 1. Dijital etkinin basit zinciri: veri toplanır, profil çıkarılır, içerik seçilir, tepkiniz yeni veri üretir ve döngü tekrar başlar.

Bu döngü günlük hayatta nasıl işler?

Örneğin bir kullanıcı ekonomik haberleri uzun süre izliyor, kira ve fiyat artışlarıyla ilgili içeriklere tıklıyor ve benzer videoları sonuna kadar seyrediyorsa platform bunu bir "ilgi sinyali" olarak görür. Sistem kullanıcının siyasi görüşünü kesin olarak bilmek zorunda değildir; sadece hangi içeriğin onu ekranda tutacağını tahmin etmeye çalışır. Zamanla kullanıcıya aynı temayı güçlendiren daha fazla içerik gösterilebilir. Böylece algoritma bir kanaati sıfırdan yaratmasa bile, hangi meselenin "ülkenin en büyük sorunu" gibi hissedileceğini etkileyebilir. **Kritik nokta: Dijital manipülasyonun en güçlü yanı çoğu zaman insanın fikrini bir anda değiştirmek değil; dikkatini, gündemini ve güven duygusunu sürekli aynı yöne itebilmektir.**

Temsili görsel: Cambridge Analytica ve Facebook veri skandalının dijital siyasi profilleme boyutu.

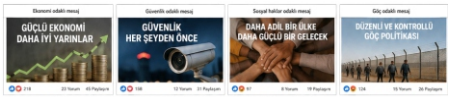
Cambridge Analytica bize ne öğretti?

2018'de ortaya çıkan Cambridge Analytica skandalı, dijital siyasi hedeflemenin ne kadar ileri gidebileceğini kamuoyuna gösteren dönüm noktalarından biri oldu. Facebook, "This Is Your Digital Life" adlı uygulama üzerinden 87 milyona kadar kullanıcının verisinin uygunsuz biçimde paylaşılmış olabileceğini açıkladı. [1] Birleşik Krallık Bilgi Komiserliği ve ABD Federal Ticaret Komisyonu, veri toplama ve profilleme süreçlerindeki ciddi ihlalleri belgeledi. [2][3]

Fakat burada sık yapılan bir hata var: "87 milyon kişinin verisi kullanıldı" cümlesi, "87 milyon kişinin oyu değiştirildi" anlamına gelmez. Skandal, büyük ölçekli veri suistimalini ve seçmenleri ayrıntılı biçimde sınıflandırma kapasitesini gösterdi; 2016 ABD başkanlık seçimindeki sonucun ne kadarının bu faaliyetler nedeniyle değiştiğini nedensel olarak hesaplayan güvenilir bir kanıt ise yok. Bu ayrımı korumak önemli, çünkü aksi hâlde gerçek riskleri anlamak yerine teknolojiye neredeyse sihirli bir güç atfetmiş oluruz.

Mikro-hedefleme: Aynı aday, farklı seçmenlere farklı yüzler.

Klasik bir televizyon reklamını herkes görür. Rakip parti de, gazeteci de, seçmen de mesajı inceleyebilir. Mikro-hedeflemede



Şekil 2. Mikro-hedefleme örneği: Aynı kampanya farklı seçmen gruplarına farklı mesajlar gösterebilir.
Temsili görsel: Aynı kampanyanın farklı seçmen gruplarına farklı siyasi mesajlar sunabilmesi

ise aynı kampanya farklı gruplara farklı mesajlar gösterebilir. Bir seçmene ekonomi, diğerine göç, bir başkasına güvenlik veya sosyal haklar öne çıkarılabilir. Sorun yalnızca kişiselleştirme değildir; kamusal denetimin zayıflamasıdır. Seçmen A'nın gördüğü mesajı seçmen B hiç görmeyebilir, dolayısıyla bir kampanyanın farklı kitlelere birbiriyle çelişen vaatler verip vermediğini takip etmek zorlaşır.

2025'te yayımlanan deneysel bir çalışma, kişilik özellikleriyle eşleşen siyasi reklamların eşleşmeyen reklamlara göre daha ikna edici algılanabildiğini gösterdi. [8] Ancak gerçek seçim davranışını ölçen saha deneyleri daha temkinli sonuçlar veriyor. Florida'daki büyük bir Facebook/Instagram deneyinde 1,1 milyondan fazla reklam gösterimine rağmen tahmin edilen oy etkisi son derece küçüktü. [4] 2020 ABD seçiminde yaklaşık 2 milyon "ikna edilebilir" seçmeni kapsayan başka bir çalışma da ortalama katılım üzerinde belirgin bir etki bulmadı. [5] Bu nedenle mikro-hedefleme için en doğru ifade şudur: güçlü bir kapasitedir, fakat her kullanıldığında büyük bir oy kayması yarattığı gösterilmiş değildir.

Yankı fanusu: Algoritma mı bizi kapatıyor, biz mi kendimizi?

Temsili görsel: Kullanıcı etkileşimleriyle benzer içeriklerin tekrar tekrar öne çıkması.

Yankı fanusu, kişinin çoğunlukla kendi görüşüne benzeyen içeriklerle karşılaşmasıdır. Burada algoritma önemli bir rol oynayabilir; fakat tek aktör değildir. Arkadaş çevresi, takip edilen hesaplar, parti kimliği, haber tercihleri ve kullanıcının kendi tıklama davranışı da bu ortamı oluşturur. 2023'te Nature'da yayımlanan büyük Facebook çalışmasında, kullanıcılara gösterilen benzer görüşlü içerik yaklaşık üçte bir azaltıldı. Karşıt görüşlü içerik arttı, ancak kutuplaşma ve aday değerlendirmelerinde anlamlı bir ortalama değişim bulunmadı. [6] Bu sonuç bize şunu söylüyor: Algoritmalar bilgi ortamını biçimlendirir, ama toplumsal kutuplaşma tek bir düğmeye basarak çözülecek kadar basit değildir.

Yankı fanusunun bir adım ötesinde ise modern video platformlarında tartışılan algoritmik "tavşan deliği" (rabbit hole) etkisi bulunuyor. Yankı fanusu kullanıcının zaten yakın olduğu görüşleri tekrar tekrar karşısına çıkarırken, tavşan deliği etkisinde öneriler giderek daha dar, benzer veya bazı durumlarda daha uç içeriklere doğru ilerleyebilir. Örneğin sıradan bir ekonomik eleştiri videosuyla başlayan izleme zinciri, kullanıcının izleme süresi ve etkileşimlerine göre komplo teorileri ya da doğrulanmamış iddialarla devam edebilir. TikTok üzerine yapılan algoritma denetimleri, kullanıcı davranışlarının önerileri hızla kişiselleştirebildiğini ve yanlış bilgiyle etkileşimin aynı veya başka konulardaki benzer içeriklere açılan bir kapı hâline gelebildiğini gösteriyor. Ancak bu, algoritmanın her kullanıcıyı otomatik olarak radikalleştirdiği anlamına gelmiyor. Seçim güvenliği açısından asıl risk, tartışmalı veya yanlış içeriklerin kısa süre içinde art arda gösterilebilmesi ve bu hızın, doğrulama mekanizmalarından önce güçlü bir ilk izlenim oluşturabilmesidir. [20]

Deepfake: Tehlike sadece sahte videoya inanmak değil

BTKıbrıs'ın Ağustos sayısında deepfake teknolojisinin teknik yapısı ve doğrulama yöntemleri ayrıntılı biçimde ele alınmıştı. Burada ise aynı tehdidin seçim güvenliği açısından ortaya çıkardığı ikinci probleme odaklanıyorum: yalnızca sahteye inanmak değil, gerçeğe de artık inanamamak.

Deepfake denildiğinde akla genellikle "sahte videoya kanan seçmen" gelir. Oysa daha büyük sorun, gerçek ile sahte arasındaki sınırın bulanıklaşmasıdır. 2024 New Hampshire ön seçimi öncesinde Joe Biden'ın yapay zekâ ile klonlanmış sesini kullanan bir robocall, seçmenlere ön seçimde oy kullanmamalarını söyledi. ABD Federal İletişim Komisyonu olayın arkasındaki kişiye 6 milyon dolar ceza verdi. [9] Burada mesele yalnızca bir ses kaydının sahte olması değildir; sahte içerik, seçmenin doğru seçim prosedürüne güvenini de hedef almıştır.

Bir başka risk "liar's dividend" yani "yalancının temettüsü" olarak adlandırılır. Deepfake'ler yaygınlaştıkça gerçek bir ses kaydı veya video da "Bu zaten yapay zekâ ile yapılmış" denilerek reddedilebilir. Deneysel araştırmalar, politikacıların gerçek skandalları "deepfake" veya "yanlış bilgi" diye etiketleyerek bazı koşullarda hesap verme baskısını azaltabildiğini gösteriyor. [14] Dolayısıyla sentetik medyanın tehlikesi yalnızca sahte kanıt üretmek değil, gerçek kanıtın değerini de düşürmektir.

Peki bu tablo KKTC'de neden özellikle önemli?

KKTC'nin ölçeği, dijital etki tartışmasını ilginç hâle getiriyor. Küçük bir seçmen havuzunda birkaç bin oy, çok yakın yarışlarda büyük siyasi anlam taşıyabilir. Ancak bu cümle "KKTC seçmeni kolay manipüle edilir" demek değildir. Tam tersine, yerel medya kültürü, yüz yüze siyasi ilişkiler, aile ve topluluk bağları dijital etkileri sınırlayabilir veya değiştirebilir. Burada yapılabilecek en sağlıklı şey, kesin sonuçlar ilan etmek yerine hangi bilgi alanlarının daha hassas olduğunu belirlemektir.

Şekil: 2020 ve 2025 KKTC Cumhurbaşkanlığı seçimlerinde oy farkının karşılaştırılması.

2020 ve 2025 bize iki farklı ders veriyor

2020 Cumhurbaşkanlığı seçiminin ikinci turunda 130.232 geçerli oy kullanıldı. Ersin Tatar 67.322, Mustafa Akıncı 62.910 oy aldı; fark yalnızca 4.412 oydu. [15] Bu, geçerli oyların yaklaşık %3,39'una karşılık geliyor. Yakın bir seçimde küçük davranış değişikliklerinin siyasi ağırlık kazanabileceği açıktır. Fakat bu matematik, ABD'de ölçülen herhangi bir dijital etkinin KKTC'ye aynen taşınabileceği anlamına gelmez.

2025 Cumhurbaşkanlığı seçimi ise ters yönde bir örnek sundu. YSK'ya göre 218.313 kayıtlı seçmenden 141.504'ü sandığa gitti; Tufan Erhürman 87.137 oyla %62,76, Ersin Tatar 49.714 oyla %35,81 aldı. [18] Aradaki yaklaşık 37 bin oyluk fark, küçük bir dijital etkinin tek başına seçim sonucunu açıklayamayacağı kadar büyüktü. Reuters da yarışı Kıbrıs sorunu konusunda federal çözüm ile iki devletli yaklaşım arasındaki belirgin siyasi ayrışma bağlamında değerlendirdi. [17] Bu iki seçim birlikte okunduğunda daha gerçekçi soru ortaya çıkıyor: "Algoritma seçimi değiştirir mi?" değil, "Seçim zaten yakınsa ve bilgi ortamı bozulursa, bunun önemi ne kadar artar?"

2020: fark 4.412 oy. 2025: fark yaklaşık 37.423 oy. Aynı dijital etkinin her seçimde aynı siyasi ağırlığı taşıması mümkün değildir; yarışın yakınlığı belirleyicidir.

KKTC'de hangi başlıklar bilgi manipülasyonuna daha açık olabilir?

Birinci alan Kıbrıs meselesidir. Federal çözüm, iki devletli yaklaşım, egemenlik, tanınma ve güvenlik gibi konular yalnızca teknik politika başlıkları değildir; kimlik ve gelecek duygusuyla ilişkilidir. Bu nedenle bir adayın ağzından üretilmiş sahte bir açıklama veya bağlamından koparılmış kısa video, gerçek bir politika tartışmasından çok daha hızlı duygusal tepki yaratabilir. Bu, herhangi bir siyasi görüşün "yanlış" olduğu anlamına gelmez. Risk, meşru siyasi ayrışmanın sahte içerikle kirletilmesidir.

İkinci alan Türkiye ile ilişkilerdir. Ekonomik destek, dış politika, güvenlik ve yerel irade tartışmaları güçlü sembolik anlam taşır. Sahte bir belge, taklit haber sitesi veya sentetik ses kaydı "gizli talimat", "anlaşma" ya da "son dakika açıklaması" görüntüsü verirse, haber doğrulanana kadar önemli bir güven krizi oluşturabilir.

Üçüncü alan ekonomidir. KKTC İstatistik Kurumu'na göre Temmuz 2026'da tüketici fiyatları yıllık bazda %38,10 arttı. [16] Maaş, kira, market, elektrik ve akaryakıt gibi doğrudan cebe dokunan konular zaten yüksek hassasiyete sahip. Böyle bir ortamda yanlış fiyat listeleri, uydurma zam kararları veya eski bir ekonomik verinin "bugün açıklanmış" gibi sunulması, siyasi söylemi kısa sürede etkileyebilir.

Dördüncü alan ise seçim prosedürüdür. "Sandık yeri değişti", "oy verme saati erkene alındı", "kimliğin geçersiz", "sonuç zaten belli" gibi yanlış bilgiler bir kişiyi başka adaya ikna etmeye çalışmaz; doğrudan sandığa gitme isteğini veya imkânını hedefler. New Hampshire örneği bu nedenle önemlidir: yapay zekâ, ikna kadar katılımı bastırmak için de kullanılabilir. [9]

Bir dijital manipülasyon dalgası pratikte nasıl görünür?

Bunu operasyon tarifi vermeden, savunma açısından düşünelim. Seçime iki gün kala bir adayın gerçek sesine benzeyen bir kayıt

yayılıyor. Aynı saatlerde yeni açılmış çok sayıda hesap bu kaydı paylaşıyor. Bazı taklit haber siteleri kaydı "son dakika" etiketiyle haberleştiriyor. Platform algoritmaları yüksek etkileşim nedeniyle içeriği daha fazla kullanıcıya gösteriyor. Haber merkezleri doğrulama yapmaya çalışırken gündem adayın politikalarından kaydın gerçek olup olmadığı tartışmasına kayıyor. Kayıt birkaç saat sonra sahte çıksa bile ilk etki tamamen geri alınamayabilir.

Burada yapay zekânın rolü tek başına "video üretmek" değildir. Sentetik içerik üretimini ucuzlatır; farklı biçimlerde yüzlerce versiyon hazırlanmasını kolaylaştırır; otomatik hesaplarla dağıtımı hızlandırabilir; aynı anlatının farklı kullanıcı gruplarına farklı tonlarda sunulmasına yardımcı olabilir. Ancak bunların hiçbiri seçmenin zihnini kontrol eden sihirli bir mekanizma değildir. Etki, içerik ne kadar inandırıcı, gündem ne kadar hassas, seçim ne kadar yakın ve güvenilir doğrulama ne kadar hızlı sorularına bağlıdır.

Hız: Sahte içerik birkaç dakika içinde üretilebilir;

KKTC DİJİTAL SEÇİM RİSK MATRİSİ

Risk	Olasılık	Etki	Tespit	Not
Kriz anında sentetik ses/video	Orta	Yüksek	Zor	Doğrulama gecikmesi gündemi
Sahte yerel haber / taklit site	Yüksek	Yüksek	Orta-Zor	Yerel marka güvenini ödünç alır
Koordineli anonim hesap ağı	Yüksek	Orta	Orta	Sahte toplumsal çoğunluk hissi
Şeffaf olmayan mikro-hedefli reklam	Orta	Orta-Yüksek	Zor	Çelişkili mesajlar görünmez kalabilir
Öneri sistemlerinin organik amplifikasyonu	Yüksek	Orta	Zor	Niyat olmasa bile öfke/yanlış içeriği
"Bu deepfake" diyerek gerçeği reddetme	Orta	Yüksek	Zor	Gerçek kanıtın güvenilirliğini

Şekil 2. KKTC için savunmacı risk matrisi. Dereceler gerçekleşmiş yerel olay sıklıkları değil, açık kaynak bulgular ve ülke ölçeği üzerinden yapılan risk projeksiyonudur.

doğrulama ise çoğu zaman daha uzun sürer. Seçim arifesinde bu zaman farkı kritik hâle gelir.

Görünmezlik: Mikro-hedefli reklam veya kapalı mesaj gruplarında farklı seçmenlerin hangi mesajı gördüğünü kamuoyu takip edemeyebilir.

Belirsizlik: İçerik sahte olduğu kanıtlansa bile "Acaba birazı gerçek miydi?" sorusu kalabilir; tersine gerçek içerik de "AI üretimi" denilerek reddedilebilir.

Buna karşı ne yapılabilir?

Çözüm daha fazla sansür kurmak değil,

DEMOKRATİK DAYANIKLILIK: 7 KALKAN

Şekil: Seçim bilgi ortamını güçlendirebilecek temel demokratik dayanıklılık önlemleri.

doğrul anab ilir bilgiyi daha hızlı ve görünür hâle getirmektir. Yüksek Seçim Kurulu; sandık yeri, oy verme saati, aday listesi ve resmi sonuçlar için mobil uyumlu tek bir doğrulama noktası sunmalı. Seçim prosedürüyle ilgili sahte bilgi yayıldığında, kurumun cevabı saatler sonra değil mümkün olduğunca hızlı gelmeli.

Müdahale siyasi görüşlere değil, doğrulanabilir seçim prosedürüne odaklanmalıdır.

Siyasi reklamlar için şeffaflık da kritik. Bir reklamın kim tarafından finanse edildiği, ne zaman yayımlandığı, yaklaşık ne kadar harcama yapıldığı ve hangi geniş kitlelere gösterildiği kamuya açık bir arşivde görülebilirse, mikro-hedeflemenin "görünmezlik avantajı" azalır. Medya kuruluşları ise bir ses veya videoyu yalnızca "deepfake tespit aracı %92 sahte dedi" diye yayımlamamalı; ilk kaynağı, yayın zamanını, resmi hesapları, bağımsız ikinci kanalı ve mümkünse içerik kökeni kayıtlarını birlikte kontrol etmeli. BTKıbrıs'ın Eylül 2026 deepfake yazısında da vurgulandığı gibi, kaynak ve bağlam doğrulaması tek bir otomatik dedektörden daha güvenilir bir başlangıçtır. [19]

Seçim güvenliğinin yeni tanımı

Dijital çağda seçim güvenliği iki ayrı soruya cevap vermek zorunda. Birincisi geleneksel ve vazgeçilmez soru: "Oylar doğru kullanıldı ve doğru sayıldı mı?" İkincisi ise giderek daha önemli hâle geliyor: "Seçmen sandığa giderken karşısına çıkan bilgi ortamı ne kadar şeffaf, doğrulanabilir ve manipülasyona dayanıklıydı?"

Bugünkü bilimsel kanıt, algoritmaların insanları uzaktan kumanda ettiği fikrini desteklemiyor. Büyük saha deneylerinde ortalama siyasal etkiler çoğu zaman sınırlı. [4][6][7] Fakat bu, riski önemsiz yapmıyor. Seçimler "ortalama kullanıcı" üzerinden değil, gerçek oy farkları üzerinden kazanılıyor. Üstelik bilgi operasyonlarının hedefi her zaman bir seçmenin A adayından B adayına geçmesi değildir. Bazen amaç gündemi değiştirmek, seçmeni sandığa gitmekten vazgeçirmek, rakibin güvenilirliğini aşındırmak veya toplumun neyin gerçek olduğu konusunda anlaşmasını zorlaştırmaktır.

KKTC açısından en önemli ders tam da burada yatıyor. 2020'deki 4.412 oyluk fark, yakın bir yarışta küçük değişimlerin neden önem kazanabileceğini gösteriyor. 2025'teki çok daha geniş fark ise her seçim sonucunu "algoritmalar yaptı" diye açıklamanın ne kadar hatalı olacağını hatırlatıyor. Teknoloji ne her şeye kadirdir ne de masumdur. Asıl gücü, milyonlarca küçük görünürlük kararını sessizce ve sürekli verebilmesidir.

Bu nedenle geleceğin seçmeni için en önemli dijital refleks karmaşık değildir: Bir içerik sizi çok öfkelendiriyor, çok korkutuyor veya "hemen paylaşmalıyım" hissi veriyorsa birkaç saniye durun. Kaynağı bulun. Tarihe bakın. Resmi veya bağımsız ikinci bir kanaldan doğrulayın. Özellikle seçim günü ve seçimden hemen önce, hız yerine doğruluğu seçmek küçük ama güçlü bir demokratik savunmadır.

Son soru artık yalnızca "Oyumu kim saydı?" olmayacak. "Oyu kullanmadan önce gördüğüm dünyayı kim seçti?" sorusu da seçim güvenliğinin merkezine yerleşecek.

KAYNAKÇA

1\. Meta (2018), "An Update on Our Plans to Restrict Data Access on Facebook". https://about.fb.com/news/2018/04/restricting-data-access/
2\. UK Information Commissioner's Office (2018), Investigation into the use of data analytics in political campaigns. https://ico.org.uk/media2/migrated/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf
3\. U.S. Federal Trade Commission (2019), Cambridge Analytica, LLC - administrative case materials. https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3107-cambridge-analytica-llc-matter
4\. Coppock, Green & Porter (2022), large-scale Facebook/Instagram political advertising field experiment, Research & Politics. https://doi.org/10.1177/20531680221076901
5\. Aggarwal et al. (2023), political advertising and turnout experiment during the 2020 U.S. election, Nature Human Behaviour. https://doi.org/10.1038/s41562-022-01487-4
6\. Nyhan et al. (2023), like-minded content reduction experiment on Facebook, Nature 620. https://doi.org/10.1038/s41586-023-06297-w
7\. Allcott et al. (2026), experiment restricting political ads on Facebook and Instagram, Nature Human Behaviour. https://doi.org/10.1038/s41562-025-02328-w
8\. Carrella et al. (2025), personality-matched political microtargeting experiments, Communications Psychology. https://doi.org/10.1038/s44271-025-00188-8
9\. U.S. FCC (26 Sep 2024), $6 million penalty in the AI-cloned Biden robocall case. https://docs.fcc.gov/public/attachments/DOC-405811A1.pdf
10\. Reuters (22 Apr 2024), deepfake videos of Indian film stars during the 2024 election. https://www.reuters.com/world/india/deepfakes-bollywood-stars-spark-worries-ai-meddling-india-election-2024-04-22/
11\. Microsoft Threat Analysis Center (17 Apr 2024), U.S.-focused influence operations assessment. https://blogs.microsoft.com/on-the-issues/2024/04/17/russia-us-election-interference-deepfakes-ai/
12\. Pew Research Center (18 Nov 2024), America's News Influencers. https://www.pewresearch.org/journalism/2024/11/18/americas-news-influencers/
13\. Freedom House (2024), Freedom on the Net 2024. https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online
14\. Schiff, Schiff & Bueno (2024), research on politicians dismissing real scandals as deepfakes/misinformation, APSR. https://doi.org/10.1017/S0003055423001454
15\. KKTC 2020 Cumhurbaşkanlığı Seçimi, 2. tur resmi sonuç dökümü. https://ysk.gov.ct.tr/2025/03/06/11-ekim-2020-cumhurbaskanligi-secimi-2-tur-secim-sonuclari/
16\. KKTC İstatistik Kurumu, Tüketici Fiyat Endeksi - Temmuz 2026. https://istatistik.gov.ct.tr/t252ketici-fiyat-endeksi-temmuz-2026
17\. Reuters (19 Oct 2025), KKTC Cumhurbaşkanlığı seçimi sonucu ve siyasi bağlam. https://www.reuters.com/world/middle-east/turkish-cypriots-vote-leader-peace-talks-hang-balance-2025-10-19/
18\. KKTC Yüksek Seçim Kurulu, 19 Ekim 2025 Cumhurbaşkanlığı Seçim Sonuçları ilanı. https://ysk.gov.ct.tr/wp-content/uploads/2025/10/KKTC-Geneli-Cumhurbaskanligi-Secim-Sonucu-Ilani.pdf
19. Küren, E. (2026), "DEEPFAKE ÇAĞI: Gördüğümüze mi, Yoksa Gerçeğe mi İnanacağız?", BTKıbrıs, Sayı 6, Eylül 2026, s. 44-45. https://www.btkibris.org/Agustos2026/index.html
20. Shin, D. & Jitkajornwanich, K. (2024), "How Algorithms Promote Self-Radicalization: Audit of TikTok's Algorithm Using a Reverse Engineering Method", Social Science Computer Review, 42(4), 1020–1040. https://doi.org/10.1177/08944393231225547

Ata Ateş
Yapay Zeka Mühendisliği
DAÜ 2. sınıf öğrencisi

Model Bir Yazılım Değil, Bir Devlet Politikasıdır

Geçen sayıyı bir söz vererek bitirmiştim, envanterin üzerine koymaya devam edecek, yasalarda nelerin değişmesi gerektiğini ve kaybettiğimiz modelin bugüne nasıl uyarlanabileceğini anlatacaktım. Bu yazı o sözün ilk yarısıdır, yasalara geçmeden önce bir şeyi netleştirmemiz gerekiyor, hangi yasanın değişeceğini, neye göre değişeceğini bilmeden konuşamayız. O "neye göre" nin adı modeldir.

Dördüncü sayıda modelle çıktığımız yolda modeli kaybettiğimizi yazmıştım. Bu kez, teknik ayrıntıya girmeden, o modelin bugünkü halini sade bir dille tarif etmek istiyorum. Çünkü yıllardır gördüğüm en büyük yanlış, dijital devletin bir yazılım ihalesi, bir portal ya da bir veri merkezi projesi sanılmasıdır. Ama gerçek maalesef bu değildir. Dijital devlet, devletin kendi kurumları arasında nasıl çalışacağına dair bir tercihtir, teknoloji o tercihin sadece aracıdır.

Model, birkaç cümleyle;
Modeli anlatmak için mühendis olmaya gerek yok. Altı cümle yeter.

Birincisi: Vatandaşın kamu hizmetine dijital yoldan erişmesi bir hak olmalı; ama bu, yaşlının, engellinin ya da interneti olmayanın kapıda bırakılması anlamına gelmemeli. Tek kapı, ama tek kanal değil.

İkincisi: Devletin bir kurumunda zaten bulunan bilgi, vatandaştan bir daha istenmemeli. Nüfus kaydında olan adresi, vergi dairesinde olan borcu, tapuda olan mülkü vatandaş elinde dosyayla kurum kurum taşımamalı.

Üçüncüsü: Veri kaynağında kalmalı. Her şeyi tek bir dev havuza yığan bir devlet değil; nüfusun nüfusta, tapunun tapuda, sağlığın sağlıkta durduğu, kurumların birbirine güvenli bir değişim katmanı üzerinden sorduğu bir devlet. Estonya'nın X-Road'undan öğrendiğimiz ve o günlerde KKTC ölçeğine uyarladığımız yaklaşım tam olarak buydu.

Dördüncüsü: Her paylaşımın kaydı tutulmalı. Hangi kurum, hangi amaçla, hangi veriye, ne zaman erişti; bu sorunun cevabı hem denetçi hem de vatandaşın kendisi tarafından görülebilmeli. Vatandaş kendi verisine kimin baktığını göremiyorsa, o sisteme güvenmesini beklemek haksızlıktır.

Beşincisi: Kurumlar açık standartlarla konuşmalı. Her kurumun kendi tedarikçisine, kendi formatına ve kendi kapalı sistemine hapsolduğu bir devlet, on yıl sonra bugünkü gibi yeniden sıfırdan başlamak zorunda kalır.

Altıncısı: Otomasyon hesap verebilir olmalı. Yapay zekâ ya da otomatik bir sistem vatandaş hakkında karar üretiyorsa, o kararın gerekçesi anlaşılabilmeli, itiraz edilebilmeli ve nihai sorumluluk bir insanda kalmalı.
Bu altı cümlenin arkasında bir de kurumsal tercih var: KKTC'de yeni ve büyük kurumlar yaratmak yerine, mevcut kurumların görevlerini netleştirmek ve onları birbirine bağlamak. DDEDK mimariyi ve entegrasyonu koordine eder; KVKK Kurulu mahremiyeti bağımsız olarak denetler; BTHK haberleşme altyapısını düzenler; Milli Arşiv elektronik belgenin ömrünü belirler; YYK yayıncılıkla sınırlı kalır. Her kurum kendi alanında uzman, ama hepsi aynı resmin parçası. Dördüncü sayıda anlattığım "o masa"nın kurumsal karşılığı budur.

Bu model hangi yasalara dayanır?

Model bir kez tarif edilince, mevzuat envanterinin neresinin eksik, neresinin eskimiş olduğu kendiliğinden görünür hale gelir. Ayrıntıya girmeden, her birini birkaç cümleyle sıralayayım.

Olmayan ve yazılması gerekenler

Dijital Devlet, Kamu Verisi ve Dijital Katılım Yasası: Modelin çatısı budur. Dijital hizmet hakkını, tek sefer veri ilkesini, kamu veri değişim katmanını, açık veriyi ve vatandaşın kendi verisine erişim günlüğünü devlet çapında bağlayıcı hale getirir. Bu yasa olmadan her kurum kendi adasında kalır; ortak devlet standardı oluşmaz.

Elektronik Kimlik ve Güven Hizmetleri Yasası: Elimizdeki elektronik imza yasası gerekli ama yeterli değil. Ulusal dijital kimlik, mobil kimlik, elektronik mühür, zaman damgası, e-tebligat ve dijital vekâlet aynı çatı altında, Avrupa'nın eIDAS mantığıyla düzenlenmeli. Dijital kimlik olmadan ne tek sefer veri ne de katılım araçları çalışır.

Ulusal Siber Güvenlik Merkezi Yasası: Kamunun kendi CERT/SOC yapısı, kritik kamu altyapısının izlenmesi, olay koordinasyonu ve zafiyet bildirimi için küçük ama uzman bir teknik otorite gerekir. Bugün bu görev fiilen sahipsizdir.

Çevrimiçi İçerik ve Dijital Hizmetler Yasası: Üçüncü sayıda anlattığım ayrımın hukuki karşılığı. Bilişim Suçları Yasası'ndan çıkarılması gereken içerik hükümleri, platform sorumluluğu, bildirim-eylem ve itiraz mekanizmasıyla birlikte ayrı bir temel hak güvence yasasında düzenlenmeli.

Kamu Yapay Zekâ ve Algoritmik Karar Yasası: Yapay zekâ kamuda kullanılacak; mesele yasaklamak değil kayıt altına almaktır. Kamu yapay zekâ envanteri, risk sınıflandırması, etki değerlendirmesi ve insan gözetimi zorunluluğu bu yasada yer almalı.

Mevcut olup değişmesi gerekenler

DDEDK Yasası (76/2023): Kuruma önemli görevler veriyor; ancak KamuNet, Kamu Bulutu, Kamu Veri Değişim Katmanı ve vatandaş veri erişim günlüğü gibi modelin omurgasını oluşturan kavramlar açıkça tanımlanmalı, kurumun mimari koordinasyon rolü kadro yasası olmaktan çıkarılıp gerçek bir yetkiye dönüştürülmeli.

Kişisel Verilerin Korunması Yasası (89/2007): Yaklaşık yirmi yıllık metin, GDPR sonrası dünyanın gerisinde kaldı. Veri ihlali bildirimi, etki değerlendirmesi, otomatik karar, çocuk ve biyometrik veri, veri sorumlusu tanımı ve caydırıcı yaptırımlar eklenmeli; Kurul gerçekten bağımsız bir denetim otoritesi haline getirilmeli.

Elektronik Haberleşme Yasası: BTHK'nın doğal alanı altyapıdır. Kritik haberleşme

altyapısı ve hizmet sürekliliği hükümleri güçlendirilmeli; ancak içerik denetimi ve kişisel veri denetimi bu yasanın işi olmaktan çıkarılmalı.

Bilişim Suçları Yasası: Gerçek siber suç çekirdeğine, yani hukuka aykırı erişim, müdahale, veri bozma, zararlı yazılım ve dijital delil alanına döndürülmeli; Budapeşte Sözleşmesi çizgisine oturtulmalı. Anayasa Mahkemesi'nin 2022 kararı zaten hangi bölgenin sorunlu olduğunu göstermişti.

Yayın Yüksek Kurulu Yasası: YYK'nın rolü interneti denetlemek değil; görsel-işitsel medya, IP TV, internet yayıncılığı ve video paylaşım platformlarının yayın boyutunu çağa uygun düzenlemektir. Bireysel yayıncılık lisans kapsamı dışında korunmalı.

Milli Arşiv ve Araştırma Dairesi Yasası: Elektronik belge, elektronik arşiv, metadata, saklama-imha planı ve belge ömür tespiti tanımlanmadan elektronik devlet sürdürülemez. Bugün üretilen dijital belgenin yirmi yıl sonra nerede ve hangi biçimde duracağı belirsizdir.

Yasalar bunlar. Altında tüzükler, standartlar ve rehberler var; onlar ayrı bir yazının konusu. Ama liste bile tek başına bir şeyi anlatıyor: Bunlar birbirinden bağımsız on ayrı iş değil, aynı modelin on ayrı parçasıdır. Biri tek başına çıkarsa, yine bir ada olur.

Sıra önemli: Önce politika, sonra inşa

Burada asıl söylemek istediğime geliyorum. Yukarıdaki listeyi bir bakanlığa verip "hazırlayın" demek hiçbir şey çözmez. Çünkü bugüne kadar yapılan tam da buydu: Her kurum kendi yasasını kendi dar penceresinden güncelledi, kimse bütüne bakmadı ve ortaya birbiriyle konuşmayan mevzuat adaları çıktı.

Doğru sıra şudur. Önce model, hükümetlerin üstünde bir devlet politikası olarak benimsenmeli; Meclis'ten geçen, seçimle değişmeyen, on yıllık ufku olan bir metin olarak. O günkü masanın en büyük eksiği de buydu: Elimizde bir yol haritası vardı, ama onu koruyacak bir devlet politikası yoktu; bir seçimde dağıldı.

Sonra kavramlar tekleştirilmeli. KamuNet nedir, ana veri kaydı nedir, kritik altyapı nedir; on yasada aynı kelime aynı anlama gelmeli. Ardından kurum yasaları birlikte okunarak tadil edilmeli, çatı yasa çıkarılmalı, tüzük ve standart paketi hazırlanmalı, pilotlarla denenmeli, ölçülmeli.

Ve en zor kısmı: Bu modele göre her şeyin yeniden inşa edilmesi gerekiyor. İhale şartnameleri ürün listesi olmaktan çıkıp standart ve entegrasyon zorunluluğu içermeli. Kurumların satın alma alışkanlıkları, yazılım tercihleri, veri saklama biçimleri, hatta personel yetkinlikleri bu modele göre yeniden tanımlanmalı. Modelden bağımsız kurulan her yeni sistem, yarın tekrar sökülecek bir yatırımdır.

Çok geç kaldık

Bunu yazarken kendimi de suçlu hissediyorum; çünkü 2010'a doğru bunların büyük kısmı Başbakanlık'ta sırasını bekliyordu. O günden bu yana Avrupa eIDAS'ı yazdı, ikinci sürümünü çıkardı; Dijital Hizmetler Yasası'nı, Yapay Zekâ Yasası'nı geçirdi. Estonya modelini dünyaya ihraç etti. Biz ise aynı yasaları hâlâ "olsa iyi olur" listesinde tutuyoruz ve yeni bir e-devlet söylemini, altında model olmadan konuşuyoruz.

Geç kaldık; ama geç kalmak, yanlış yerden başlamanın mazereti olamaz. Bugün de bir portal, bir uygulama ya da bir veri merkezi ile başlarsak on yıl sonra yine aynı yazıyı yazarız. Başlangıç noktası tektir: Modeli tarif etmek, onu bir devlet politikası yapmak ve geri kalan her şeyi ona göre kurmak.

Önümüzdeki sayıda sözümün ikinci yarısına geçeceğim: Kaybettiğimiz modelin bugünün teknolojisine ve bugünün KKTC'sine nasıl uyarlanacağını, kurumların bu modelde tam olarak nerede duracağını ve vatandaşın bu resimde neyi görüp neyi talep edebileceğini anlatacağım.

Eralp Curcioğlu
Elektrik ve Elektronik Mühendisi
EMI Technologies Ltd. Direktörü

PEGASUS: BİR TELEFONDAN CEMAL KAŞIKÇI CİNAYETİNE UZANAN DİJİTAL GÖLGE

Ve Kıbrıs'ın Ortasında Büyüyen Yeni Bölgesel Güvenlik Tehdidi

Bir insanı takip etmek için artık peşine ajan takmak, evinin karşısına araç park etmek veya telefon hattını fiziksel olarak dinlemek gerekmiyor. Cebindeki akıllı telefon yeterli. Üstelik günümüzün gelişmiş casus yazılımlarında hedef kişinin şüpheli bir uygulama yüklemesi, garip bir bağlantıya tıklaması, hatta bazen telefonuna dokunması bile gerekmiyor.

İşte Pegasus'u sıradan zararlı yazılımlardan ayıran nokta tam olarak burada başlıyor.

İsrailli NSO Group tarafından geliştirilen Pegasus; hedef telefondaki mesajlara, fotoğraflara, e-postalara, konum bilgilerine ve kişi listelerine erişebilen, bazı senaryolarda mikrofon ve kamerayı uzaktan kullanabilen son derece gelişmiş bir mobil gözetleme sistemi olarak tanınıyor. Günümüzde bu sınıftaki sistemler için **"mercenary spyware"**, yani **paralı/ticari casus yazılım** tanımı kullanılıyor.

Pegasus başlangıçta terörizm ve ağır suçlarla mücadele amacıyla devlet kurumlarına sunulan bir istihbarat ürünü olarak tanıtıldı. NSO Group da ürünlerinin suç ve terörle mücadele amacıyla yetkilendirilmiş devlet kurumlarına satıldığını uzun yıllardır savunuyor.

Sorun teknolojinin varlığından çok, **kimin telefonunun, hangi gerekçeyle ve hangi hukuki denetim altında izleneceği** sorusunda ortaya çıktı. Çünkü Pegasus'un hikâyesi kısa süre içerisinde gazetecilerin, insan hakları savunucularının, avukatların, diplomatların, siyasetçilerin ve muhaliflerin telefonlarına kadar uzandı.

Ve bu hikâyenin en karanlık duraklarından biri, 2 Ekim 2018'de İstanbul'daki Suudi Arabistan Başkonsolosluğuna giren ve bir daha canlı çıkamayan gazeteci **Cemal Kaşıkçı** oldu.

Önce Telefonlar İzlenmeye Başladı

Pegasus'un kamuoyunda geniş biçimde tanınması 2016 yılına uzanıyor. Birleşik Arap Emirlikleri'nden insan hakları savunucusu Ahmed Mansoor'un aldığı şüpheli mesajlar Citizen Lab araştırmacıları tarafından incelendiğinde, iPhone'ların o dönemde bilinmeyen güvenlik açıklarını kullanan son derece gelişmiş bir saldırı zinciri ortaya çıkarıldı.

Ancak sistem giderek daha karmaşık hâle geldi. Başlangıçta kullanıcıları sahte kargo mesajları, haber bağlantıları veya çeşitli sosyal mühendislik yöntemleriyle zararlı bağlantılara tıklatmaya çalışan saldırılar görülürken, daha sonra **"zero-click"** adı verilen saldırılar ortaya çıktı. Zero-click saldırının ürkütücü tarafı şudur:

Kurbanın hata yapmasına gerek yoktur.

- Mesaja tıklamayabilirsiniz.
- Bilinmeyen uygulama kurmayabilirsiniz.
- Telefonunuzu güncel tutabilirsiniz.

Buna rağmen işletim sistemi veya mesajlaşma altyapısındaki bilinmeyen bir güvenlik açığı kullanılarak cihaz hedef alınabilir.

Amnesty International'ın Temmuz 2021'de yayımladığı kapsamlı teknik inceleme, Pegasus ekosisteminin yalnızca telefona yüklenen küçük bir casus programdan ibaret olmadığını; saldırı altyapısı, exploit zincirleri, anonimleştirme sunucuları, müşteri sistemleri ve veri toplama altyapısıyla birlikte çalışan karmaşık bir istihbarat sistemi olduğunu ortaya koyuyor.

Bu nedenle hedef alınan bir telefon aslında kişinin yalnızca kendi sırlarını açığa çıkarmıyor.

Telefon;

- ailesini,
- arkadaşlarını,
- iş arkadaşlarını,
- kaynaklarını,
- görüştüğü gazetecileri,
- gideceği yerleri,
- planladığı toplantıları

da açığa çıkarabilecek bir dijital istihbarat sensörüne dönüşüyor.

Cemal Kaşıkçı vakasını önemli kılan noktalardan biri de tam olarak budur.

Kaşıkçı'ya Giden Dijital Yol

Cemal Kaşıkçı, 2017 yılında Suudi Arabistan'dan ayrılarak ABD'ye yerleşmiş ve Washington Post'ta özellikle Suudi yönetimini eleştiren yazılar kaleme almaya başlamıştı.

Bu dönemde görüştüğü kişilerden biri Kanada'da yaşayan Suudi muhalif **Omar Abdulaziz** idi.

İkili WhatsApp üzerinden yoğun biçimde haberleşiyor, Suudi Arabistan'daki gelişmeleri tartışıyor ve çeşitli projeler üzerinde konuşuyordu.

Fakat Abdulaziz'in telefonu güvenli değildi.

Citizen Lab, yaptığı adli inceleme sonucunda Omar Abdulaziz'in telefonunun **Pegasus ile enfekte edildiğini yüksek güvenle değerlendirdi** ve operasyonu Suudi Arabistan bağlantılı bir Pegasus operatörüyle ilişkilendirdi. Araştırma 1 Ekim 2018 tarihinde yayımlandı.

Tarihe dikkat:

2 Ekim 2018: Cemal Kaşıkçı İstanbul'daki Suudi Arabistan Başkonsolosluğunda öldürüldü.

2 Ekim 2018'den birkaç gün sonra: Abdulaziz'in Pegasus ile

izlendiğine ilişkin araştırma yayımlandı.

Bu kronoloji tek başına "Pegasus cinayeti gerçekleştirdi" anlamına gelmeyebilir.

Ancak çok daha ciddi bir soruyu gündeme getirir:

Kaşıkçı'nın iletişim ağı, planları ve özel görüşmeleri, yakın çevresindeki insanların telefonlarının ele geçirilmesi sayesinde önceden izlenmiş olabilir miydi?

Birleşmiş Milletler Özel Raportörü Agnès Callamard'ın 2019 yılında hazırladığı Kaşıkçı raporunda da Omar Abdulaziz'in telefonunun Pegasus ile enfekte edilmesine ayrı bir bölüm ayrıldı. Raporda, Abdulaziz'in Kaşıkçı ile sık iletişim hâlinde olduğu ve telefonun ele geçirilmesinin mesajlar, kişiler, e-postalar ve diğer özel verilere erişim imkânı sağlayabileceği kayda geçirildi.

Bu, olayın dijital gözetim boyutunun uluslararası bir insan hakları soruşturmasına girdiği anlamına geliyordu.

Cinayetten Sonra da Telefonlar Susmadı

Pegasus Project kapsamında 2021 yılında yayımlanan araştırmalar tabloyu daha da genişletti.

Amnesty International Security Lab'in adli incelemesine göre Cemal Kaşıkçı'nın nişanlısı **Hatice Cengiz'in telefonu, cinayetten yalnızca dört gün sonra Pegasus ile başarılı biçimde enfekte edilmişti.**

Kaşıkçı'nın eşi Hanan Elatr'ın da Nisan 2018'de BAE'de gözaltındayken birçok kez hedeflendiği, oğlu Abdullah'ın telefon numarasının da potansiyel hedefler arasında bulunduğu bildirildi.

NSO Group ise Kaşıkçı cinayetiyle teknolojileri arasında bağlantı bulunduğu yönündeki suçlamaları reddetti ve Pegasus'un Kaşıkçı'nın öldürülmesiyle ilişkili olmadığını savundu.

Bu ayrım önemlidir.

Bugün kamuya açık teknik veriler bize **Pegasus'un Kaşıkçı'nın yakın çevresindeki kişilere karşı kullanıldığını** gösterebiliyor.

Ancak kamuya açık adli kanıtlar "cinayet Pegasus sayesinde planlandı" şeklinde kesin bir teknik hüküm kurmamıza izin vermiyor.

Buna rağmen ortaya çıkan tablo, modern istihbarat faaliyetlerinin fiziksel ve dijital dünyayı nasıl birleştirebildiğine ilişkin son derece ciddi bir örnek oluşturuyor.

ABD Ulusal İstihbarat Direktörlüğü'nün 2021'de kamuoyuna açıkladığı değerlendirme ise Kaşıkçı'nın öldürülmesi operasyonunun başka bir boyutunu ortaya koydu. ABD istihbarat topluluğu, Suudi Veliaht Prensi Muhammed bin Selman'ın Kaşıkçı'yı yakalamaya veya öldürmeye yönelik İstanbul operasyonunu onayladığı değerlendirmesinde bulundu.

Dolayısıyla karşımızda birbirinden ayrı fakat aynı dönemde gelişen iki alan bulunuyor:

Bir tarafta **fiziksel operasyon**, diğer tarafta **dijital gözetim ağı**.

21'inci yüzyıl istihbaratının tehlikeli birleşimi de burada ortaya çıkmaktadır.

Pegasus Bugün Hala Yaşıyor

Pegasus'u yalnızca 2018 yılında yaşanmış bir skandal olarak değerlendirmek büyük hata olur.

Mart 2025'te Amnesty International, Sırbistan'daki iki araştırmacı gazetecinin Pegasus ile hedeflendiğine ilişkin yeni teknik bulgular yayımladı.

Temmuz 2022-2023'de ise daha çarpıcı bir vaka açıklandı.

Pegasus ve benzeri casus yazılımları araştırmak üzere kurulan Avrupa Parlamentosu **PEGA Komitesi'nde görev yapmış eski Avrupa Parlamentosu üyesi ve gazeteci Stelios Kouloglou'nun telefonunun, komitede görev yaptığı dönemde Predator/Pegasus dinleme skandalı (Dinleme Kriz / Predatorgate) ile enfekte edildiği adli olarak doğrulandı.**

Yani casus yazılımı araştıran kişilerin dahi casus yazılımla hedef alınabildiği bir dünyadan söz ediyoruz.

Apple da tehdidin devam ettiğini açıkça kabul ediyor.

Şirket, 2021'den bu yana yılda birkaç kez paralı casus yazılım saldırıları konusunda kullanıcılarına tehdit bildirimleri gönderdiğini ve bugüne kadar **150'den fazla ülkedeki kullanıcılara bildirim yapıldığını** belirtiyor. Apple ayrıca bu saldırıların özellikle gazeteciler, aktivistler, siyasetçiler ve diplomatlar gibi çok küçük fakat özel olarak seçilmiş bir grubu hedef aldığını vurguluyor.

Buradaki mesaj açıktır:

Pegasus bir geçmiş zaman hikâyesi değildir.

Peki Kıbrıs Neden Önemli?

Konuyu KKTC açısından değerlendirdiğimizde mesele çok daha yakınımıza geliyor.

Avrupa Parlamentosu'nun Pegasus ve benzeri casus yazılımları araştıran PEGA çalışmasında Kıbrıs, Avrupa'daki gözetim teknolojileri sektörü bakımından önemli noktalardan biri olarak ele alındı.

Parlamentonun 2023 tarihli değerlendirmesinde, o tarihe kadar Kıbrıs Cumhuriyeti'nde doğrulanmış casus yazılım enfeksiyonu iddiası bulunmadığı özellikle belirtilirken, **Kıbrıs'ın gözetim teknolojileri açısından önemli bir Avrupa ihracat merkezi olduğu vurgulandı.**

Aynı raporlarda NSO Group'un geçmiş kurumsal varlıkları yanında, Predator casus yazılımıyla ilişkilendirilen Intellexa ve başka gözetim teknolojisi şirketlerinin Kıbrıs bağlantıları da ele alındı.

Bu nedenle Kıbrıs Adası'nı yalnızca coğrafi açıdan değerlendirmek yanlış olur.

Ada;

- Avrupa Birliği,
- Türkiye,
- İsrail,
- Orta Doğu,
- Doğu Akdeniz enerji politikaları,
- askeri ve diplomatik faaliyetler…

arasında son derece hassas bir jeopolitik bölgede bulunuyor.

KKTC'de görev yapan diplomatların, siyasetçilerin, gazetecilerin, kamu yöneticilerinin, iş insanlarının ve kritik kurum çalışanlarının telefonlarında yalnızca KKTC'ye ait bilgiler bulunmuyor.Bu cihazlar Türkiye, Avrupa Birliği, Orta Doğu ve farklı ülkelerle yapılan görüşmelerin de kesişim noktası hâline gelebiliyor. Dolayısıyla tek bir telefonun ele geçirilmesi yalnızca **kişisel veri ihlali değil, bölgesel istihbarat problemi** hâline gelebilir.

KKTC İçin Artık Sorulması Gereken Soru

KKTC'de mobil cihazlar üzerinde gerçekleştirilen adli incelemelerde Pegasus ve benzeri paralı casus yazılımlarla ilişkilendirilebilecek IOC'lerin, şüpheli kayıtların veya tehdit göstergelerinin görülmeye başlanması, konunun artık bizim için de teorik olmaktan çıktığını düşündürmektedir.

Ancak burada son derece önemli bir teknik ayrım yapmakta fayda oolabileceğini düşünmekteyim:

Bir eşleşmesi veya uyarı tek başına "bu telefon kesin olarak Pegasus ile enfekte edildi" demek değildir.

Mobil adli vaka araçlaryla elde edilen kayıtların zaman çizelgesi, alan adları, süreçler, mesajlar, ağ kayıtları ve diğer adli verilerle birlikte değerlendirilmesi gerekir.

Ciddi vakalar mümkünse ikinci bir bağımsız laboratuvar tarafından da doğrulanmalıdır.

Çünkü yanlış alarm kadar gerçek saldırının gözden kaçırılması da tehlikelidir.

Asıl yapılması gereken korku yaratmak değil, **kurumsal kapasite oluşturmaktır**.

KKTC'nin artık üst düzey kamu yöneticileri, diplomatlar, gazeteciler ve kritik görevlerde bulunan kişiler için bir **Mobil Tehdit ve Adli Analiz Merkezi** oluşturmayı değerlendirmesi gerekir.

Apple veya başka üreticilerden paralı casus yazılım tehdidi uyarısı alan kişiler için başvurulabilecek resmi bir mekanizma belirlenmeli; cihaz sıfırlanmadan önce adli imaj ve gerekli kayıtlar korunmalı; IOC'ler merkezi biçimde değerlendirilerek kurumların firewall, DNS ve diğer güvenlik sistemleriyle paylaşılmalıdır.

Ve en önemlisi:

Bir kişiye gelen casus yazılım uyarısı yalnızca o kişinin özel problemi olarak görülmemelidir.

Çünkü hedef bazen telefonun sahibi değildir.

Hedef, onun tanıdığı başka biri olabilir.

Kaşıkçı Vakasının Bize Bıraktığı Ders

Cemal Kaşıkçı cinayetinden çıkarılması gereken en önemli siber güvenlik derslerinden biri budur.

Bir insanın telefonuna ulaşamıyorsanız onun arkadaşının telefonuna ulaşırsınız.

Arkadaşına ulaşamıyorsanız eşine…
Meslektaşına…
Danışmanına…
Avukatına…
Gazetecisine…

Ve dijital dünyanın görünmez bağlantıları sonunda hedef kişiye ulaşmanızı sağlar.

Pegasus'un gerçek gücü yalnızca mikrofonu açabilmesinde değildir.

Asıl güç, **bir insanın çevresindeki bütün ilişki ağını görünür hâle getirebilmesidir**.

Cemal Kaşıkçı 2 Ekim 2018'de İstanbul'daki Suudi Arabistan Başkonsolosluğuna girdiğinde dünya hala telefonları büyük ölçüde iletişim aracı olarak görüyordu.

Bugün biliyoruz ki cebimizde taşıdığımız cihaz aynı zamanda bulunduğumuz yeri, görüştüğümüz insanları, yazdığımız mesajları, fotoğraflarımızı, düşüncelerimizi ve kimi zaman devletlerin sırlarını taşıyor.

2026 yılında artık tartışmamız gereken soru "Pegasus KKTC'ye gelir mi?" değildir. Yapılan testler göstermektedir ki Pegasus ve benzeri başka casus yazılımlar **bazı mobil cihazlarımızda bulunmuştur**.

Daha doğru soru şudur:

Pegasus veya onun kadar gelişmiş başka bir paralı casus yazılım bugün KKTC'deki bir telefonu hedef alırsa bunu kim fark edecek, kim inceleyecek, kime bildirecek ve devlet hangi mekanizmayla karşılık verecek?

Çünkü dijital dünyada sınır kapısı yoktur.

Casus yazılım pasaport göstermez.

Ve bazen bir cinayete giden yol, sokaktaki bir takip aracıyla değil, cebimizde sessizce duran bir telefonla başlayabilmektedir.

Kazım ATEŞ

kazimates@yahoo.com

Bir Müzik Efsanesinin İzinde: Sting, The Police Mirası ve Kıbrıs'ın BT Merkezi Limasol

Kıbrıs'ın güney kıyısında Akdeniz güneşinin denizle buluştuğu Limasol (Leymosun), 4 Ağustos 2026 gecesi tarihi müzik olaylarından birine ev sahipliği yaptı. 17 Grammy ödüllü efsanevi müzisyen Sting, "STING 3.0" World Tour kapsamında Tsirion Stadyumu'nu dolduran binlerce müzikseverle buluştu. Müzik tarihine altın harflerle yazılan The Police geçmişinden solo kariyerine uzanan bu performans, Limasol'un büyüleyici atmosferi ve teknoloji odaklı vizyonuyla birleşerek unutulmaz bir ada kaçamağı sundu.

The Police Köklerinden Trio Enerjisine: Bir Müzik Efsanesinin Evrimi

1977 yılında Londra'da kurulan **The Police**, punk rock'ın ham enerjisini reggae ritimleriyle ve caz armonileriyle harmanlayarak New Wave akımının öncülerinden biri oldu. Gordon Sumner (Sting), Stewart Copeland ve Andy Summers'tan oluşan bu ikonik üçlü, rock müzik tarihine damga vuran kült albümlere imza attı. Sting, 1980'lerin ortasında başarılı solo kariyerine adım atsa da The Police şarkılarındaki dinamizm ve Bas-Vokal performansı müzik kimliğinin ana omurgasını oluşturmaya devam etti. **STING 3.0** turnesi, tam da bu köklere bir saygı duruşu niteliğinde. Sahnede dev orkestralar yerine uzun yıllardır birlikte çalıştığı virtüöz gitarist **Dominic Miller** ve davulcu **Chris Maas** ile birlikte minimalist bir "trio" (üçlü) formatında yer alan Sting, The Police'in o ham ve yüksek enerjili stüdyo ruhunu Tsirion Stadyumu'na taşıdı.

Resmen Sting ve 2 arkadaşının Tsirion Stadyumu salladığı Limasol Konseri Setlist'i aşağıdaki parçalardan oluşmuştu.

1. Message in a Bottle *(The Police)*
2. Voices Inside My Head *(The Police)*
3. If I Ever Lose My Faith in You
4. Englishman in New York
5. Every Little Thing She Does Is Magic *(The Police)*
6. Fields of Gold
7. Never Coming Home
8. Mad About You
9. Shape of My Heart
10. Driven to Tears *(The Police)*
11. Walking on the Moon *(The Police)*
12. So Lonely *(The Police)*
13. Desert Rose
14. King of Pain *(The Police)*
15. Every Breath You Take *(The Police)*
16. Roxanne *(The Police)*
17. Fragile

Genelde 50 yaş ve üstü 10 binlerce kişini katıldığı konserde Tüm parçalar birbirinden eşssiz değer gördü.Ama benim canlı olarak ilk kez dinlediğim Fragile benim için herhalde bir numaraydı.

Konser ve Limasol ile ilgili bazı notlar

- Sting Konserin yapıldığı Tsirion Stadyumu Limasol'un en bilinen ve tarihi spor ve kültür komplekslerinden biridir. Stadyum 1975 yılında hizmete açılmıştır. Stadyum açılışında finansal kaynak sağlayan ve arazisini bağışlayan hayırsever Petros Tsirostan almaktadır.13300 oturma koltuğuna sahip olmasına karşın ayakta durma ile konser sayısı 20000 lere ulaşmaktadır. Tsiron stadyumu eskiden limasol takımlarının ev sahipliğini yapmaktaydı.
- Konserde ana sponsorlar Bilgi Teknolojileri firmalarıydı. Özellikle Routing, Switching, Data Center, Software Infrastructure reklamlarını bol bol konser boyunce tüm reklam panolarında görmek benim içi şaşırtıcı olmuştu.
- Konserde tek bir marka Bira ve Su satılması yine ilginç bir ayrıntıydı. Yalnız ve yalnız yerel KEO birası satılıyor ve reklam panolarında yer alıyordu.Şunu söylemeliyim ki bu kadar teknoloji firmasının bulunduğu konserde bira ve satış noktalarındaki kuyruk ve satıcı çocukların amatörlüğü dikkat çekiciydi.
- Konserde yüzlerce Kıbrıslı türk vardı. Nerdeyse Siyasi görüşleri farklı kesimden olan insanlar Stingi dinlemek için Limasol sahasına akın etmişlerdi.
- Konser alanının etrafındaki park alanları yetersiz olmasına karşın trafik kısa zamanda olaysız dağıldı. Bizler kendi arabamızla konser yerine gelmektense taksi kullandık.
- Defalarca gitiğim limasola son 10 yıldır ilk kez gittim.Şehir merkezinde diklemesine büyüyen 10 larca yeni binalar dikkat çekici boyutdaydı. En güzel yanı Limasol sahil şeridinin yapılaşmadan mümkün olduğunca korunmasıydı. Halkın denize erişiminde hiç bir engel bulunmuyordu.
- Kaldığımız Nyx hotel limasol merkezde olup iyi sayılabilecek bir yerdi. Fakat Sting Konseri tüm merkezi hotellerin Fiyatını artırmıştı. Hotel kahvaltısı çok çok iyiydi.

- Hotel civarında Zara,H&M gibi markaların nerdeyse hepsi bulunması kısmen de olsa alış veriş yapma imkanımız oldu. Giyim fiyatları mevsim nedeniyle gayet ucuz sayılabilecek durudaydı.

Limasol da Özellikle Rusya etkisini rahatlıkla görebiliyorsunuz. Yani LimassolGrad Kavramı abartı olmadığını anlıyoruz.

Doğu Akdeniz'in Bilişim ve Fintek Üssü: Limasol ve ICT Destekçileri

Limasol yalnızca tarihi kalesi, palmiyeli sahil kordonu (Molos) ve marina yaşamıyla değil; son yıllarda "Akdeniz'in Silikon Vadisi" olarak anılan uluslararası bilişim (ICT), yazılım ve fintek ekosistemiyle de öne çıkıyor.

Bu çapta devasa bir organizasyonun gerçekleşmesinde teknoloji, yazılım ve dijital altyapı firmalarının sponsorluğu kritik rol oynadı. Sunumu **QTech World** tarafından üstlenilen ve Platin Sponsorluğunu uluslararası dijital ödeme çözümleri sağlayıcısı **Ecommbx**'in yürüttüğü organizasyonda, oyun yazılımı geliştiricisi **Brickworks Games** gibi ICT odaklı destekçiler öne çıktı.

Bilişim ve Teknoloji Sektörünün Limasol'a Katkıları

- **Ekonomik Dönüşüm ve İstihdam:** Limasol; Uluslararası Yazılım, Fintek, RegTech ve GameDev şirketlerinin merkezlerini adaya taşımasıyla geleneksel bir liman kentinden yüksek katma değerli bir teknoloji merkezine dönüştü.
- **Altyapı ve Akıllı Şehir Yatırımları:** Bölgeye yerleşen teknoloji devleri, fiber optik veri altyapısının, veri merkezlerinin (Data Center) ve 5G ağlarının gelişmesine doğrudan finansal katkı sağladı.
- **Kültürel ve Küresel Etkinlik Çekim Gücü:** ICT sektörünün adaya kazandırdığı uluslararası iş gücü ve ekonomik sermaye, Sting 3.0 gibi dev dünya turnelerinin, BEONIX gibi elektronik müzik festivallerinin ve uluslararası teknoloji zirvelerinin Limasol'a gelmesini doğrudan tetikliyor.

Leymosun Yazımdan beklentilerim

- **Devlet menfaatinde ve kontrolünde bir Teknolojik Yatırım İklimi :** Özellikle dış yatırımların teşviki devlet menfaatleri ile beraber yönlendirip teşvik etmek hayali
- **Kıbrıs Türk ICT mühendislerinin göçünün engelenmesi:** Özellikle yeni nesil mühendis kardeşlerimiz uluslararası standartlarda iş sahibi olması
- **Bizim de bir Teknoloji şehrimiz olsun.** Birinci tercihim Mağusa ikincisi ise Lefke olsun. Akıllı bir şehrimiz olsun.
- **Teknoloji tartışmaları son bulsun:** Halen daha yok fiber yok 5G yok Starlink yok saçma sapan siber saldırı edebiyatları bitsin.Tüm dünya halletti halen daha empoze teknolojiler.Tüm düya neyi yaparsa biz de onu yapalım.

Biraz Utopik bir yazı oldu: Bugünlerde seyrettiğim Tudors dizisi belki Thomas Moore'dan etkilenmişimdir.

YUSUF KÜÇÜK
yusufkucuk2014@gmail.com

Eylül 2026
btkibris.org

İnsan aklın sınırlarını zorlamadıkça hiçbir şeye ulaşamaz.
Albert Einstein

BTKıbrıs
Bilim, Bilişim, Teknoloji Dergisi