Deloitte.

Pandemi'den Kaçarken Doluya Tutulmak

Nisan 2020

Risk Advisory

Pandemi’den Kaçarken Doluya Tutulmak

Her geçen gün, COVID-19 ülkemizde ve dünyada yayıldıkça daha fazla şirket, çalışanlarını evden çalışmaya teşvik etmektedir. Dünya Sağlık Örgütü mevcut krizi “Pandemi” ilan ettiğinden, işyerleri ve okullar kapanmakta, bazı ülkelerde herkes için bazılarında ise belirli yaş grupları için sokağa çıkmama kuralları getirilmekte, herkese gerekmedikçe evinde kalması tavsiye edilmektedir. Uzaktan çalışma, çalışanlar ve şirketler için bir zorunluluk haline geldiğinden, belki de en çok zayıf noktalardan birisi de bilgi sistemleri riskleri değerlendirilmeden harekete geçilmesidir. Oysa her kriz bir fırsattır, siz de bu fırsatı şirketiniz genelinde bilgi sistemleri riskleri ve siber güvenlik bilincini artırmak için kullanabilirsiniz.

Ayrıca unutmayın, Dünya COVID-19'un sistemik tehdidine odaklanırken, bu krizi fırsata çevirmek isteyecek olan sadece siz değilsiniz. Dünyadaki siber suçlular da şüphesiz farklı bir “virüs” başlatarak krizden yararlanmaya çalışmaktadır. Bu çerçevede, hem işverenlerin hem de çalışanların şirket gizli bilgilerinin yanı sıra kendilerini de korumak için azami özen göstermeleri gerekmektedir. İşverenlerin ve çalışanların riski en aza indirgemek için akıllarında tutmaları gereken bazı temel şeyler bulunmaktadır. Giderek daha fazla sosyal uzaklaşma önlemi alındıkça, işverenler iş gücünü toplu olarak uzaktan çalışma modeline geçirmektedir. COVID-19 salgını sayısız zorlukla karşılaşmamıza sebep olurken, özellikle şirket çalışanlarının verimliliklerini korumak için gerekli araç ve sistemlerle donatmak, aslında o kadar keşfedilmiş bir bölge değildir.

Bugünün dünyasında, şirketinizin üretken ve rekabetçi kalmasını istiyorsanız, uzaktan çalışan personelin masalarından yapabilecekleri her şeyi yapabilmesi gerekir. Ancak, çalışanların yönetmediğiniz veya güvenmediğiniz makineler ve ağlardan kritik iş sistemlerine ve verilere erişmesine izin vermek, riskin katlanarak büyüdüğü anlamına gelir. Bu eşi benzeri görülmemiş bir zamanda güvenliği sürdürmek son derece önemlidir. Devlet kurumları ve şirketler hızla COVID-19'a uyum sağladıkça siber saldırıların da bu noktaya odaklanabileceğine dair kanıtlar gördük. Kötü amaçlı yazılım yüklü web sitelerinde bulunan COVID-19 bağlantıları, geçmişte katılmış olunan bir etkinlikte bir kişinin COVID-19 olabileceğini belirten bir e-posta, e-postada bireyin teşhisinin durumu hakkında güncel bilgi için bağlantılar, insanları resmi bir sağlık otoritesinden gelmiş gibi görünen, ancak gerçekten kötü amaçlı yazılım veya diğer zararlı kodlar içeren belgeleri indirmeye teşvik etme, yeni bir COVID-19 tedavisi hakkında bilgi edinmek için bir bağlantı içeren e-postalar, COVID-19 için sahte hayır kuruluşları veya yeni ortaya çıkan gruplar için bağış talepleri, sahte tedavi veya koruma bilgileri bunların örnekleri arasında yer almaktadır. Unutmayın, siber suçlular da her türlü krizi sever.

Şirket çalışanları, kablosuz ev ağlarına bağlanıyor veya güvenli olmayan genel kablosuz ağ kullanarak kurumsal hesaplarına erişiyor olabilir. Bu şekilde, kötü niyetli kişiler bağlantılarını kolayca gözetleyebilir ve gizli bilgileri toplayabilir. Örneğin, düz metin olarak şifrelenmemiş bir biçimde gönderilen veriler bu kişiler tarafından ele geçirilebilir ve çalınabilir. Bu nedenle, çalışanların güvenli uzaktan bağlantı yönetimi örneğin VPN bağlantısı kullanmadığı sürece bu tür bilgi aktarmalarına izin verilmemelidir. Uzaktan erişimin zorunlu olduğu hallerde çok bileşenli kimlik doğrulamaya dayanan güvenli bağlantı yöntemleri uygulanmalı, söz konusu bağlantının süresi ve bağlantının yapılabileceği cihazlar kısıtlanmalı ve kullanıcı belli aralıklarla kimliğini tekrar doğrulamaya zorlanmalıdır. Uzaktan çalışma yapılması gerekli olan her durumda, yalnızca güvenli, parola korumalı internet bağlantılarında çalışılması önerilmelidir. Herkese açık kablosuz ağ kullanılması gerekiyorsa, gizli veya hassas bilgilere erişmekten kaçınılmalıdır. Çalışanlara, sadece kurumsal bilgi güvenliği konusunda değil, evlerindeki kablosuz ağ şifrelerini nasıl güncelleyecekleri, minimum uzunluk, karmaşıklık gibi konularda ve açık kablosuz ağların kullanımı ile kullanım riskleri konusunda bilgilendirme yapılmalıdır.

Şirketler elbette çalışanlarının doğru olanı yapmalarına güvenirler. Ancak, sadece insanlara güvenmenin bir diğer sorunu da çalışanların bunu her zaman bilerek yapmamasıdır. Özellikle veri sızıntısı sorunları söz konusu olduğunda her zaman kasıtlı değildir. Çalışanlarınıza güvenebilirsiniz. Ancak, şirketin sağladığı araçlar, çalışanlara kullanım kolaylığı veya işlerini yapmak için ihtiyaç duydukları her şeyi sağlamadığında sorunun arttığını bilmek gerekir. Bu durumlarda, çalışanlar işlerini yapmanın başka yollarını bulacaklardır ve aslında kötü çalışan olmaya çalışmıyorlardır. Ancak bu durum şirketi daha fazla riske maruz bırakır.

Uzaktan çalışma için farklı kategoriler vardır. İlk olarak, şirket tarafından yönetilen kurumsal dizüstü bilgisayarlarla uzaktan çalışılabilir. Son yıllarda zamanda, çalışanların genellikle "Kendi Cihazınızı Getirin" (BYOD-Bring You Own Device) politikası olarak adlandırılan kişisel cihazlarını iş amaçlı kullanmalarına izin verme eğilimi de ortaya çıkmıştır. İşle ilgili konularda kişisel cihazlarını kullanan çalışanların ilgilendiği sorunların tamamen farkında olunması gerekir. Örneğin, aniden şirketten ayrılabilir ve istihdamları sırasında cihazlarında saklanan gizli bilgileri tutabilirler ve Şirketin bunu silme şansı olmayabilir. Dahası, çalışanların kendi cihazlarında yazılımlarını güncel tutmayabilirler, bu da Şirket bilgileri açısından güvenlik açıklarına sebep olabilir. Veri barındıran medya ya da cihazların kullanımdan kaldırılması durumunda, içerdikleri bilgilerin gizlilik derecesine uygun olarak güvenli bir şekilde imha edilmesi sağlanmalıdır. Çalışanlara, ofisteymiş gibi, bilgilerin aynı gizlilik derecesinde olduğu hatırlatılmalıdır. Kişisel e-postalar herhangi bir şirket işi için kullanılmamalıdır ve çalışanların evdeki yazıcıları kullanımı sınırlandırılmalı, yazıcılarda yazdırdıkları takip edilebilmelidir. Yazdırılan belge ofis ortamında parçalanmaya maruz kalacaksa, aynı belgeyi evde ayırmaya ve parçalamaya dikkat edilmeli veya daha ilk aşamada yazdırmaktan kaçınılmalıdır.

Yazılım yamalarını zamanında uygulama hala çok önemli bir bilgi sistemleri kontrolüdür. Esas olarak, çalışanların kişisel cihazlarını iş amaçlı kullanmalarına izin verilmemesini tavsiye etmekle birlikte, önemli bir iş ihtiyacı olması halinde de en azından MDM (Mobile Device Management) uygulamaları ile riskler azaltılmalıdır. Peki, ağınıza erişmek için kullanılan cihazlar tam olarak kontrol edilemediğinde şirketler özel verilerini nasıl koruyabilir? Uzaktan çalışmanın güvenli olduğundan emin olmak için nereden başlanmalıdır? İlk adım, özellikle uzaktan çalışanlar için tasarlanmış bir güvenlik politikası oluşturmaktır. Bugün pek çok şirketin hâlihazırda resmi bir uzaktan çalışma politikası bulunmamaktadır. Hangi rollerin uzaktan çalışma için uygun olduğu açıkça tanımlanmalıdır. Çalışanlara karşı şeffaf olunmalı, hangi rollerin uzaktan çalışmasına izin verildiğini ve hangilerinin bilgi sistemi risklerini yönetmek nedeniyle olduğu bilinmelidir.

Ne yazık ki, her pozisyon uzaktan çalışma için uygun değildir. Bir rehber yoksa uzaktan çalışma onaylarının haksız olarak değerlendirilme olasılığı bulunmaktadır ve bu da suistimal riskini artırmaktadır. Çalışanlara şirket tarafından verilen dizüstü bilgisayarları kullanmaları veya kullandıkları kendilerine ait cihazdan emin olmadıkları takdirde bilgi güvenliği personeline başvurmaları istenmelidir. Kişisel cihazların kullanımı, şirket bilgilerinin korunmasında sorunlar yaratmakta ve risk artışı sağlamaktadır. Hiçbir şirket kasıtlı veya kasıtsız olarak veri sızıntısı istemez. Ancak çalışanlar genellikle işlerini basit bir şekilde yapmak için riskli davranışlarda bulunabilirler - örneğin, bir ev bilgisayarında daha kolay düzenleme veya yazdırma için ekli kurumsal e-postaları kişisel bir e-posta hesabına iletebilirler. Artık bu eklenti, kötü amaçlı yazılım bulaşabilecek kişisel bir bilgisayarda açıkta durmaktadır.

Bilgi sistemleri riskleri odak noktamız olduğundan, şirket hassas bilgileri söz konusu olduğunda fiziksel güvenliği tamamen geride bırakamayız. Örneğin, halka açık yerlerde çalışırken yüksek sesle konuşan, dizüstü bilgisayarlarının ekranını bir kafenin içindeki tüm kalabalığa maruz bırakan ve cihazlarını gözetimsiz bırakan çok sayıda çalışan olduğu herkes tarafından gözlemlenmektedir. Bu sebeple, hiçbir işlem yapılmayan hareketsiz oturumlar için sisteme erişim belirli bir süre sonra sonlandırılmalıdır. Uzaktan çalışma, cihazlarınızın kaybolması veya çalınması olasılığını artırır. Suistimal riskini en aza indirmek için kaybolan veya çalınan her cihazı derhal şirket bilgi güvenliği personeline bildirilmesi gerekliliği anımsatılmalıdır. Pandemi nedeniyle herkes el yıkama düzenini kontrol ederken, çalışanlara kurumsal riskleri yönetmek için en iyi uygulamaları hatırlatmak önemlidir. Bu ortamlarda kaybedilen veya çalınan kurumsal cihazlar için, veri sızıntısını önlemek amacıyla disk şifreleme yöntemleri mutlaka kullanılmalıdır.

Bilgi sistemleri risklerinin yönetilmesinin temel ilkelerinden birisi de verilerin bütünlüğünü korumaktır. Sadece bilgilerin çalınabilmesi değil, değiştirilebilmesi de önemlidir. Ayrıca, IoT'ye (nesnelerin interneti) girdiğinizde artık veri toplayan cihazlarınız da önem kazanır. Yalnızca aktarılan veya son noktadaki verileri korumak yeterli değildir, toplanan verilerin de gerçekten doğru olması ve bütünlüğünü de koruyabilmesi için cihazın kendisini de korumalısınız. Uzaktan çalışanlar için, kötü amaçlı yazılımların ve saldırganların verileri çalamamasının yanı sıra değiştirememeleri için son noktanın tamamen korunduğundan emin olmalısınız. Tüm şirketler, verilerin korunmasının, verilerin bütünlüğünü korumak anlamına da geldiğinin farkında olmalıdır.

Kurumsal sistemlerde, kullanıcı hesaplarının güçlü parolalarla korunmasını sağlamak her zamanki gibi önemlidir. Ne yazık ki, birçok kişi birden fazla hesapta aynı şifreyi kullanmaya devam etmektedir. Hatta şirket içi sistemlerde kullanılan parolaların pek çoğu aynı zamanda özel amaçla da güvenilir olmayan web sitelerinde kullanılmaktadır. Tüm kurumsal sistemlerde parolalar her hesap için benzersiz olmalı ve yeterince uzun ve küçük harfler, sayılar ve özel karakterler içeren bir dizeden oluşmalıdır. Uzaktan çalışma konusundaki yoğunluk sürdükçe, potansiyel risklerin artması sebebiyle, kurumsal sistemlerde şifre değiştirme sıklığının artırılması düşünülmelidir. Sistemlere başarısız erişim teşebbüslerinin belirli bir sayıyı aşması halinde ise ilgili kullanıcının erişimi bloke edilmeli, bu teşebbüsü gerçekleştiren kişiye, hatalı girilen kullanıcı adı bilgisi veya parola ile ilgili, böyle bir kullanıcı adının sistemde olmadığı veya parolanın hatalı girildiği gibi gereksiz bilgi verilmemelidir. Uzaktan çalışma koşullarında, unutulan parolalar sebebiyle yeni parola tanımlanması süreçlerinde normal çalışma düzenindeki güven unsuru yerine sistemsel kontroller ile parolaların sıfırlanması temin edilebilmelidir. Şirket tarafından, tüm kurumsal bilgilere olan erişimlerin, görevler ayrılığı prensibine göre belirlenmiş kullanıcılar tarafından ve bu kişilerin sorumluluğu gereği kendileri için tanımlanan erişim kontrolleri uyarınca gerçekleştirilmesi sağlanmalıdır.

Sistemlere izinsiz erişimlerde en çok faydalanılan olanaklardan birisi de ayrıcalıklı yetkilere sahip kullanıcı ve uygulama hesaplarıdır. Bu sebeple ayrıcalıklı yetkilere sahip kullanıcılar için çok bileşenli kimlik doğrulama uygulanmalı, ayrıcalıklı yetkilere sahip kullanıcı ve uygulama hesaplarının sayısı kısıtlanmalı ve yalnızca gerekli olan kullanıcılara bu yetkiler atanmalı ve sadece gerekli olan durumlarda bu hesaplar kullanılmalıdır. Bu tür hesaplar ile gerçekleştirilen işlemleri daha yakından takip edecek şekilde logların tutulması ve bunların düzenli olarak gözden geçirilmesi önerilir. Şirket içinde kullanılan sistemlerde ayrıcalıklı yetkilere sahip bir kullanıcı hesabı oluşturulduğunda veya silindiğinde bu tür işlemler için uyarı üretilebilir. Ayrıcalıklı yetkilere sahip kullanıcı hesaplarının parolaları güvenli ortamlarda saklanmalı ve bu parolaların belirli sıklıkta değiştirilmesini sağlayacak düzenlemeler yapılmalı, ayrıcalıklı yetkilere sahip uygulama hesaplarına ilişkin parolaların tahmin edilmesi zor ve günün teknolojisine uygun uzunluk ve zorlukta olacak şekilde sıklıkla değiştirilmelidir. Günümüzün koşullarında olduğu gibi, Şirket yetkili çalışanlarının uzaktan çalışması gerektiği ortamlarda, acil durumlara özgü yetkilendirmeler geçici olarak yapılmasına gerek duyulabilir. Bu sebeple bu geçici durumu takip edebilecek, acil durum ortandan kalktığında yetkinin de kaldırılmasını sağlayabilecek ve bu yetkilendirme süresince gerçekleştirilecek işlemlerin takibine imkân verecek logların tutulmasını sağlayacak süreçler ve teknik olanaklara sahip olunmalıdır.

Şirketler, her türlü cihazlar ve sunucuları üzerindeki işletim sistemi, veritabanları ve uygulamalar ile güvenlik duvarları, yönlendirici ve anahtarlama cihazları gibi tüm ağ cihazları için sıkılaştırılmış ve test edilmiş güvenli standartları oluşturmalıdır. Bu çerçevede güvenli standartlar dışında kalacak her türlü değişiklik isteği için bu değişikliği gerektiren iş gereksinimi ve bu iş gereksinimine ihtiyaç duyan iş sorumlusunun kim olduğu ve gereksinim süresi gibi bilgiler de kayıt altına alınmalıdır. Kullanıcıların kullanmaları gereken araçlar ve platformlar listelenmelidir. Hem uzak hem de yakın çalışanlar için bulut depolama platformları, iletişim / video konferans araçları, proje yönetim araçları gibi aynı onaylanmış araçlar kullanmalıdır. Böylelikle yalnızca ihtiyaç duyulan uygulamaların sistemlerde yüklü olması ve bu liste dışındaki herhangi bir uygulamanın sistemlere yüklenmesi veya çalıştırılmasının engellenmesi sağlanmalıdır. Şirket aynı zamanda, sistemleri üzerinde listede yer almayan herhangi bir uygulamanın yüklü olup olmadığına yönelik düzenli olarak tarama gerçekleştirmelidir. Zorunlu bir iş gereksinimi olmadıkça ve ilgili Şirket yetkilisi tarafından onaylanmadıkça Şirket personelinin ya da dış hizmet sağlayıcıların kullandıkları cihazda yerel yönetici haklarına sahip olması engellenmelidir. Bu sayede olası güvenlik açıklarının oluşması, uygulama güncellemelerinin veya düzenli antivirüs taramasının engellenmesi gibi kullanıcı yetkileri de kısıtlanmış olacaktır.

Şirket, tüm masaüstü, dizüstü ve iş istasyonu makineleri ile sunucularını, sürekli bir şekilde izleyerek üzerindeki zararlı yazılımları tespit edecek etkin araçları kullanmalıdır. Şirketin tüm uç nokta cihazlar ile sunucular, bu makinelere taşınabilir bir medya veya harici cihaz takıldığında otomatik olarak içeriği oynatmayacak şekilde yapılandırılmalı ve zararlı yazılım engelleme araçları bu tür cihazlar takıldığında otomatik olarak bu cihazları tarayacak şekilde ayarlanmalıdır. Şirketler, sistem, yazılım ve cihazlardaki güvenlik açıklarını hızlı ve etkin bir şekilde ele alacak bir yama yönetimi süreci tesis etmelidir. Tespit edilen yamaları uygulamanın ya da uygulamamanın etkisinin değerlendirilmesi, uygulanacak yamaların uygulama öncesi test edilmesi, uygulanamayan yamaların gidermeye çalıştığı güvenlik açıklarına ilişkin riskleri azaltmaya yönelik telafi edici kontrollerin tesis edilmesi gibi bilgi sistemleri kontrolleri uygulanmalıdır.

Bilgi sistemlerinde bulunan bilgiler insan hatası, donanıma fiziksel hasar veya siber saldırı da dâhil olmak üzere çeşitli şekillerde kaybedilebilir. Fidye ve diğer kötü amaçlı yazılım türleri, tespit etme şansı olmadan tüm sistemleri silebilir. Açıkçası, bilgileri yedeklemenin birçok nedeni vardır. Her şirket, tüm sistemin veya faaliyetlerinin önemli bir bölümünün çalışamaz hale gelmesini önlemek adına kritik donanım ve sistemler için yedekli çalışır ya da hazırda bekleme düzenleri kurar. Bir sistemin alınan yedeğinden geri yüklenebilmesi için, işletim sistemi, yazılımı ve veriler gibi sistemin çalışmasını sağlayan tüm bileşenler yedeklemeye dâhil edilmelidir. Yedeklemenin düzgün bir şekilde çalıştığından emin olmak için, veri geri yükleme testleri gerçekleştirilmesi önemli bilgi sistemleri kontrollerindedir. Ayrıca yedeklerin, siber suçluların sistem bilgilerine erişebilmesi olasılığına karşı farklı bir donanım veya medya üzerinde bulunması sağlanmalıdır.

Şirketin büyüklüğü bilgi sistemleri risklerine hazırlığı ve siber güvenliğe karşı bir plan geliştirmesi açısından önemli değildir. Aradaki fark, büyük bir şirketin siber güvenliğe adanmış bütün bir ekibe sahip olması ve onlara yardım etmek için çalışan danışmanları olması olabilir. Organizasyon büyüklüğünden bağımsız olarak, siber güvenlik planlaması ve müdahale hazırlığı kritiktir. İyi bir bilgi sistemleri risk yönetimi ve siber güvenlik süreci ile ilgili temel şeyler yalnızca kaynaklar veya ekiple ilgili değildir. Riski yönetmek ve siber güvenlik herkesin işidir. Örneğin bir aile şirketinde, veritabanı uzmanı varsa, siber güvenlik için oynayacakları bir rolleri vardır. Yalnızca bilgi sistemleri bölümünde değil, şirketteki herkesin siber güvenlik alanında oynayacağı bir rol vardır. Herkesin bilgi sistemleri risklerinin farkında olması gerekir. Kimlik avı nasıl anlaşılır? Kötü bir şeylerin gerçekleştiğini düşünürsem, bu tür olayları bildirmek için kimi ararım? Diğer yandan, bildirimi yeni almış olan yetkili personelin durumu ele almak için bir planı olmalıdır. Bu plan geliştirilmeli, test edilmeli, böylece gerçek bir olay olduğunda, kimse ne yapılması gerektiğini merak etmemelidir. Günümüz koşullarının farklı çalışma yöntemlerini zorunlu kıldığı düşünüldüğünde, Şirket genelinde siber güvenlik farkındalık seviyesini artırmak için bir siber güvenlik farkındalık programı oluşturulmalıdır.

Program, bilgi güvenliği politikaları ve standartları ile birlikte, bilgi güvenliği konusundaki bireysel sorumlulukların neler olabileceği ve bilgi varlıklarını korumak için alınması gereken önlemler hakkında bilgi içermeli ve bu bilgilendirmeler yoluyla Şirketin bilgi sistemlerine erişimi olan herkesin bu kaynakların kullanımı ile ilgili mevzuat ve yönergeler hakkında bilgi sahibi olması sağlanmalıdır. Bu doğrultuda, siber güvenlik ile ilgili düzenli olarak Şirket içi bültenler hazırlanabilir, çalışanlara düzenli olarak bilgi güvenliğiyle ilgili hatırlatma e-postaları gönderilebilir, çalışanların kişisel işlerinde kullandıkları parolaları, Şirketin iş süreçlerinde kullanmamaları gerektiği konusunda bilgilendirilebilir, siber güvenlikle ilgili ekran koruyucuların ve arka plan resimleri oluşturulabilir, çalışanlara yönelik düzenli olarak siber güvenlik farkındalığını ölçecek anketler yapılabilir. Şirketlerin bünyesinde bilgi sistemleri risklerinin azaltılmasında nihai sorumluluk yönetim kurullarındadır. Yönetim kurulu, bilgi sistemlerine ilişkin önlemlerin uygun düzeye getirilmesi hususunda gerekli kararlılığı göstermeli ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis etmelidir.

Şirketler, bilgi sistemleri yönetimini kurumsal yönetim uygulamalarının bir parçası olarak ele almalı, bilgi sistemlerinin doğru yönetimi için gerekli finansman ve insan kaynağını tahsis etmeli, bilgi varlıklarının güvenliği, gizliliği, bütünlüğü ve erişilebilirliğini sağlamak amacıyla bilgi sistemleri üzerinde etkin kontrollerin tesis edilmesini sağlamalı ve bilgi sistemlerinin kullanımından kaynaklanan risklerin yönetilmesi için etkin bir gözetim yürütmelidir. Bilgi sistemlerinin kullanımından kaynaklanan riskleri yönetmek ve bilgi varlıklarını korumak amacıyla uygulanması gereken usul ve esaslar ile tesis edilmesi gereken kontrolleri tarif eden BS politika, prosedür ve süreç dokümanları oluşturulmalıdır. Alınan tüm önlemlerin beklenilen faydayı sağlayıp sağlamadığı da düzenli olarak bilgi sistemleri denetim ekipleri tarafından kontrol edilmelidir.

Dünya tarihinin en farklı günlerini yaşadığımız şu dönemde herkese sağlıklı günler dilerken, her şirketin de sağlıklı bir bilgi sistemi ortamına sahip olmasını dilerim.

İletişim:

Barış Bağcı
Ortak
Risk Danışmanlığı
bbagci@deloitte.com

Deloitte.

Deloitte Türkiye

İstanbul Ofis
Deloitte Values House
Eski Büyükdere Caddesi
Maslak No:1
Sarıyer, İstanbul
+90 (212) 366 60 00

Ankara Ofis
Armada İş Merkezi
A Blok Kat:17 No:27-28
06510
Söğütözü, Ankara
+90 (312) 295 47 00

İzmir Ofis
Punta Plaza
1456 Sokak
No:10/1 Kat:12
Daire:14-15
Alsancak, İzmir
+90 (232) 464 70 64

Bursa Ofis
Zeno Center İş Merkezi
Odunluk Mahallesi
Kale Caddesi
No:10 D Blok Kat:5
Nilüfer, Bursa
+90 (224) 324 25 00

Çukurova Ofis
Günep Panorama İş Merkezi
Reşatbey Mahallesi
Türkkuşu Caddesi
No:1 B Blok Kat:7
Seyhan, Çukurova, Adana
+90 (322) 237 11 00

www.deloitte.com.tr

@deloitteturkiye **@deloitteturkiye** **@deloitteturkiye**

@deloitteturkey **@deloitteturkey** **@deloitteturkey**