THE Fine PRINT

Gökçe

Mart 2019

78

DİJİTAL ÇAĞIN YENİ KÜLTÜRÜ: SİBER GÜVENLİK

Öne çıkanlar

Dr. Mehmet Bedii Kaya ile Röportaj

DİJİTAL ÇAĞIN YENİ KÜLTÜRÜ: SİBER GÜVENLİK

Çağımızda en değerli şeylerden biri bilgiye hızlı ve zahmetsiz ulaşabilmek. Tüm teknoloji buna hizmet edebilmek ve bunu daha iyi hale getirebilmek adına gelişiyor. Gün geçtikçe daha hızlı gelişen teknoloji kamu kurum ve kuruluşları ve özel hukuk kişileri tarafından daha fazla kullanılıyor ve hatta kendi çalışma organizasyonlarına entegre ediliyor. Bu kapsamda pek çok kamu kurum ve kuruluşu kendi altyapısını daha "elektronikleştirmek" için çabalıyor. Türkiye İstatistik Kurumu (TÜİK) 2018 yılı Hanehalkı Bilişim Teknolojileri Kullanım Araştırması verileri 16-74 yaş arası bireylerin bilgisayar ve internet kullanımının 2017 yılındaki yüzdeleri aşarak bilgisayar kullanımının %59,6, internet kullanımının ise %72,9'a yükseldiğini gözler önüne serdi[1]. TÜİK'in 2018 yılı Girişimlerde Bilişim Teknolojileri Kullanım Araştırması sonuçları da 10 ve daha fazla çalışanı olan girişimlerin internete erişim oranının %95,3 olduğunu gösteriyor[2].

Bilgi ve iletişim teknolojilerinin sadece özel sektörde değil; vatandaşın kamu kurum ve kuruluşlarıyla olan ilişkilerine de son derece entegre olmuş durumda. Bu kapsamda idare nezdinde gerçekleştirilen en kapsamlı elektronikleşme örneği olarak "e-Devlet" sistemi gösterilebilir. Bu sistem sayesinde vatandaşlar kamudan talep edecekleri evrakı çevrimiçi sistemler aracılığıyla talep edebiliyor ve pek çok başvuruyu bu sistem üzerinden gerçekleştirebiliyor. Yine, son yıllarda fazlaca gündemde olan elektronik tebligat sistemi ve kayıtlı elektronik posta (KEP) de bu teknolojiye ayak uydurma çabalarının esaslı emarelerinden.

Yukarıda belirttiğimiz örnekler, teknolojiye ayak uydurma çabalarının sadece birkaç tanesi. Bilgisayar ve elektronik düzeneklerin bu denli hayatımıza girmiş olması, yıllar içerisinde doğası gereği bunun korunmaya değer bir varlık haline gelmesine sebebiyet verdi. Gerek bu yaygın kullanım, gerek bilginin zaman içerisinde kendi ekonomisini yaratmış olması siber güvenlik ve veri gizliliği risklerini gün geçtikçe daha çok konuşulur hale getirdi. İşte siber güvenlik kavramı da tam olarak bu noktada gündeme gelmekte:

Siber güvenlik neyi ifade ediyor?

Ulaştırma ve Altyapı Bakanlığı tarafından hazırlanan Ulusal Siber Güvenlik Stratejisi metinleri kapsamında siber güvenlik; **siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunması, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, saldırıların ve siber güvenlik olaylarının tespit edilmesi, bu tespitlere karşı tepki mekanizmalarının devreye alınması ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi** olarak tanımlanmaktadır[3]. Bu tanım doğrultusunda siber güvenlik kısaca bilişim sistemleri ve bu sistemlerde yer alan verilerin güvenliği ve gizliliği başta olmak üzere siber alemin bir uçtan bir uca korunabilmesi olarak tanımlanabilir.

Yukarıdaki tanımdan da anlaşılacağı üzere siber güvenlik özünde sadece kamu kurum ve kuruluşlarının ya da sadece bireylerin sanal alemdeki güvenliğini konu edinmemekte; bunların hepsini kapsayan bir şemsiye kavram olarak kullanılmaktadır. Dolayısıyla siber güvenliğin bireylerin hayatındaki yansımaları "kişisel verilerin korunması", şirketler veya idare nezdindeki yansıması ise bilgi güvenliği ve operasyon güvenliği gibi farklı görünümlerde olabilir. Ancak bu siber güvenliğin sınırlı sayıda görünümü olduğu anlamına gelmemelidir. Dolayısıyla siber güvenlik veri güvenliği ile ilişkilendirilip genellikle kişisel verilerin korunması kapsamında ele alınsa dahi siber güvenliği sadece bu kapsamda değerlendirmek bu konunun önemini indirgemek olacaktır.

Siber güvenlik zafiyetleri sonucu meydana gelebilecek olumsuzluklar özel sektör aktörleri bakımından sadece veri ihlalleri

1 http://www.tuik.gov.tr/PreHaberBultenleri.do?id=27819
2 http://www.tuik.gov.tr/PreHaberBultenleri.do?id=27820
3 http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf

Daha fazla bilgi için, contact@gokce.av.tr adresinden iletişime geçebilirsiniz.

ile sınırlı olmaksızın, müşteri ve iş ortaklarının güveninin yitirilmesi, sermaye, rekabet gücü ve itibarın kaybedilmesi, idari cezalar ve tazminat talepleri karşı karşıya kalınması gibi farklı farklı olabilir. Bu farkındalığa sahip olan özel sektör aktörleri bilgi ve iletişim teknolojilerini kullanırken siber güvenliğe özel bir önem vermekte ve sistemlerindeki zayıflıkları tespit edip bunları kapama, detaylı ve düzenli raporlama yapma, sistemlerini güncel tutma, verilerini yedekleme gibi gerekli politika ve önlemleri almak konusunda çabalamaktadır. Bunun yanında, sistemin büyüdüğü şartlarda alınması gereken önlemlerin de arttığı düşünülecek olursa, pek çok şirket siber güvenlik zafiyetleri sebebiyle söz konusu olabilecek kayıpları önlemek adına "siber sigortalar"a başvurmaktadır. Siber sigortalar bu sebeple son yıllarda fazlaca popüler hale gelmiş ve birçok şirketin de sığınağı olmuş durumdadır.

Siber Güvenlik Düzenlemeleri

Yakın zamanda siber güvenliğe ilişkin en önemli hukuki gelişmelerden biri Avrupa Parlamentosu tarafından Siber Güvenlik Yasası'nın onaylanması olmuştur. Siber Güvenlik Yasası ile bağımsız uzman kuruluş olarak hareket edecek Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) kalıcı hale getirilmiş, siber güvenlik amaçlarını gerçekleştirebilmesi için ENISA'ya daha fazla kaynak sağlanmış ve Avrupa Birliği genelinde dolaşacak mal, hizmet ve işlemleri için siber güvenlik sertifikasyon sistemi oluşturulmuştur.

Avrupa Birliği'nde siber güvenliğe ilişkin böyle bir düzenleme olmasına rağmen; Türkiye'de spesifik bir siber güvenlik düzenlemesi bulunmamaktadır. Bu kapsamda ülkemizde siber güvenliğe ilişkin başlıca düzenlemeler şu aşamada 5809 sayılı Elektronik Haberleşme Kanunu ile Bakanlar Kurulu'nun 2012 tarihli Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar'dan ibarettir. Bu mevzuat kapsamında Siber Güvenlik Kurulu oluşturulmuş ve ülkemizde siber güvenliğe ilişkin çeşitli görevler Bilgi Teknolojileri ve İletişim Kurumu'na verilmiştir. Bunun yanında, Kişisel Verilerin Korunması Kanunu da siber güvenlik mevzuatı kapsamında sayılabilecek bir diğer düzenlemedir. Siber güvenliğe ilişkin yapılan açıklamalar ve eylem planlarında da bu konunun en kısa sürede regüle edilmesinin amaçlandığı anlaşılmaktadır.

Belirtmek gerekir ki, teknolojinin gelişme hızıyla orantılı olarak bilgi ve operasyon güvenliği konuları da ihlale ve zafiyete açık duruma gelmektedir. Siber güvenlik uzmanları 2019 yılında karşılaşılabilecek siber güvenlik tehditleri arasında kritik altyapı güvenliği, siber saldırılarda makine öğrenmesi ve yapay zekâ kullanımı, IoT riskleri gibi pek çok noktaya işaret ediyor. Bu sebeple şirketlerin olabildiğince hızlı şekilde sistemlerini güvenli hale getirmesi, bir denetim mekanizması olarak ISO 27001 gibi sertifikasyon süreçlerini gündemine alması ve riskleri tespit ederek gidermeye çalışması gün geçtikçe daha önemli hale geliyor. Bu öngörülerin gerçekleşmemesini umuyor olsak da teknolojiyle teması olan herkesin olası zarar ve kayıpları göz önünde bulundurarak siber güvenlik konusuna önem vermesi ve gerekli önlemleri alması en doğru yaklaşım olarak görünüyor.

Daha fazla bilgi için, contact@gokce.av.tr adresinden iletişime geçebilirsiniz.

DR. MEHMET BEDİİ KAYA İLE RÖPORTAJ

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü öğretim görevlilerinden Dr. Mehmet Bedii Kaya'ya siber güvenlik alanında merak edilenleri sorduk. Gerek Avrupa gerekse Türk hukuk dünyasında siber güvenlikle ilgili yoğun çalışmaları bulunan hocamızla gerçekleştirdiğimiz keyifli röportaja aşağıdan ulaşabilirsiniz.

1. Siber güvenlik hakkında bilgi sahibi olmayanlara siber güvenliği nasıl açıklarsınız?

Siber güvenlik çok farklı katman ve boyutları içermekte. Bu nedenle siber güvenliği steril ve basit bir şekilde izah etmek her zaman kolay olmuyor. Konuyu daha iyi ortaya koyabilmek için ufak bir analoji yapabiliriz. Nasıl ki kişisel güvenliğimiz kapsamında evimizin güvenliğine ve fiziksel güvenliğimize dikkat ediyorsak, siber güvenliğimiz de gerekli dikkat ve özeni göstermeliyiz. Bu kapsamda siber güvenliği, kullandığımız bütün bilişim sistemlerinin her seviyesinde güvenliğe dikkat etmek ve ilgili tedbirleri almak şeklinde açıklayabiliriz.

2. Toplumumuzun siber güvenlik algısını nasıl değerlendiriyorsunuz? Sizce mevzuatımız gereklilikleri karşılıyor mu?

Toplumumuzda siber güvenlik konusunda yeterli bir hassasiyet olduğunu söyleyebilmek gerçekten de zor. Gerçek kişi ya da şirketler, bir ihtilaf ya da sorunla karşılaşması, somut bir zararın meydana gelmesi halinde bir konuya hassasiyet duymaya başlıyor. Bu sebeple şirketlerin çoğunun siber güvenlik yatırımlarını ihmal ettiğini görüyoruz. Ancak somut bir ihlal yaşanıp gerçek bir zarar görüldükten sonra bu proaktifliği görebiliyoruz.

Siber güvenliğe ilişkin bu algı çeşitli mevzuatlarda yükümlülükler bulunmadığı anlamına da gelmiyor. Belirtmek gerekir ki siber güvenliğe ilişkin düzenlemelerin bulunmadığı bir dünyada dahi şirketlerin en önemli yükümlülüklerinden birinin bu güvenlik olduğunu malum, çünkü zaten sözleşme hukukundan kaynaklanan özen yükümlülükleri bulunuyor. Tüm bunlar birlikte değerlendirildiğinde, aslında konunun mevzuat ve hukuktan ziyade doğrudan bilinçle bağlantılı olduğunu görüyoruz. Siber güvenlik konusuna öncelik verilir, gerekli yatırımlar yapılır ve böylelikle bir farkındalık yaratılırsa; şirket bilgileri ve ticari sırlarının korunmasından rekabete kadar birçok alanda bu farkındalığın faydaları görülecektir.

3. Türkiye'deki kamu ve özel hukuk kişilerinin siber güvenlik farkındalığı hakkında ne düşünüyorsunuz?

Siber güvenlik çok dinamik bir alan, hızlı refleks gösterilmesi ve gerekli güncellemelerin yapılması gerekiyor. Bu sebeple her ne kadar çeşitli projeler ve düzenlemeler olsa da kamu siber güvenlik konusunda bir tık geride kalıyor ve kamunun hızı teknolojik gelişmenin hızına ayak uyduramıyor maalesef. Geleneksel kamu yönetim anlayışı nedeniyle bu ayak uyduramama durumuyla karşılaşıldığı kanaatindeyim. Özel hukuk kişileri, önceki soruda belirttiğim üzere, somut bir ihlal ve zarar yaşanmadığı sürece tepkilerin çok kısıtlı olduğunu ve dar bir çerçeveden bakıldığını görüyoruz. Bu noktada, siber güvenliğin genel bir refleks ve alışkanlıklarla bağlantılı hareket haline dönüşmesi gerektiğini vurgulamalıyız.

4. Siber güvenlik, kişisel verilerin korunması ve bilişim suçları arasındaki ilişki hukuken nasıl olmalı?

Aslına bakılırsa, kişisel verilerin korunmasına ilişkin düzenlemeler dar bir çerçevede de olsa bilgi güvenliği kapsamında siber güvenlikle ilgili çeşitli yükümlülükler getirdi. Türkiye'de siber güvenlik alanında asıl momentum bununla, kişisel verilerin korunmasına ilişkin düzenlemelerle yakalandı. Böylece bu konu daha da dinamik hale geldi ve kişisel veriler

Daha fazla bilgi için, contact@gokce.av.tr adresinden iletişime geçebilirsiniz.

adeta bu işin lokomotifi oldu. Belirtmek gerekir ki, kişisel verilere ilişkin uyumlaştırma süreçleri tamamlansa bile siber güvenlik anlamında tam bir uyum süreci yürütüldüğü düşünülmemelidir. Çünkü siber güvenlik daha kapsamlı bir bakış açısını ve bu sebeple daha geniş bir uyumluluk sürecini gerekli kılıyor.

5. Avrupa Parlamentosu tarafından onaylanan Siber Güvenlik Yasası'nı nasıl değerlendiriyorsunuz? Bizim mevzuatımız sizce bu gelişmeleri takip eder mi?

Avrupa'da bu konuda tedbirci bir uyum süreci olduğunu söyleyebiliriz. Yakın zamanda kişisel verilere ilişkin 1995 yılında yürürlüğe giren bir direktiften Avrupa Birliği Genel Veri Koruma Tüzüğü'ne (GDPR) geçiş yapan Avrupa, altyapılara ilişkin bir düzenleme olan NIS Direktifi'nden (Directive on Security of Network and Information Systems) yeni Siber Güvenlik Yasası'na doğru geçiyor. Türkiye de bu gelişmeleri yakından takip ediyor. Ülkemizde de Bilgi Toplumu Stratejileri belgelerinde ayrı bir siber güvenlik yasasının hazırlanması politik hedefler içerisine konulmuş durumda. Bu gibi düzenlemelerde her zaman paydaş katılımlı demokratik yöntemlerle geliştirilme ve Türkiye şartlarına uygun bir şekilde kademeli geçiş sürecinin öngörülmesi önemli oluyor, dolayısıyla böyle bir sistem kurgulanması gerekliliği es geçilmemeli.

6. Sizce yakın gelecekte siber güvenlik alanında hangi tehditler ön plana çıkacak?

Siber güvenlik tehditleri yavaş yavaş evrimleşmekte ve steril siber dünya aktörlerine nazaran hibrit aktörler karşımıza çıkmakta. Örneğin, gri şapkalı hackerı örnek alalım. Yakın zamanda Avrupa'da bir gri şapkalı hacker güvenlik açığını kapatarak binlerce bilişim sistemini daha güvenli hale getirdi. Yaptığı şey sistemlere girip sistemin açıklarını kapatmak. Aslında biraz garip gelebilir ama yapılan şey iyi niyetli. Ama günün sonunda bilişim sistemlerine girmiş, müdahalede bulunmuş oldu. Bunun yanında fidye yazılımları da farklı noktalara geldi. Yakın zamanda bir fidye yazılım vardı, dosyalarınızı elinde bulunduran hackerlar fidyenin serbest kalabilmesi için para istemiyor, tek bir şart var o da Youtube sayfalarının 100 milyon beğeniyi geçmesi. Bu sayı sağlanınca otomatik bot sayesinde fidye yazılımı dosyalarınızı serbest bırakıyor.

Siber güvenlik alanında her geçen gün yeni tehditleri, yeni nesil suçluları, yeni nesil Robin Hood'ları, meydan okuma ve ego savaşlarını gözlemlemek mümkün. Hacking yöntemlerinden birisi olan phishing'in (fişleme veya oltalama) artık yerini zıpkınlama olarak adlandırdığımız bir başka yönteme bıraktı. Fişleme denildiğinde ağ genel olarak atılıyor, ağa kim düşerse bu kişiler siber saldırıdan muzdarip oluyorlardı. Zıpkınlamada ise artık bir sektör hedef alınarak, onlara yönelik siber saldırıda bulunuluyor. Türkiye'de sanayi sektöründe olup yurtdışından ödeme alan ya da yapan şirketlerin muhasebe birimlerinin zaman zaman hedef alındığını görüyoruz. Bu şirketlerin hesapları manipüle edilerek (zıpkınlanarak) ödemeleri farklı kanallara yönlendiriliyor veya bir şekilde üst düzey yöneticiler hedef alınıyor. Bu gibi durumlar bir araya gelmesinin mümkün olmadığını düşündüğümüz örgütler, birimler veya yapıların bir araya gelerek iş ve amaç birlikteliği yapmasına sebebiyle veriyor. Dolayısıyla her geçen gün tehditlerin evrimleştiğini; genel nitelikli olmaktan ziyade kişiselleştiğini görüyoruz.

Daha fazla bilgi için, contact@gokce.av.tr adresinden iletişime geçebilirsiniz.

THE Fine PRINT
Gökçe
Mart 2019
78

Teori değil. Cevap.

Gökçe Avukatlık Ortaklığı

Editörler:

Assoc. Prof. Dr. Ali Paslı
ali.pasli@gokce.av.tr

Yağmur Yollu
yagmur.yollu@gokce.av.tr

Bahadır Bektaş
bahadir.bektas@gokce.av.tr

Ahmet Başaran
ahmet.basaran@gokce.av.tr

Dila Erol
dila.erol@gokce.av.tr

Fatih Ermiş
fatih.ermis@gokce.av.tr

Hakkımızda

Gökçe Avukatlık Ortaklığı birleşme ve devralma, iş ortaklığı, özel sermaye ve ortak girişim işlemleri, bankacılık ve finans, sermaye piyasaları, sigortacılık, teknoloji, medya, telekom ve internet, e-ticaret, veri koruma, fikri mülkiyet, regülasyon, ticari alacak takipleri, gayrimenkul ve ticari dava alanlarını içeren geniş bir yelpazede hukuki hizmetler sunan İstanbul'da bulunan bir hukuk bürosudur. Hukuki personel ve uzmanlığımız hakkında daha fazla bilgi için ***www.gokce.av.tr*** adresinden web sitemizi ziyaret edebilirsiniz.

Lütfen bizimle iletişime geçin
contact@gokce.av.tr
0 212 352 88 33

Daha fazla bilgi için, contact@gokce.av.tr adresinden iletişime geçebilirsiniz.