Gizliliğe ve Mahremiyete ilişkin Türkiye Gereklilikleri Işığında

Uyumluluk: Microsoft Azure

Yasal Uyarı

Yayın Tarihi: Ekim 2016

İşbu doküman sadece bilgilendirme amacı gütmektedir. MICROSOFT BU BELGEDEKİ BİLGİLERE DAİR SARİH, ZIMNİ VEYA YASAL HİÇBİR TAAHHÜTTE BULUNMAMAKTADIR.

İşbu doküman "olduğu gibi" sağlanmaktadır. URL ve diğer İnternet web sitesi referansları dahil dokümanda ifade edilen bilgiler ve görüşler, önceden bir bildirimde bulunmaksızın değiştirilebilir. İşbu dokümanı dikkate alan müşteriler, kullanıma ilişkin riskleri üstlenmektedir.

İşbu doküman, herhangi bir Microsoft ürünündeki herhangi bir fikri mülkiyet için müşterilere herhangi bir hak sağlamaz. Müşteriler, referans amacıyla bu dokümanı kurum içinde kopyalayabilir ve kullanabilir.

İşbu dokümanda yer alan bilgiler, hukuki görüş ve/veya mütalaa olarak değerlendirilmemelidir. Müşteriler, kendi organizasyonlarını etkileyebilecek yasal gerekliliklere uyum konusunda tavsiye edinmek üzere kendi hukuk danışmanlarından görüş almalıdır.

Burada belirtilen bazı örnekler yalnızca açıklama amaçlıdır ve kurgusaldır. Gerçek bir ilişki ya da bağlantı amaçlanmamış olup, bu şekilde görülenler tamamen tesadüfidir.

NOT: İşbu dokümandaki bazı öneriler veri, ağ ya da bilişim kaynaklarının kullanımının arttırılmasıyla sonuçlanabilir ve bir müşterinin lisans veya abonelik maliyetlerini arttırabilir.

Hedef kitle

Bu teknik inceleme, Türkiye'de Bilişim Teknolojileri alanında karar verici konumunda olan kişiler için hazırlanmış olup bu kişilere, Microsoft Azure'un ilgili ülkelerdeki uyumluluk, güvenlik ve mahremiyet gereksinimlerini karşılamak konusunda kendilerine nasıl yardımcı olabileceği hakkında bilgiler sağlamaktadır.

Yönetici Özeti

Microsoft Azure, Microsoft müşterilerine bulut bilgi işlemin avantajlarını gerçekleştirme imkanı veren, bulut tabanlı güvenilir bir platformdur. İşbu doküman, buluta geçiş yapmayı düşünen Türkiye'deki müşteriler tarafından yöneltilen soruları yanıtlamayı amaçlamaktadır. Buluttaki veriler ne kadar güvenli, veriler nerede depolanır, nasıl kullanılır ve kimler erişebilir gibi sorular yaygın olarak sorulan sorular arasındadır. Bu tür sorular genellikle şu üç alandan biri ile ilgilidir: uyumluluk, güvenlik ve mahremiyet.

Uyumluluk konusunda endişesi olan müşteriler için Microsoft Azure'un, 07 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ile yürürlüğe giren düzenlemelere aykırı bir çözüm olmadığını ve ISO 27001, ISO 27018 ve AB Model Maddeleri gibi güvenliğe ve gizliliğe ilişkin uluslararası standartlara ve bunlarla ilgili sertifikalara sahip olduğunu belirtmek gerekir. Bu uyumluluk, hem kamu kurumlarının hem de ticari kurumların, Kanun ile kendilerine yüklenen sorumlulukları yerine getirdikleri sürece, verilerini buluta yüklemeleri ile birlikte Kanun'a ve uluslararası standartlara uyumlu bir çözüm kullandıklarını bilmenin güveniyle hareket edebilecekleri anlamına gelir.

Güvenlik, buluta geçiş yapmayı değerlendiren müşteriler için birincil odak noktasıdır. Microsoft Azure, fiziksel izinsiz giriş, elektrik kesintisi ve ağ kesintilerine karşı veri merkezlerinin bulunduğu lokasyonlarda sağladığı fiziksel koruma ile birlikte birden çok seviyede güvenlik sağlar. Azure, aktarılmakta olan ve durağan konumdaki verileri korumak için şifreleme yöntemini kullanır ve kapsamlı izleme ve günlüğe kaydetme özellikleri ile ilgili görevli personel ve müşteriler için ortam görünürlüğü sağlar. Microsoft, Azure'u Microsoft Security Development Lifecycle (SDL), Microsoft Operational Security Assurance (OSA) gibi programlar ile somutlaşan en iyi güvenlik uygulamalarını ve "assume breach" adı verilen ihlal varsayım stratejisini kullanarak tasarlar ve işletir. Bu programlar ve stratejiler, Azure'un saldırılar karşısında dayanıklı olmasını sağlamaya yardımcı olur. Microsoft, bu yaklaşımın faydalarını doğrular nitelikte olan ISO 27001 güvenlik sertifikasını almıştır.

Bulutun global yapısı nedeniyle müşteriler, mahremiyetlerinin güvence altında olduğunu bilmek ister. Microsoft Azure, ISO 27018 gibi mahremiyete ilişkin oldukça katı standartlar belirleyerek uygulamaya alır ve müşteri verilerinin reklam amaçlı veya ticari amaçlar için kullanılmaması da dahil pek çok konuda müşterilere güvence verir. Müşterilerin veri bütünlüğü konusunda kaygıları olması durumunda Azure, müşterilerinin Asya, Amerika ve Avrupa'daki 26 Azure bölgesi arasından seçim yapmalarına izin vererek verilerin bulunduğu lokasyon üzerinde tam kontrol imkanı sağlar. Buna ek olarak Microsoft, herhangi bir üçüncü tarafın müşteri verilerine doğrudan veya sınırsız erişimine olanak sağlamaz[1] ve kamu kurumlarının müşteri verileri ile ilgili taleplerini her zaman müşteriye yönlendirmeye çalışır. Son olarak, kullanıcı yalıtımı ve sıkı erişim denetimleri, yalnızca müşterilerin verilere "varsayılan" olarak erişebilmesini sağlamaya yardımcı olur.
Microsoft Azure, Türkiye tarafından tanımlanan uyumluluk, güvenlik ve mahremiyet kurallarının birçoğunu karşılıyor olsa da, yönetici parolalarının denetimi gibi bir takım gereksinimler müşterinin sorumluluğundadır ve müşterilerin Microsoft Azure ile ilişkili ortak sorumlulukları anlamaları oldukça önemlidir.

[1] https://www.microsoft.com/en-us/TrustCenter/Privacy/You-own-your-data#subcontractors

İçindekiler

Giriş

İşbu doküman, verilerini Microsoft Azure'a taşıma konusunu değerlendiren, Türkiye'de Bilişim Teknolojileri alanında karar verici konumunda olan kişiler için hazırlanmıştır ve sıkça sorulan bazı soruların yanıtlarına yer vermektedir:

- Microsoft Azure, Türkiye'ye ilişkin uyumluluk gereksinimlerini karşılıyor mu?
- Veriler nerede depolanır ve bunlara kimler erişebilir?
- Microsoft verileri korumak için ne yapıyor?
- Müşteriler Microsoft'un yaptığını söylediği uygulamaları hayata geçirdiğini nasıl doğrulayabilir?

İçerik üç ana bölüme ayrılmıştır:

- *Türkiye uyumluluk gereksinimleri.* Bu bölümde Azure'un, mevzuatta öngörülen hususları ve uluslararası sertifikalara ilişkin gereklilikleri nasıl karşıladığı belirtilmiştir.
- *Temel güvenlik ilkeleri.* Bu bölümde Azure'un, şifreleme ve en iyi güvenlik uygulamaları gibi temel güvenlik ilkelerini, Türkiye'de bulunan müşterilere nasıl sağladığı ile ilgili teknik bilgiler sağlanmıştır.
- *Temel mahremiyet ilkeleri.* Bu bölümde Azure'un, veri konumu ve resmi istekler gibi temel mahremiyet ilkelerini, Türkiye'de bulunan müşterilere nasıl sağladığı ile ilgili teknik bilgiler sağlanmıştır.

Azure'un Türkiye'deki güvenlik ve mahremiyet gereksinimlerini karşılamak üzere müşterilerle sorumlulukları nasıl paylaştığını anlamak, verileri buluta taşıma yönünde atılacak önemli bir adımdır.

Microsoft ve müşteriler arasında paylaşılan sorumluluklar

Verileri buluta taşırken, güvenliğe ve mahremiyete ilişkin birtakım gerekliliklerinin müşterinin sorumluluğunda olduğunu, bazılarının ortaklaşa üstlenildiğini ve bazılarının da bulut hizmeti sağlayıcısının (CSP) sorumluluğunda olduğunu anlamak önemlidir. Her bir bulut tabanlı çözüme dair sorumluluklar hakkında daha fazla bilgi almak için lütfen Bulut bilişim çözümlerinde paylaşımlı sorumluluk adlı dokümanı inceleyiniz.

1. Türkiye uyumluluk gereksinimleri

Kişisel Verileri Koruma Kanunu

6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") Türkiye'de ilk defa 2007 yılında Avrupa Birliği ile uyum kapsamında hazırlanmış ancak aradan geçen 9 yıl boyunca çeşitli sebeplerle yasalaşma süreci tamamlanamamıştır. Konunun artan önemi dolayısıyla 64. Hükümet Programı ve 64. Hükümet Eylem Planı kapsamında söz konusu kanunun 2016 yılının ilk çeyreğinde yasalaşması öngörülmüştür. Bu kapsamda Kanun, önceki metinler üzerinde yapılan çeşitli değişikliklerle 18 Ocak 2016 tarihinde TBMM Başkanlığı'na sevk edilmiştir. Kanun 24 Mart 2016 tarihinde TBMM Genel Kurulu tarafından kabul ederek yasalaşmış ve 7 Nisan 2016 tarihinde Resmî Gazete'de yayımlanarak yürürlüğe girmiştir.

Kanun genel olarak kişisel verilerin işlenmesine ilişkin kuralları düzenlemektedir. Kişisel verilerin işlenmesi ise verilerin elde edilmesi, kaydedilmesi, depolanması, değiştirilmesi, üçüncü kişilerle paylaşılması,

yurtdışına transfer edilmesi de dahil olmak üzere kişisel veriler üzerinde gerçekleştirilen her türlü işlemi ifade etmektedir.

Kanun ile uyumlu bir veri işleme döngüsüne sahip olabilmek Kanunda düzenlenen para cezaları ve hapis cezaları ile karşılaşmamak açısından önem taşıdığı gibi, verilerin üçüncü kişilere veya yurt dışına transfer edilebilmesi açısından da bir zorunluluk olarak karşımıza çıkmaktadır. Verilerin üçüncü kişilere veya yurtdışına hukuka uygun biçimde transfer edilebilmesi, sadece Kanunda öngörülen kurallara uygun olarak gerçekleştirilebilecektir.

Kanun kapsamında veri sorumluları, ayrıca verilerin hukuka aykırı olarak işlenmesini önlemek ve veri güvenliğini sağlamak için gereken tüm teknik tedbirleri almakla sorumludurlar. Hatta veri işlemenin başkasına yaptırılıyor olması durumunda dahi veri sorumlularının bu tedbirlerin alınmasını sağlamak ve gerekli denetimleri yapmak yükümlülüğü devam etmektedir. Belirtilen yükümlülüklere, verisi işlenen kişinin bilgilendirilmesi yükümlülüğü de dâhildir. Verileri işlenen ilgili kişinin, Kanun'un uygulanması ile ilgili tüm taleplerini iletebileceği bir şikâyet mekanizması kurulması ve ilgili taleplerin en geç 30 gün içerisinde sonuçlandırılması gerekmektedir.

Yukarıda sayılan tüm uyum faaliyetlerinin yerine getirilebilmesi için Kanunda bir geçiş dönemi öngörülmektedir. Kanun'un yasalaşmasından önce işlenen verilerin Kanun ile uyumlu hale getirilmesi için iki yıllık bir geçiş süreci bulunmaktadır. Fakat verilerin Kanun'da belirtilen kurallara uygun olarak işlenmesi yükümlülüğü, Kanun'un yasalaşması ile yürürlüğe girmektedir. Suç ve kabahatlere ilişkin düzenlemelerin ise Kanun'un yasalaşmasından itibaren 6 ay (7 Ekim 2016) içerisinde yürürlüğü girmesi öngörülmüştür.

Kanun Neyi Düzenliyor?

Kişisel verilerin elde edilmesi, kaydedilmesi, depolanması, 3. kişilere veya yurtdışına aktarılması da dahil veriler üzerinde gerçekleştirilen her türlü işlemi düzenlemektedir.

Kanun Neden Önemli?

Kişisel verilerin işlenmesinde yeni bir çağın başlangıcı olarak kabul edilmektedir. Milyonlarca verinin artık Kanun'da düzenlenen rejime uygun olarak işlenmesi gerekmektedir.

Kanun Kimleri Kapsıyor?

Kişisel veri işleyen tüm gerçek ve tüzel kişiler ile kişisel verileri işlenen gerçek kişileri kapsamaktadır. Kanun istisnalara da yer vermektedir.

Yaptırımlar Neler?

1 yıldan 4 yıla kadar hapis cezası ve ayrıca 1.000.000-TL'ye varan idari para cezaları öngörülmektedir.

Hangi Kurum?

Kanun, 200'e yakın personeli olan Kişisel Verileri Koruma Kurumu kurulmasını öngörmektedir. Kurum Kanun ile uyumluluğu sağlamakla ve gerekli tedbirleri almakla yükümlüdür.

Nasıl Etkiler?

Kanun ile iş yapış süreçlerinin değişeceği; yeni iş süreçlerinin geliştirileceği öngörülmektedir. Etkili bir veri koruma programını benimsemenin yeterli olmayacağı, organizasyon kültürünün değiştirilmesi gerektiği vurgulanmaktadır.

Microsoft Azure uyumluluğu

Kanun, kişisel verilerin yurtdışına aktarılmasını yasaklamamakta; yalnızca kişisel verilerin üçüncü kişilere ve/veya yurtdışına aktarılması noktasında uyulması ve yerine getirilmesi gereken kuralları belirlemektedir. Her koşulda regüle sektörlerde faaliyet gösteren müşterilerin bu sektörlerin tabi olduğu kanun ve düzenlemelere de uyumlu hareket etmeleri gerekmektedir.

Kanun, kişisel verileri işleyen "veri sorumluları"nın, söz konusu faaliyeti hukuka ve amaca uygun bir biçimde yerine getirmeleri, işlenen verilerin korunması noktasında gerekli güvenlik tedbirlerini almaları ve verilerin mahremiyetini sağlamaları gerektiğini belirtmektedir.

Microsoft, son 1 yıl içerisinde güvenlik alanında yaklaşık 1 milyar dolar tutarında yatırım yapmıştır ve önümüzdeki dönemde yapmaya da devam edecektir. Bu yatırımlar, Microsoft Azure'un daha güvenli bir platform haline gelmesinde büyük bir rol oynamaktadır. Güvenlik ile ilgili detaylara işbu dokümanın devamında yer veriyor olacağız. Dilerseniz her daim Azure Güven Merkezi'ni de ziyaret edebilirsiniz.

Kişisel verilerin hukuka ve amaca uygun işlenmesi, kişisel verileri işleyen veri sorumlularının uymakla yükümlü olduğu bir diğer unsurdur. Bu noktada veri sorumluları Microsoft Azure'u kullanarak, bu platformun kullanıcılara sağladığı avantajlardan yararlanmış olurlar. Bu avantajlar: (i) Şeffaflık, (ii) Avrupa Birliği 29'uncu madde çalışma grubu (*Article 29 Working Party*) tarafından onaylanmış anlaşma maddeleri, (iii) Bulut Hizmetlerinde Kişisel Verilerin Korunmasına ilişkin ISO 27018 sertifikası.

Gizlilik uygulamalarımızda saydam olmaya, size anlamlı gizlilik seçenekleri sunmaya ve depoladığımız ve işlediğimiz verileri sorumlu bir şekilde yönetmeye çalışıyoruz. Müşteri verilerinin gizliliğine olan bağlılığımızın bir ölçüsü, dünyanın ilk bulut gizliliği uygulama kodu olan ISO 27018'i benimsemiş olmamızdır. Azure'da, Azure'un kullanımı aracılığıyla sizin tarafınızdan veya sizin adınıza Microsoft'a sağlanan metin, ses, video veya görüntü dosyaları ve yazılımları dahil tüm müşteri verileri size aittir. İstediğiniz zaman ve herhangi bir nedenle Microsoft'un yardımı olmadan müşteri verilerinize erişebilirsiniz. Reklamcılık veya veri madenciliği amacıyla müşteri verilerini kullanmayız veya bu verilerden bilgi elde etmeyiz. Azure'da barındırdığınız müşteri verileri size ait olduğu için, verilerin depolanacağı yer ile bunların erişim ve silme işlemlerinin güvenli bir şekilde gerçekleştirilmesi sizin denetiminizdedir.

Bulut sertifikaları

Microsoft, yerel sertifikasyon gereksinimlerinin karşılanmasına yardımcı olmak ve güvenli buluta ilişkin kararlılığımızı dünya çapında pekiştirebilmek adına aşağıdakiler ışığında gayretle çalışır:

- ISO 27018, bulut gizliliği konusunda ilk uluslararası uygulama ilkeleri olan ISO 27001'e ek olarak gelen standarttır. AB veri koruma yasalarına dayanarak, kişisel verileri işleyen bulut servis sağlayıcılarına (veri işleyen), risklerin değerlendirilmesi ve kişisel verilerin korunması için son teknoloji kontrollerin uygulanmasına ilişkin belirli yönergeler sağlar. Kişisel verilerin gizliliği ile ilgili daha fazla ayrıntı için aşağıda yer alan Temel Mahremiyet İlkeleri bölümüne bakabilirsiniz,

- AB Model Maddeleri – Avrupa'nın mahremiyetten sorumlu düzenleyici kurumu, Microsoft Azure'un müşterileri için sözleşme kapsamında uyguladığı mahremiyet korumasının, verilerin uluslararası aktarımları konusunda mevcut AB standartlarına uygun olduğuna karar vermiştir. Microsoft, bu onaya sahip ilk bulut servis sağlayıcısıdır.

2. Temel güvenlik ilkeleri

Bu bölümde, başta Azure'un şifreleme ve güvenlik ile ilgili en iyi uygulamaları gelmek üzere, temel güvenlik ilkelerini Türkiye'de bulunan müşteriler için ne şekilde karşıladığı hususunda teknik bilgiler sağlanmıştır.

Azure, aktarılmakta olan ve durağan veriler için şifreleme sağlar

Microsoft Azure, hem aktarılmakta olan hem de durağan verilerin korunmasına yardımcı olacak özellikler sunar. Aktarılmakta olan veriler için Azure, müşteri ile Microsoft veri merkezleri arasındaki bağlantıları şifrelemek için Aktarım Katmanı Güvenliği (*Transport Layer Security - TLS*) protokolünü kullanır. TLS, güçlü kimlik doğrulaması, ileti gizliliği, bütünlük (ileti üzerinde oynanması, engelleme ve sahteciliğin saptanmasını sağlayarak) birlikte çalışabilirlik, algoritma esneklik, kolay kurulum ve kullanım kolaylığı sağlar. İstemci sistemleri ile Azure arasındaki her bağlantının benzersiz anahtarlar kullanmasını sağlamak amacıyla Kusursuz İletme Gizliliği (*Perfect Forward Secrecy*) kullanılır. Buna ek olarak Azure Sanal Ağları, sanal ağlar üzerinde yer alan sanal makinelerin (VM) yanı sıra, kurumsal VPN ağ geçitleri ile Azure arasındaki trafiği şifrelemeye yarayan endüstri standardı IPsec protokolünü kullanma imkanı sağlar.

Durağan veriler için müşteriler, BitLocker ile Windows sanal makineler için sabit disk şifreleme ve Saydam Veri Şifreleme (*Transparent Data Encryption*) ile SQL veritabanı şifreleme gibi kendilerine sunulan bir dizi şifreleme seçeneklerinden faydalanabilir. Azure, verinin gizliliğini şifrelemek ve korumak için güçlü simetrik ve asimetrik anahtarlar kullanan bir şifreleme uygular:

- Yazılım tabanlı AES-256 ile simetrik şifreleme/şifre çözme.
- Asimetrik anahtar için 2048 bit ya da daha yüksek seviyede.
- Güvenli anonimleştirme için SHA-256 ya da daha yüksek seviyede.

Daha fazla ayrıntı için Azure'da Veri Koruması isimli teknik inceleme yazısını okuyabilir (39 sayfa) ve Durağan verileriniz beklerken güvende mi? videosunu (5 dakika) izleyebilirsiniz.

Microsoft, Azure'u güvenlik ile ilgili en iyi uygulamaları kullanarak tasarlar ve işletir

Microsoft, Azure'u güvenlik konusuna en başından itibaren ihtimam göstererek tasarlamıştır. Microsoft Security Development Lifecycle'dan yararlanılan Azure geliştirme sürecinde, saldırı yüzeyinin azaltılması ve tehdit modelleme gibi güvenlik kavramları hizmetin içine inşa edilmiştir. Operasyon bakış açısıyla ele aldığımızda, Microsoft Operational Security Assurance, "assume breach" adı verilen ihlal varsayım stratejisi ve global olay-fiili geri dönüş, Azure altyapısının saldırılara karşı dayanıklı olmasını sağlamaya yardımcı olur.

Güvenlik açıkları, özellikle İnternete açık olanlar başta olmak üzere tüm bilgi sistemleri için önemli bir risk oluşturur. Bu riskleri azaltmak için atılacak ilk adımlardan biri, ilgili bölgeyi hedef alan tehditleri, güvenlik açıklarından yararlanan programları ve güvenlik açıklarını anlamaktır. Microsoft Güvenlik İstihbarat Raporu'nda, bölgesel risklerin ve kötü niyetli etkenler tarafından kullanılan güvenlik açıklarından yararlanan programların daha iyi anlaşılabilmesi için Türkiye dahil olmak üzere 106 bölge için bilgiler bulunmaktadır. Müşterilerin, Microsoft Azure kullanırken kullanmakta oldukları IaaS hizmetleri için güvenlik yamalarını düzenli olarak takip etmeleri gerektiğini anlamaları da büyük önem taşımaktadır. Geliştirilmiş yamalar ve güvenlik açığı yönetiminin, genellikle buluta geçişte başlıca avantajlardan biri olduğu kabul edilmektedir.

Azure altyapı koruması sağlar

Azure altyapısı, donanım, yazılım, ağlar, idari ve operasyonel personel ve bunların tamamına ev sahipliği yapan fiziksel veri merkezlerini içermektedir. Windows Azure, diğer Microsoft çevrimiçi hizmetleriyle alanı ve yardımcı programları paylaşarak bölgesel veri merkezlerinde çalışır. Her bir tesis, 365 gün 7/24 çalışacak şekilde tasarlanmıştır ve operasyonların elektrik kesintisi, fiziksel izinsiz giriş ve ağ kesintilerine karşı korunmasına yardımcı çeşitli tedbirler uygulanmaktadır. Bu veri merkezleri, fiziksel güvenlik ve kullanılabilirlik konularını kapsayan ISO 27001 endüstri standartları ile uyumludur. Bu veri merkezleri, Microsoft'un operasyonel personelleri tarafından yönetilir, izlenir ve idare edilir. Üçüncü şahıslar (örn: Tedarikçiler) bir değerlendirme sürecine tabi tutulur ve onaylı bir tedarikçi listesi oluşturularak kullanılır. Bu tedarikçiler Microsoft'un güvenlik politikalarına uymak zorundadır ve uyumluluk konusunda denetime tabi tutulurlar.

Müşteriler veri merkezi çeşitliliğinden yararlanabilir

Müşteriler, uyumluluk veya gecikme süresi hususları bakımından ülke içinde depolamayı veya güvenlik ve olağanüstü durum kurtarma amaçları için ülke dışında depolama yapmayı tercih edebilir. Veriler, yedekleme amacıyla seçilen bölgeler içinde çoğaltılabilir. Microsoft, Azure'un yalıtım ve kullanılabilirlik ilkelerinden faydalanabilmek amacıyla iş yüklerinin Azure bölgesel çiftleri arasında çoğaltılmasını önerir.

Müşteriler, izleme ve günlüğe kaydetme işlevleri sayesinde veri görünürlüğü elde ederler

Merkezi izleme, korelasyon ve analiz sistemleri, Azure ortamındaki cihazlar tarafından üretilen büyük miktardaki bilgileri yöneterek, hizmeti işleten ekiplere sürekli görünürlük imkanı verir ve ekiplerin zamanında uyarılmalarını sağlar. Ek izleme, günlüğe kaydetme ve raporlama işlevleri müşterilere

görünürlük imkânı verir.

Müşteriler kendi ağlarını koruyabilir

Bir hizmetin yönetim iş istasyonları ve harici veya daha az güvenilir arabirimleri tespit edilmeli ve saldırılara karşı savunma için gerekli uygun korumalara sahip olmalıdır. Bir arabirim, tüketicilerin veya yabancıların kullanımına sunulduğu ve yeterince sağlam olmadığı takdirde, hizmete veya içindeki verilere erişmek amacıyla saldırganlar tarafından çökertilebilir. Kullanıma sunulan arabirimler, özel arabirimler içeriyorsa (yönetim arabirimleri gibi), saldırının etkisi daha da büyük olabilir.

Microsoft'un Microsoft Azure'u güçlendirmek amacıyla kullandığı en iyi temel operasyonel uygulamalardan biri "assume breach" adı verilen ihlal varsayım stratejisi olarak bilinir. Yazılım güvenliği uzmanlarından oluşan bir ekip, Azure'un ihlalleri algılama, ihlallere karşı koruma ve kurtarma işlevlerini test etmek amacıyla dünyada gerçekleşen mevcut saldırıları ağ, platform ve uygulama katmanlarında simüle eder. Ayrıca Microsoft, müşterilerinin Azure'da barındırılan uygulamaları için yetkili sızma testleri yürütebilmeleri adına bir politika belirlemiştir. Microsoft, hizmetin güvenlik yeteneklerini sürekli zorlayarak ortaya çıkan tehditler karşısında avantajlı durumunu korumaya devam etmektedir.

3. Temel mahremiyet ilkeleri

Bu bölümde, Azure'un veri konumu ve kamu kurumlarından gelen talepler gibi temel mahremiyet ilkelerini, Türkiye'de bulunan müşteriler için nasıl karşıladığı ile ilgili teknik bilgiler sağlanmıştır.

Microsoft, müşteri verilerini reklam için kullanmaz

Microsoft, mahremiyet konusunu oldukça ciddiye alır ve kurumsal müşteri verilerini asla pazarlama veya reklam amacıyla kullanmaz. Bu ilke, Microsoft Çevrimiçi Hizmet Koşulları'nda belirtilmiştir ve Azure'un uluslararası gizlilik standardı olan ISO 27018 sertifikasını almasıyla da onaylanmıştır. Microsoft gizlilik konusundaki uygulama ilkeleri olan ISO 27018 sertifikasını alan ilk büyük bulut servis sağlayıcısıdır. Ek bilgilere bu 5 dakikalık videodan ulaşabilirsiniz: Microsoft'un Gizlilik Bölümü Başkanı Brendon Lynch ile Mahremiyet üzerine.

Azure, mantıksal kullanıcı yalıtımı işlevi sunar

Microsoft, bir müşterinin verilerinin başka bir müşterinin verileri ile karıştırılmamasını sağlamak ve zararlı bir programdan etkilenmiş ya da veri bütünlüğü bozulmuş bir müşterinin başka bir müşterinin hizmetini ya da verilerini etkilemesini önlemeye yardımcı olmak için tasarlanmış özel teknolojiler sayesinde, farklı müşteriler için depolama ve işleme proseslerini mantıksal olarak ayırır. Microsoft, ayrıca, müşteri verilerinin uygunsuz kullanımını, yetkisiz erişimleri ve kayıp vakalarını engellemek için de güçlü önlemler alır. Bu ek önlemler arasında, yönetim erişimi için güvenli kullanıcı kimlik doğrulaması gibi denetimler yer alır.

Mevcut bir Azure aboneliği olan müşteriler için, kullanıcı yalıtımına dair ayrıntılı bilgilere, Hizmet Güven Portalı (*Service Trust Portal - STP*) üzerinde bulunan "Azure Active Directory Çok Kullanıcılı Yalıtım" adlı teknik inceleme yazısından ulaşılabilir. STP, Microsoft Azure'un bağımsız denetim raporları, risk değerlendirmeleri, güvenlik ile ilgili en iyi uygulamaları ve benzer diğer materyalleri içeren güvenlik, gizlilik ve uyumluluk konusunda zengin kaynaklara erişim imkanı sunar.

Microsoft, saydam veri kullanım ilkelerine sahiptir ve bağımsız denetim hizmetlerini kullanır

Microsoft Çevrimiçi Hizmetleri Gizlilik Bildirimi'nde, Microsoft'un veri kullanım ilkelerinin anlaşılmasını sağlamak adına basit, şeffaf bir dil kullanılmıştır. Azure ayrıca, Microsoft'un verdiği taahhütleri yerine getirdiği konusunda hiçbir şüpheye yer bırakmayacak şekilde ISO 27001, ISO 27018 ve CSA CCM 3.0.1 gibi uluslararası standartlara göre yapılan bağımsız denetimlerden de geçer. İlave uyumluluk raporları Hizmet Güven Portalı'nda mevcuttur.

Müşteriler, verilerinin hangi bölgede yaşayacağını seçebilirler

Müşterilerimiz, uyumluluk gereksinimlerini en iyi karşılayan bölgeyi seçebilirler ve bu bakımdan verilerinin depolanmasını istedikleri lokasyon konusunda tam kontrole sahiptirler. Şu anda, aşağıdakiler de dahil olmak üzere 26 adet Azure bölgesi bulunmaktadır:

- Asya: Singapur, Hong Kong, Çin (Şanghay, Pekin), Japonya (Osaka, Tokyo), Hindistan (Pune, Chennai, Bombay) ve Avustralya (New South Wales, Victoria).
- Amerika Kıtası: Amerika Birleşik Devletleri (Iowa, Virginia, Illinois, Teksas, Kaliforniya), Amerika Birleşik Devletleri Hükümeti (Iowa, Virginia), Kanada (Toronto, Quebec) ve Brezilya (Sao Paulo eyaleti).
- Avrupa: İrlanda, Hollanda.

Buna ek olarak, Microsoft özellikle aşağıdakiler başta olmak üzere 8 adet daha Azure bölgesi olduğunu açıklamıştır:

- ABD Savunma Bakanlığı (iki tesis - duyurulacak), Almanya (Frankfurt, Magdeburg), Birleşik Krallık (iki tesis - duyurulacak), Güney Kore (Seul, bir tane daha duyurulacak).

Ayrıntılı bilgilere Azure Bölgeleri web sayfasından ulaşılabilir.

Müşteriler, verilerine kimlerin erişebileceğini kontrol edebilirler

Microsoft, müşterilerin kendi verilerine erişebilecekleri ve verilerini yönetebilecekleri self servis bir model oluşturmuştur. Microsoft mühendisleri veya alt yüklenicileri, örneğin bir sorunu giderme sırasında müşteri verilerine erişmesi gerektiğinde, kendilerine müşteri tarafından açıkça erişim izni verilmiş olması ve gereklilik ortadan kalktığında ise erişimin iptal edilmesi gerekir. Müşteri verilerine erişimi ve bu verilerin kullanımını düzenleyen operasyonel işlemler ve denetimler, veriye erişim yetkisini yalnızca yetkili personel ile sınırlandırmayı sağlayan çoklu onay mekanizması (*multi-factor authentication*) gibi güçlü denetimler ve kimlik doğrulama işlemleri tarafından korunmaktadır.

Müşteriler, aboneliklerinin sona ermesi üzerine kendi verilerini geri çekebilirler

Bir müşterinin kullandığı hizmetlerden biri için aboneliğini sonlandırmayı seçmesi durumunda, kendilerine verilerini sistemden çekmeleri için 90 gün verilir ve bundan sonra Microsoft, müşteri verilerini kendi kontrolü altındaki sistemlerden temizleme konusunda ilgili standartları takip eder.

Microsoft'un kamu kurumlarından gelen taleplere yaklaşımı

Microsoft, müşteri tarafından talimat verilmediği sürece herhangi bir üçüncü tarafa (adli merciler, diğer devlet kuruluşları veya davanın sivil tarafları dahil) müşteri verilerine doğrudan veya sınırsız erişim hakkı sağlamaz. Bir kamu kuruluşundan ya da adli mercilerden müşteri verilerine erişim talebi alındığında Microsoft aşağıda belirtilen politikayı uygular:

- İlgili üçüncü tarafı, her zaman, müşteri verilerini doğrudan müşteriden talep etmeleri konusunda yönlendirmeye çalışır. Müşteriye yönlendirilemeyecek haklı talepler için Microsoft bilgileri yalnızca yasal olarak yerine getirilmekle yükümlü olduğunda ve iletilen talep içeriği ile sınırlı olacak şekilde açıklar.
- Herhangi bir üçüncü taraf talebinde, yasal olarak bir engel bulunmadığı sürece, derhal müşterileri bilgilendirir ve talebin bir kopyasını gönderir.

Microsoft, hiçbir resmi kuruluşa asla şifreleme anahtarlarını sağlamaz ya da şifreleme sistemini kırma yeteneği vermez. Ek bilgilere Microsoft Şeffaflık Merkezi ve Prensipler, İlkeler ve Uygulamalar SSS web sayfaları üzerinden erişilebilir.

Microsoft, mahremiyete ilişkin katı standartlar oluşturur ve bunlara uygun davranır

Microsoft bulut gizliliği, Microsoft'un temel gizlilik gereksinimlerini ve uygulamalarını ayrıntılı olarak açıklayan Microsoft Gizlilik Standardı ve yazılım geliştirme sürecindeki gizlilik gereksinimlerini ele alan Microsoft Security Development Lifecycle kapsamında temellendirilmiştir. Microsoft, bu koruma yöntemlerini müşteri verilerini korumak adına sözleşmelerde yer verdiği güçlü taahhütler ile de destekler. Ek bilgilere bu 5 dakikalık videodan ulaşabilirsiniz: Microsoft Baş Hukuk Müşaviri, Başkan Brad Smith ile röportaj: Bulutta Güvenlik ve Gizlilik.

Sonuç

Microsoft, uyumluluk, güvenlik ve mahremiyet uygulamaları bakımından şeffaf olmayı hedeflemektedir. Ayrıca Microsoft, belirli bir amaca hizmet eden mahremiyet seçenekleri sunar ve depoladığı ve işlediği verileri yönetmek konusundaki sorumluluklarını ciddiye alır. Microsoft'un müşteri verilerinin güvenliğini ve mahremiyetini sağlama konusundaki taahhüdü, Microsoft'un kurumsal bulut hizmetlerindeki müşteri verileri için tanımlanmış mahremiyet ilkeleri ve uygulamalarının anlatıldığı Microsoft Çevrimiçi Hizmetleri Gizlilik Bildirimi tarafından desteklenmektedir.

Uyumluluk konusunda endişesi olan müşteriler için Microsoft Azure'un Kanun ile tutarlı bir şekilde ISO 27001, ISO 27018 ve AB Model Maddeleri gibi uluslararası güvenlik ve mahremiyet gereksinimleri açısından onaylı ve sertifikalı olduğunu belirtmek gerekir.

Microsoft, Azure'un kamu sektöründeki ve her ölçekteki ticari müşterilerin ihtiyaçlarını karşılayabilmek adına güvenli ve uyumlu bir bulut hizmeti sağlayabildiğine inanmaktadır.