Bulut Bilişim Güvenlik ve Kullanım Standardı

(Taslak)

TÜRK STANDARDLARI ENSTİTÜSÜ

07.03.2014

Standart Hakkında

Bu Standart, Türk Standardları Enstitüsü bünyesinde faaliyet gösteren olan Siber Güvenlik Özel Komitesi Bulut Bilişim Çalışma Grubu tarafından hazırlanmıştır.

2013/4890 sayılı Bakanlar Kurulu Kararı doğrultusunda, 20/06/2013 tarihli ve 28683 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda güvenlik alanında standartların oluşturulması konusunda eylem sorumlusu olarak Türk Standardları Enstitüsü görevlendirilmiştir. Söz konusu görevlendirme kapsamında, TSE tarafından bilişim alanında pek çok konuda standart ve rehberler oluşturulmaya başlanmıştır. Bu standart, söz konusu çalışma kapsamında oluşturulmuştur. Türk Standardları Enstitüsü tarafından yürütülen tüm standart çalışmalarına bilisim.tse.org.tr adresinden erişilebilir.

İçindekiler

Tanımlar

Ana Bilgisayar	Ağ altyapısı ile bağlı olduğu diğer bilgisayarlara hizmet sunan bilgisayara verilen addır.
Ara Katman	İşletim sistemi ile uygulamalar arasında koordinasyonu sağlayan katmandır. Dağıtık mimarilerde ara katman, uygulamaların altyapının karmaşıklığından bağımsız olarak tek bir bilgisayar üzerinde çalışır gibi çalışabilmesine imkân sağlar.
Arayüz (Uygulama Arayüzü)	Bir mekanizma ile bu mekanizmanın kullanıcısı arasındaki etkileşime aracılık eden yüzey veya ortama verilen isimdir.
Arka Kapı	Sistem üzerinde sıradan incelemelerle tespit edilemeyecek şekilde, normal kimlik kanıtlama süreçlerininden hariç olarak sisteme uzaktan erişim imkânı sağlayan yöntemlerdir.
Birlikte Çalışabilirlik	Birbirinden bağımsız bilişim sistemlerinin bütünleşik bir şekilde çalışabilme yeteneğidir.
Bulut Bilişim	İşlemci gücü ve depolama alanı gibi bilişim kaynaklarının ihtiyaç duyulan anda, ihtiyaç duyulduğu kadar kullanılması esasına dayanan, uygulamalar ile altyapının birbirinden bağımsız olduğu ve veriye izin verilen her yerden kontrollü erişimin mümkün olduğu, gerektiğinde kapasitenin hızlı bir şekilde arttırılıp azaltılabildiği, kaynakların kullanımının kolaylıkla kontrol altında tutulabildiği ve raporlanabildiği bir bilişim türüdür.
Bulut Bilişim Hizmet Sağlayıcısı	Kuruluşlara bulut bilişim hizmeti sunan firma veya kuruluşlara verilen addır.
Çok Kiracılılık	Farklı kuruluşlara ait çok sayıda sistemin, uygulamanın veya verinin aynı fiziksel donanım üzerinde barındırılmasıdır. Çok kiracılılık yöntemi, bulut bilişim altyapılarında kullanılan bir yöntemdir.
Dağıtık Mimari	Farklı nitelikte bilgisayarlardan oluşturulmuş bir bilgisayar ağı üzerinde uygulamaların dağıtılmış bir biçimde çalıştırılabilmesini sağlayan mimari yapıdır.
Depo (Repository)	Bir veri yığınının kategorize edilmiş bir şekilde genellikle bilgisayar depolama alanında saklandığı ve sürdürüldüğü merkezi alandır.
Firma Bağımlılığı	Bulut bilişim bağlamında; standart protokollerin, uygulama programlama arayüzlerinin, veri yapılarının ve hizmet modellerinin

	yetersizliği sebebiyle bir hizmet sağlayıcısından diğer bir hizmet sağlayıcısına geçişin zor olması ve tek bir hizmet sağlayıcısına bağımlı kalınması durumudur.
Sanal Makine Gözlemcisi (Hypervisor)	Sanal cihazları oluşturan ve çalıştıran yazılım, ara katman veya donanım bileşenidir.
İmaj	Bilgisayar terminolojisinde imaj, bilgisayar sisteminin veya bir parçasının bütün içeriğinin dosya benzeri bir yapıda kalıcı olarak saklanan kopyasına verilen addır.
İnce İstemci	Merkezi bir sunucuya bağlanarak bu sunucu üzerinde oturum açmaya ve program çalıştırmaya yarayan kullanıcı terminalleridir. Sunucu tabanlı bilgi işlem olarak adlandırılan bu yapıda bütün uygulamalar sunucu üzerinde çalışır. İnce istemcilerin işlevi ise kullanıcı girdilerini sunucuya, sunucudan gelen ekran görüntüsünü ise kullanıcıya iletmekten ibarettir.
İstemci	Diğer bir bilgisayar sisteminden (örneğin ana bilgisayardan) önceden belirlenmiş bir protokol aracılığıyla hizmet talep eden ve talebe verilen cevap doğrultusunda işlemlerini yürüten bilgisayardır.
Keylogger	Bilgisayarın kullanımı esnasında klavye ve benzeri ortamlar aracılığıyla girilen tüm karakterleri bir günlük dosyasına kaydetme yeteneğine sahip olan bir casus yazılım türüdür.
Kullanım Bazlı Ücretlendirme	Hizmet sağlayıcısının hizmetin kullanıldığı süre kadar değil, hizmet esnasında kullanılan kaynak miktarınca ücret talep ettiği ücretlendirme modelidir.
Metaveri (Metadata)	Belirli bir veri kümesi, nesnesi veya kaynağında tutulan verilerin format, biçim ve özelliklerini tanımlayan veridir.
Sanallaştırma	Bir fiziksel kaynağın birden fazla mantıksal kaynağa bölünmesi ve ortaya çıkan her bir mantıksal kaynağın ayrı birer fiziksel kaynak gibi davranmasının sağlanması işlemidir.
Sanal Makine	Doğrudan bir donanım üzerinde çalışmayan, sanal makine yöneticisi yazılımlar aracılığıyla yönetilen yazılım tabanlı bilgisayardır.
Senkronizasyon (Eşzamanlama veya Eşleme)	Eşgüdümlü çalışan parçalı sistemlerin zamanlamalarının eşleştirilmiş olduğunu ifade eder. Birimleri bu şekilde çalışan sistemler senkronize veya eşzamanlı olarak anılır.
Sosyal Mühendislik	Bilgi güvenliği terminolojisinde sosyal mühendislik, kişi, kuruluş veya bilgi sistemlerine ilişkin gizli bilgilerin elde edilmesi veya bilgi

	sistemlerine yetkisiz erişim sağlanması amacıyla psikolojik manipülasyon yöntemlerinin kullanılmasıdır.
Truva Atı	Faydalı yazılım gibi görünen, ancak kurulduğu bilgisayar sistemine özel yetkiye sahip olarak bilgisayar sistemi üzerine zararlı yazılımların yüklenmesine veya yetkisiz erişime imkan veren zararlı yazılımdır.
Yazılım Standardı	Yazılım geliştiricilerinin yazılımın geliştirilmesi esnasında üzerinde mutabık kaldıkları standart, protokol ya da doküman, dosya veya veri transferine ilişkin ortak formatlardır.
Web 2.0	İnternet teknolojisinin kullanım biçimlerindeki değişimi ve yenilikçilik, etkileşim, güvenli bilgi paylaşımı ve ortak çalışma gibi işlevsel özellikleri mümkün kılan, kullanıcının hâkimiyetine dayanan internet sitesi tasarımlarını tanımlayan kavramdır.

Kısaltmalar

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
API	Uygulama Programlama Arayüzü (Application Programming Interface)
BHS	Bulut Bilişim Hizmet Sağlayıcısı
BT	Bilgi Teknolojileri
CSA	Bulut Güvenlik Birliği (Cloud Security Alliance)
DDoS	Dağıtık Hizmet Engelleme Saldırısı (Distributed Denial of Service)
DoS	Hizmet Engelleme Saldırısı (Denial of Service)
HSS	Hizmet Seviyesi Sözleşmesi (Service Level Agreement – SLA)
NIST	ABD Ulusal Standartlar ve Teknoloji Enstitüsü
SAML	Güvenlik Beyanı İşaretleme Dili (Security Assertion Markup Language)
XACML	Genişletilebilir Erişim Kontrolü İşaretleme Dili (Extensible Access Control Markup Language)
XML	Genişletilebilir İşaretleme Dili (Extensible Markup Language)

1. Giriş

Bulut bilişime olan ilgi, düşük ücretlere sağladığı yüksek esneklik ve erişilebilirlik sebebiyle son yıllarda hızla artmıştır. Öte yandan, güvenlik ve gizlilik, uygulamalarını ve verilerini buluta taşırken kuruluşlar için bazı endişeler doğurmaktadır. Söz konusu endişelerin azaltılması için dünya genelinde pek çok ülkede standart çalışmaları yürütülmektedir. Bulut bilişimin ülkemizde de artan oranda kullanılmaya başlanması, bu alanda standartlaşma ihtiyacını gündeme getirmiştir.

2013/4890 sayılı Bakanlar Kurulu Kararı doğrultusunda, 20/06/2013 tarihli ve 28683 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda güvenlik alanında standartların oluşturulması konusunda eylem sorumlusu olarak Türk Standartları Enstitüsü görevlendirilmiştir. Söz konusu görevlendirme, bu standardın oluşturulmasında önemli bir etken ve dayanak niteliğindedir.

Bulut bilişime yönelik standartların oluşturulması ihtiyacı güvenlikle sınırlı olmayıp, güvenlik, güvenilirlik, performans ve firma bağımlılığının önlenmesi gibi geniş bir alana yayılmaktadır. Bu nedenle hazırlanmış olan bu standart güvenlikle ilgili hususların yanı sıra güvenilirlik, performans ve firma bağımlılığı gibi konular da göz önünde bulundurularak daha geniş ve bütüncül bir bakış açısıyla hazırlanmıştır.

Dokümanın ana konusu, bulut bilişim hizmet sağlayıcılarının hizmet sunumuna ilişkin tüm süreçlerinde göz önünde bulunduracakları önemli hususların ortaya konmasıdır. Yöntem olarak, yönlendirici bilgilerin ardından kolay takip açısından bir kontrol listesine de yer verilmiştir.

1.1 Amaç ve Kapsam

Bu dokümanın amacı, bulut bilişimin getirdiği güvenlik ve gizlilik problemlerini kısaca gözden geçirmek, kuruluşlara ilgili hususlarda yönlendirici bilgiler sunmaktır. Doküman bulut ortamındaki tehditleri, teknoloji risklerini, koruma yöntemlerini tartışarak bu teknolojilerin kullanımıyla ilgili karar vermek için gereken bilgi ve anlayışı sağlamayı hedeflemekte, bu anlamda hem bulut bilişim hizmet sağlayıcıları, hem de bulut bilişim alıcısı kurum ve kuruluşlar için önemli bilgiler içermektedir. Doküman hiçbir bulut hizmeti, hizmet sağlayıcısı, hizmet anlaşması veya yayımlama modeliyle ilgili bir reçete sunmaz, belirli bir hizmet sağlayıcısı veya teknolojiye yönlendirmede bulunmaz. Her organizasyon kendi ihtiyaçlarına göre kendi analizini gerçekleştirmelidir.

Bulut bilişim, çok boyuta sahip geniş bir konudur. Bulut bilişimin güvenlik bakış açısıyla ele alındığı bu dokümanda genel itibariyle bulut bilişimin güvenliğine, güvenilirliğine ve veri mahremiyetine yönelik hususlar ele alınmıştır. Bununla birlikte, bulut bilişim hizmet sağlayıcıları ile hizmet alıcıları arasındaki ilişkilere yönelik hususlar da, bu alandaki artan ihtiyaç sebebiyle dokümanın bir parçası haline getirilmiştir.

Bu doküman hazırlanırken, başta Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) ve Bulut Güvenliği Birliği (CSA) olmak üzere, bulut bilişim ve bulut bilişim güvenliği alanında otorite sayılabilecek kuruluşların çalışmalarından yoğun şekilde faydalanılmış, ancak Türkiye'ye özel hususlarda ayrıma ve/veya detaylandırmaya gidilmiştir. Çalışma kapsamında faydalanılan yayınıların listesine "Referanslar" bölümü altında yer verilmiştir.

Konuyla ilgilenen tüm tarafların bu dokümandan elde edeceği faydanın azami düzeyde olması için dokümanın son kısmına bir kontrol listesi eklenmiştir. Dokümanın baş kısmında yer alan

açıklayıcı bilgiler, önemli hususların vurgulanması amacıyla hazırlanmış olup, dokümanın kapsamına giren tüm hususları içermez, bu nedenle kontrol listesinde yer alan tüm bileşenler bu kısımda kapsanmamaktadır.

1.2 Hedef Kitle

Dokümanın hedef kitlesi aşağıdaki kategorilerdeki şahısları içermektedir.

- Bulut Bilişim Hizmet Sağlayıcıları
- Kamu Kurum ve Kuruluşları
- Sistem yöneticileri, çalıştırıcıları ile bulut bilişimle ilgili kararlar veren BT çalışanları
- Güvenlik Uzmanları, yöneticileri, denetçileri ve güvenlikle ilgili sorumluluğu bulunan BT çalışanları
- Bulutta güvenlik ve gizlilik endişesi taşıyan BT yöneticileri.
- Sistem ve ağ yöneticileri
- Bulut hizmetlerinin kullanıcıları

Doküman doğası gereği teknik içerikli olmakla birlikte, okuyucuların incelenen konuları anlamasına yardımcı olmak için gerekli temel bilgileri de sunmaktadır. Bununla beraber okuyucuların temel işletim sistemleri ve ağ bilgisi ile başlangıç seviyesinde bulut bilişim bilgisine sahip olduğunu varsaymaktadır.

2. Bulut Bilişim

Bulut bilişim NIST tarafından, minimum yönetim çabası ve hizmet sağlayıcısı desteği ile yayımlanabilecek ortak havuzlara ve konfigüre edilebilir kaynaklara (örneğin ağlar, sunucular, veri depoları, uygulamalar ve hizmetler) anında erişim sağlayan model olarak tanımlanmaktadır.

Bulut bilişim, kaynakların esnek kullanımından dolayı ekonomik fayda, özelleştirilebilirlik ve daha başka verimlilikler sağlar. Ancak bulut bilişimin, hala yeterince gelişmemiş ve standartlaştırılmamış dağıtık sistemlerin gün yüzüne çıkan bir kolu olduğu unutulmamalıdır.

2.1 Yayımlama Modelleri

Genel bulut bilişim tanımlanmış birkaç yayımlama yönteminden bir tanesidir. Yayımlama modelleri, bilişim kaynaklarının yönetimi ve müşterilere tahsisi konularının yanı sıra müşteri sınıflarının ayrıştırılmasını da detaylıca tanımlar. Bir genel bulut, bir altyapının ve içerdiği bilişim kaynaklarının internette genel erişime açık olduğu yayımlama modelidir.

Genel bulut hizmeti, bir bulut hizmet sağlayıcısından temin edilir, kuruluşlarda barındırılmaz. Öte yandan özel bulutta, bilişim ortamı tek bir kuruluş tarafından işletilir. Yine aynı kuruluş tarafından yönetilebileceği gibi harici kuruluşlar tarafından da yönetilebilir. Sistem, kuruluşun kendi veri merkezlerinde barındırılabileceği gibi kuruluş dışında da barındırılabilir. Özel bulut bilişim, kuruluşa sistem kaynaklarının yönetiminde tam kontrol imkanı sunar.

Bunların dışında topluluk ve hibrit olmak üzere iki farklı bulut bilişim yayımlama modeli daha vardır. Topluluk modeli genel bulut ile özel bulut arasında kalan bir modeldir. Yapı olarak özel buluta benzemekle birlikte bulut tek bir kuruluş tarafından değil, aynı gizlilik gereksinimlerine sahip birden çok kuruluş tarafından işletilir. Hibrit model ise hem genel hem de özel bulutları içeren daha karmaşık bir yapıdır.

Yayımlama modellerinin güvenlik ve gizliliğe farklı etkilerinin olmasına karşın, modelin kendisi belli bir güvenlik ve gizlilik seviyesi dayatmaz. Seviye, güvenlik ve gizlilik poliçesine, bulut ortamının sağladığı kontrol sistemlerinin sağlamlığına ve hizmet sağlayıcısı ya da kuruluş tarafından belirlenen yönetimle ilgili detaylar gibi etkenlere bağlıdır.

2.2 Hizmet Modelleri

Yayımlama modellerinin bulut bilişimde önemli bir rol oynaması gibi hizmet modelleri de aynı önemle değerlendirilmesi gereken bir konudur. Hizmet modeli kuruluşun kapsamını, bilişim ortamı üzerindeki kontrolünü ve kullanılan soyutlama seviyesini belirler. En sık kullanılan üç servis modeli şunlardır:

- **Yazılım Hizmeti (Software-as-a-Service).** İhtiyaç duyulan uygulamaların ve çalışmalarını sağlayacak kaynakların temin edildiği hizmet modelidir. Esas amacı yazılım geliştirme, bakım, yönetim ve donanım ücretlerinin düşürülmesidir. Güvenlik, büyük oranda hizmet sağlayıcısı tarafından sağlanır.
- **Platform Hizmeti (Platform-as-a-Service).** Uygulamaların geliştirilip yayınlanması için ihtiyaç duyulan platformun temin edildiği modeldir. Esas amacı, gereken donanım ve yazılım bileşenlerini satın alma ve barındırma zahmetini ve fiyatını düşürmektir. Bulut

müşterisi yazılım ve yazılımın çalışacağı ortam üzerinde kontrole sahiptir. Güvenliğin bir bölümünden hizmet sağlayıcı, bir bölümünden ise müşteri sorumludur.

- **Altyapı Hizmeti (Infrastructure-as-a-Service).** Uygulamaların geliştirilip çalıştırılması için ihtiyaç duyulan sunucu, yazılım ve ağ ekipmanlarından oluşan temel bilişim altyapısının sağlandığı modeldir. Esas amacı temel yazılım ve donanımı satın alıp barındırmaktan kaçınıp, yerine bir hizmet arayüzü ile kontrol edebilmektir. Güvenlik temel ekipmanlar dışında müşteri tarafından sağlanır.

2.3 Dış Kaynak Kullanımı ve Hesaplanabilirlik

Bulut bilişim sadece bir kuruluş tarafından özel bulut olarak gerçekleştirilebilmesine karşın altında yatan teşvik, genel bulut aracılığıyla dış kaynakların kuruluşun bilişim ortamının bir parçası olarak kullanılabilmesini sağlamaktır. Güvenlik ve gizlilikle ilgili endişeler, diğer bilişim teknolojilerinde dış kaynak kullanımında olduğu gibi burada da vardır.

Yaygın olarak kullanılan üç genel bulut çeşidi mevcuttur. İlkinde hizmet bedelleri tamamen reklam gelirlerinden karşılanır, kuruluşa ek bir masrafı olmaz. Örnek olarak arama ve e-posta hizmetleri verilebilir. İkinci tür, reklam içermez fakat hizmet sözleşmesi hizmet sağlayıcısı tarafından hazırlanır, kuruluşa maliyeti düşük olur. Üçüncü tür yine reklam barındırmaz, hizmet sözleşmesi hizmet sağlayıcı ve hizmet alan kuruluş tarafından ortak hazırlanır. Servisler kuruluşun ihtiyaçlarına göre ayarlanır ve maliyet de bu ihtiyaçlara bağlı olarak değişir.

Genel buluta taşınmadaki ana motivasyon maliyeti düşürüp, verimliliği arttırmaktır, ancak bunu yaparken güvenlik ve gizlilikten ödün vermemek gerekir. Performans ve veri gizliliği gibi güvenlik de kuruluşun gözetiminde olmalıdır. Bulut bilişim yeni güvenlik sorunlarını gündeme getirdiğinden dolayı kuruluş, hizmet sağlayıcısının bilişim ortamını nasıl güvenli ve sürdürülebilir kıldığını gözlemleyerek verisinin güvenliğinden emin olmalıdır.

3. Genel Bulut Hizmetleri

Kuruluşların bulut bilişime bakış açıları, farklı amaçları, yasal sorumlulukları, yüzleştikleri tehditler ve yüzleşebilecekleri teknik/idari/yasal sorunların farklı seviyelerde olması sebebiyle büyük ölçüde değişkenlik gösterebilir. Örneğin vatandaşlar hakkında detaylı biligiler barındıran bir kamu kurumu ile bu tarz bir bilgi barındırmayan başka bir kurum veya kuruluşun güvenlik ve gizlilik hedefleri farklı olacaktır. Risk açısından bakıldığında, bir kuruluşun bulut ortamına uygunluğu ancak karşılaşabileceği tehditlerin ve sonuçlarının analizi yapılarak belirlenebilir.

Bir kuruluş için güvenlik ve gizlilik hedefleri, bilgi teknolojilerinde dış kaynak kullanımıyla ilgili verilen kararlarda, özellikle kuruluşun kaynaklarının genel buluta taşınması ve hizmet sağlayıcı ile yapılacak anlaşmalarla ilgili olanlarda, kritik faktörlerden biridir. Bir kuruluş için işe yarayan seçimin başka bir kuruluşta da işe yarayacağı kesin değildir. Ayrıca, birçok kuruluş bütün bilişim kaynaklarını koruyacak bir yapıyı mali olarak karşılayabilecek durumda değildir. Bu sebeple maliyet, kritiklik ve hassasiyet kriterleri göz önüne alınarak önceliklendirme yapılmalıdır. Sonuç olarak, bulut bilişimle ilgili kararlar bu kriterlerin risk analizini içermelidir.

3.1 Hizmet Sözleşmeleri

Genel bulut bilişim hizmetleriyle ilgili spesifikasyonlar genellikle hizmet sözleşmesi olarak adlandırılırlar. Ayrıca hizmetin süresini, sonlanma koşullarını ve sonlandıktan sonra verinin saklanacağı süreyi içerir. Bir hizmet sözleşmesindeki bütün kural ve koşullar; hizmet seviyesi sözleşmesi (HSS / SLA), gizlilik poliçesi, kabul edilebilir kullanım poliçesi ve kullanım kuralları olacak şeklide birden fazla dökümanda taahhüt edilir.

İki çeşit hizmet sözleşmesi mevcuttur: öntanımlı, tartışmaya kapalı sözleşmeler ve tartışılabilir sözleşmeler. Tartışmaya kapalı sözleşmeler içeriği hizmet sağlayıcısı tarafından belirlenmiş ve gerektiğinde müşteriye doğrudan haber verilmeden sözleşmenin yeni sürümünün online olarak yayınlanması suretiyle güncellenebilirler.

Tartışılabilir hizmet sözleşmeleri daha çok geleneksel bilgi teknolojilerinde dış kaynak kullanım sözleşmeleri gibidir. Belli bir kuruluşun güvenlik ve gizlilik endişelerini, prosedürlerini ve teknik kontrollerini belirtmek için kullanılabilirler.

Kritik veri ve uygulamalar bir kuruluşun tartışılabilir sözleşmeyi tercih etmesini gerektirebilir. Sözleşmede belirtilen ek hizmetlerin veya taahhütlerin getireceği ek maliyetten dolayı tartışmaya kapalı hizmet sözleşmeleriyle alınan hizmetlere oranla daha yüksek maliyetli olması beklenir. Sözleşmenin türü ne olursa olsun yasal ve teknik tavsiyelerin alınması kuruluşun ihtiyaçlarını karşılayacak doğru sözleşmenin hazırlanmasına katkıda bulunacaktır.

3.2 Güvenlik ve Gizlilikle İlgili Avantajlar

Genel bulutun yüzleştiği en büyük engellerden biri güvenlik olmasına karşın, bulut bilişim paradigmasının güvenlik ihtiyaçlarını karşılamak için sunduğu yeni imkanlar bazı kuruluşların mevcut güvenliğinin iyileştirilmesine de katkıda bulunabilir. En büyük faydayı az sayıda sistem yöneticisi ve bilgi güvenliği çalışanı bulunan küçük kuruluşlar, sistemlerini genel buluta taşımak suretiyle büyük kuruluşların sahip olduğu imkânlara kavuşarak sağlayabilirler.

Güvenlik seçeneklerinin iyileştirilmesi gizliliğe de katkıda bulunur. Gerçek anlamda bir gizlillik

ancak sağlam bir bilgi güvenliği yapısıyla mümkün olur. Benzer şekilde gizliliğin de tıpkı güvenlik gibi kurumsal, yönetimsel ve teknik etkenleri vardır.

Organizasyonların genel bulut bilişime geçişte güvenlik ve gizlilik açısından iyileştirmesi gereken muhtemel alanlar şunlardır:

- **Çalışanların Uzmanlaştırılması.** Bulut hizmet sağlayıcıları, tıpkı diğer büyük bilişim imkanlarına sahip kuruluşlar gibi, çalışanlarını güvenlik, gizlilik veya başka birçok alanda uzmanlaştırma imkanına sahiptir. Verilen hizmetin boyutu arttıkça uzmanlaşma seviyesi de artar.
- **Platform Gücü.** Bulut bilişim platformu geleneksel bilişim sistemlerine göre daha tekdüze bir yapıya sahiptir. Bu tekdüzelik ve homojenlik platformu güçlendirmeyi; güvenlik, yönetim, bakım, test ve yama işlemlerinde ise daha fazla otomasyonu mümkün kılar.
- **Kaynaklara Erişim.** Bulut bilişim sistemleri ölçeklenebilirliklerinden dolayı üst seviye bir erişilebilirlik sağlamaktadır. Bulut bilişim ortamının yedekleme ve doğal felaketler sonrası kurtarma seçenekleri ciddi hasarlardan sonra sistemi kısa sürede ayağa kaldırma imkânı sunar. İhtiyaç duyulduğunda sağlanabilecek kaynak kapasitesi ise artan hizmet taleplerine veya dağıtık servis dışı bırakma saldırılarına (DDoS) karşı dayanıklılığı arttırmak için kullanılabilir.
- **Yedekleme ve Geri Yükleme.** Bulut hizmet sağlayıcısının yedekleme ve geri yükleme poliçe ve prosedürleri kuruluşlara göre daha üstün olabilir. Bulutta korunan veri daha erişilebilir, kurtarılması kolay ve birçok durumda geleneksel veri merkezlerinde saklanan veriye göre daha güvenilirdir. Ayrıca bulut farklı coğrafi konumlardan erişim ihtiyaçlarına da cevap verebilir.
- **Taşınabilir Uçlar.** Bulut istemcileri genel amaçlı web tarayıcıları veya daha özel amaçlı uygulamalar olabilir. Bulut bilişimde, bulutta çalışan uygulamaların ihtiyaç duydukları esas kaynaklar hizmet sağlayıcı tarafından karşılanır. Bu sayede uygulamalar dizüstü, notebook, netbook, tablet, cep telefonu gibi istemcilerde çalıştırılabilir.
- **Veri Konsantrasyonu.** Genel bulutta barındırılan veri, mobil çalışma ortamı sunan kuruluşlar için taşınabilir bilgisayarlar ve mobil cihazlarda saklanan veriye oranla daha az risk arz eder. Birçok kuruluş verimliliği ve yaratıcılığı arttırmak için mobil çalışma ortamı sunmak amacıyla buluta geçişini yapmıştır. Dikkatle yapılandırılmış uygulamalar ve kısıtlanmış erişimle istemcilerin ele geçirilmesi durumundaki bilgi sızıntısı riski en alt seviyeye çekilebilir.

3.3 Güvenlik ve Gizlilikle İlgili Dezavantajlar

Genel bulut bilişim, güvenlik ve gizlilik açısından birçok avantaj sağlama potansiyelinin yanı sıra bu konuda bazı yeni endişeler de getirmektedir. Geleneksel bilişim sistemleriyle karşılaştırıldığında genel bulutun güvenlik ve gizlilik adına sebep olabileceği temel endişeler şunlardır:

- **Sistem Karmaşıklığı.** Geleneksel veri merkezleriyle karşılaştırıldığında, genel bulut

oldukça karmaşık bir yapıdadır. Genel bulutu oluşturan birçok bileşen geniş bir saldırı yüzeyine sahiptir. Genel bulut, genel amaçlı uygulamalar, sanal makine araçları ve veri depolama sistemlerinin yanı sıra arka planda çalışan kaynak paylaştırma, hizmet seviyesi kontrolü ve hizmet yönetimiyle ilgili buluta özel birçok bileşen barındırmaktadır.

Güvenlik sadece bileşenlerin kendi başlarına verimli ve doğru çalışmalarına bağlı değildir. Aynı zamanda bu bileşenlerin birbirleriyle etkileşimleriyle de alakalıdır. Bileşen sayısı arttıkça bu etkileşimin karmaşıklık seviyesi, bileşen sayısının karesi oranında artar. Karmaşıklık seviyesi arttıkça da güvenlik zafiyetlerinin sayısının artması muhtemel bir durumdur.

- **Çok Kiracılı Ortam.** Hizmet sağlayıcılar tarafından sunulan genel bulut hizmetinin belli başlı zorluklarından biri de ortak kaynak ve bileşenleri kullanan ve birbirini tanımayan müşterilerdir. Bulut bilişim kaynakların fiziksel ayrımından daha çok mantıksal ayrımına dayanır. Bu sayede saldırgan bulut müşterisi olarak sisteme dahil olup bulut bileşenlerindeki zafiyetleri istismar ederek diğer müşterilerin sistemlerine yetkisiz erişim sağlayabilir.
- **İnternete Açık Hizmetler.** Yönetim panelleri de dahil olmak üzere genel bulut hizmetleri internet üzerinden sunulur. Dolayısıyla daha önce sadece kuruluşun yerel ağından erişilebilir olan verilerin genel buluta taşınması yeni riskler doğurur. Daha önce üst seviye bir tehdit olarak düşünülmeyen ağ tabanlı saldırılar artık ciddi bir endişe konusu olur.
- **Kontrol Kaybı.** Bulut bilişimdeki güvenlik ve gizlilik endişelerinin geleneksel bilişim sistemlerindekilere benzer olmasının yanı sıra bu sistemlerin haricen yönetilmesi ve muhtemel yanlış yönetimlerin getireceği endişeler de vardır. Genel buluta taşınma daha önce kuruluşun doğrudan kontrolünde olan sistemlerin sorumluluğunun bulut hizmet sağlayıcısına verilmesini gerektirir. Bu da sistemin düzenli gözlenmesi veya siber saldırı olaylarına müdahale gibi süreçlerin kuruluşun ve hizmet sağlayıcısının işbirliği ile yürütülmesi gerektiği anlamına gelir.

  Sistem ve veri üzerindeki bu kontrol kaybı kuruluşun farkındalık seviyesinin, alternatif ve önceliklerinin değişmesine sebep olur. Veri, harici bir hizmet sağlayıcısı tarafından saklandığında gizlilikle ilgili yasal korumalar da değişecektir. Bu koşullar altında hesaplanabilirliği sürdürmek eskiye oranla daha zor olacaktır.
- **Veri Hakimiyetinin Paylaşılması.** Bulut bilişim genel bulutlarının fiziki konumlandırmasının veri sahibinin lokasyonu dışında olması sebebiyle, verinin sahip olma hakimiyetinin dolaylı olarak paylaşılmasını gerektirecek durumlar ortaya çıkabilmektedir. Diğer yandan veri ve verinin paylaşımı ile ilgili olarak, veri merkezinin bulunduğu yere bağlı olmak üzere, veri sahibi dolaylı olarak üçüncü ülkelerin kanunlarına ve mahkemelerinin emirlerine uymak durumunda kalacaktır. Ülkemizde veri korumaya ilişkin mevzuatta, verilerin yurtdışında barındırılmasına yönelik kısıtlamalar getirilmiştir.

Bu temel endişeler üzerine, güvenlik ve gizlilikle ilgili daha detaylı açıklamalar bir sonraki bölümde sunulmuştur.

4. Güvenlik ve Gizlilik

Bulut bilişim henüz gelişim içinde olsa da güvenlik konusu yaşanan tecrübelere, yapılan araştırmalara ve ilgili teknolojilere bakılarak incelenebilir. Ele alınan örnekler olabildiğince tanımlanmış, ortaya çıkarılmış sorunlardan alınmıştır. Ancak sorun, genelin aksine tek bir yöne odaklanmış olabilir.

Bulut bilişim hizmet odaklı mimarı, sanallaştırma, web 2.0 gibi farklı teknolojileri bir araya getirdiği için gizlilik ve güvenlik meseleleri başka bir çerçevede incelenmelidir. Genel bulut bilişim standart olandan verinin açık olarak çok katmanlı korunduğu bir altyapıya köklü bir değişiklik getirir.

Aşağıdaki gizlilik ve güvenlikle ilgili başlıkların, bulut bilişimle ilgili uzun vadeli öneme sahip olduğu düşünülmektedir.

4.1 Veri Yönetimi

Yönetim, kuruluşun prosedür, politika ve standartlarla uygulamaları tasarım, uygulama, test ve kullanım açısından denetlemesi ve gözetlemesidir. Bulut bilişimin geniş bir alanda basit kullanım olanağı sağlaması, kuruluşların çalışanlarının keyfi kullandığı hizmetleri kontrol etmesini zorlaştırır.

Bulut bilişim ile sermaye yatırımına harcanan kaynakların azalıp ve operasyonal hizmetler için yapılan giderlerin karşılanması önemli bir avantajdır. Bu sayede hem yeni hizmetler için gerekli maddi ve zamana dair harcamalar azalır, hem de maddi yatırımların geri dönüşümü hızlanmış olur. Eğer bir kuruluş için normal süreç ve prosedür bilişim kaynaklarının satın alınması ise, kuruluş denetiminden geçmeden, kişisel veya departmana bağlı yapılan bir hata sonucu gizlilik ve güvenlikle ilgili zafiyetler ortaya çıkabilir (zafiyet içeren sistemlerin kullanılması, yasal düzenlemelerin göz ardı edilmesi gibi). Kuruluşların uygulamaların geliştirilmesi, uygulanması, test edilmesi ve izlenmesi ile alakalı prosedür ve standartları bulut bilişimi de kapsayacak şekilde genişletmesi faydalı olacaktır.

Bulut bilişimde kuruluş ile bulut sağlayıcısı arasında rollerin ve sorumlulukların belirlenmesinde özellikle risk yönetimine ve kuruluşun ihtiyaçlarının giderilmesi hususuna dikkat edilmesi yerinde olacaktır.

Bulut bilişim, güvenliğin sağlanması ve risk yönetimi hususlarında fazladan uğraş gerektirir. Kontrol mekanizmalarının ve araçlarının, hizmetlerin ve politikaların geçerliliğini koruması için, verinin nasıl depolandığını, korunduğunu ve kullanıldığını gösterecek şekilde yerleştirilmesi önerilir. Risk yönetim programının da risk faktörlerinin değişimini ve gelişimini takip edecek şekilde esnek olması, riski azaltacak önemli bir unsurdur.

4.2 Uyumluluk

Uygunluk bir kuruluşun işletim için yasalara, düzenlemelere, standartlara ve tanımlamalara olan sorumluluğunu ifade eder. Özellikle uluslararası çapta hizmet sunmayı hedefleyen bulut bilişim hizmet sağlayıcıları, yasaların bölgeden bölgeye farklılık göstermesinin tüm süreçleri karmaşıklaştıracağını göz önünde bulundurmalıdır.

- **Yasa ve Düzenlemeler:** Ülkemizde doğrudan bulut bilişimle alakalı yürürlükte olan bir

mevzuat bulunmamaktadır. Bununla birlikte, bilişim sistemleriyle doğrudan veya dolaylı olarak alakalı mevzuat hükümleri vardır. Ayrıca henüz yürürlüğe konmamış olmakla birlikte bulut bilişimle doğrudan alakalı mevzuat bileşenleri de vardır. Buna örnek olarak Kişisel Verilerin Korunması Kanun Tasarısı verilebilir. Yürürlükteki mevzuata ek olarak, yürürlüğe konması kuvvetle muhtemel kanun ve ilgili mevzuatın da göz önünde bulundurulması, bulut bilişim hizmet sağlayıcısı kuruluşun uyumluluk sorunlarını asgari düzeye indirecektir.

- **Veri Konumu:** Kuruluş içinde bulunan bilişim merkezleri kuruluşa yapı ve güvenlik konusunda bilginin nerede ve nasıl saklandığıyla ilgili detaylı denetim imkanı verir. Bulut bilişim sağlayıcıları ise genelde veriyi farklı lokasyonlarda saklar ve müşterilerle lokasyon bilgilerini paylaşmaz. Özellikle verinin sınır değiştirdiği durumlarda gizlilikle alakalı ülkelerin yasa ve düzenlemelerine bağlı belirsizlikler ortaya çıkar. Verilerin sınır ötesine taşınması ile ilgili asıl kaygılar, verilerin toplandığı bölgedeki yasaların veri akışına ve transferine izin verip vermemesi ve verinin ulaştırıldığı bölgenin yasalarının ek olarak oluşturduğu risk ve çıkarlardır. Örnek olarak Avrupa'dan belirlenmiş ülkeler haricinde kalan ülkelere taşınan veriler için Avrupa veri güvenliği yasalarına göre ek yükümlülükler uygulanmaktadır.
- **Elektronik Keşif:** Dava aşamasında veya yasal tedbirlerin bir gereği Elektronik Olarak Saklanan Bilgi (ESI- Electronically Stored Information)'nin tanımlanması, işlenmesi, analizi ve oluşturulmasını ifade eder. ESI elektronik postalar, ekler, bilgisayarlarda depolanan diğer veri çeşitleri ve depolama ortamlarının yanı sıra bütün metaveri (verinin oluşturulma ve değiştirilme tarihleri gibi özelliklerini tanımlayan veri) ve yorumlanamayan dosya içerikleri bilgisini de kapsar. Bulut bilişim sağlayıcılarının verinin orijinal metaverisi gibi bilgileri saklayabilecek ve işleyebilecek yeterlilikte olması beklenir. Aksi durumda kuruluşlar kasıtlı veya kasıtsız değişikliklerle yasalar karşısında mağdur durumda kalabilir.

Bulut bilişim hizmet sağlayıcılarının uyumluluk konusunda yaşayabileceği muhtemel sorunlar genel itibariyle mevzuat değişikliğiyle çözüme kavuşturulabilecek niteliktedir. Bu nedenle, bu Standart kapsamında konuya ilişkin önlem ve tedbirlere yer verilmemektedir.

4.3 Güvenilirlik

Bulut bilişimde kuruluşlar gizlilik ve güvenlikle ilgili bir çok konuda feragat ederler ve kontrolü bulut sağlayıcılarına bırakırlar. Bu bulut bilişim sağlayıcılara büyük bir sorumluluk yükler. Aynı zamanda kuruluşlarda bilginin güvenliğiyle ilgili ve bilgiye zarar verebilecek her türlü izinsiz erişim, değiştirme, bozulma gibi durumlar için risk ile zararın büyüklüğü arasında dengeyi sağlama konusunda sorumlulukları vardır.

- **İçeriden Erişim:** Bir kuruluşun fiziksel sınırları dışında işlenen veya depolanan veriler, güvenlik duvarı ve diğer güvenlik kontrolleri beraberinde riskleri de getirir. İç tehdit bulut bilişim için de geçerli bir sorundur. İç tehdit, eski veya halen çalışanlar, bağlı kuruluşlar ve diğer kuruluş sistemlerine, ağına girme yetkisi olanları kapsar. Bunun dışında kuruluş çalışanlarının kasıtsız ihmalleri de olabilir. Bu tehditin amacı sahtekarlık, sabotaj veya hassas bilgilerin çalınması olabilir.
- **Veri Mülkiyeti:** Kuruluşların veriler üzerindeki kullanım hakkına ve sahipliğine ilişkin

hususlar, bulut bilişim hizmet sağlayıcısı ile yapılan sözleşmede açık bir şekilde ifade edilmektedir. Sözleşme ile bulut bilişim sağlayıcıya veri üzerinde herhangi bir hak verilmemesi, fikri mülkiyet haklarının ve lisansların korunması ve sağlayıcının güvenlik nedeniyle dosyalara erişimle ilgili bir istekte bulunmaması gibi konularda bu sözleşmeler önemli rol oynamaktadır.

- **Birleşik Hizmetler:** Bazı hizmetler diğer hizmetlerle iç içe yada katmanlı biçimde çalışabilir. Örneğin Yazılım hizmetinin (SaaS) bazı kısımları Platform Hizmetinin (PaaS) veya Altyapı Hizmetinin (IaaS) üstünde çalışabilir. Hizmetlerinin bir kısmını üçüncü parti sağlayıcılar üzerinde barındıran bulut bilişim sağlayıcıları için kontrol alanının kapsamı, aradaki alt sözleşmeler, sorunların çözümü için müracaat imkânı üzerinde düşünülmelidir. Ayrıca bu durum sorumluluk ve performans konularında da ciddi sorunlar oluşturabilir (hizmetlerin yanıt verememesi gibi).
- **Görünürlük:** Bilgi güvenliğinde sistemin düzenli takibinin yapılması halihazırda kullanılan güvenlik kontrollerine ilişkin farkındalıkla zafiyetlerin ve tehditlerin izlenmesini gerektirir. Sistemin anlık durumunun analizi için verilerin toplanması, güvenlik ve gizlilikle ilgili risklerin belirlenmesi ve bunların kuruluşun tüm süreçleri için uygulanması gibi eylem adımlarının düzenli olarak kuruluşların ihtiyacına göre yapılması önerilir. Bulut hizmetine geçilmesiyle birlikte kuruluşun veri ve uygulamalarıyla ilgili sorumluluğu da bulut sağlayıcıya devredilir. Bu noktada düzenli takip için ilgili yaptırımların yerine getirilmesi bulut bilişim hizmet sağlayıcısıyla kuruluşun işbirliğini gerektirmektedir.

  Bulut bilişim hizmet sağlayıcısının güvenlik konusundaki tecrübesi, kuruluşunda risk yönetimini yapabilmesini sağlar. Ancak bulut bilişim hizmet sağlayıcıları gizlilik ve güvenlik konusunda uygulamalarıyla ilgili detayları vermekte gönülsüz olabilir. Çünkü bu hem şirketin fikri mülkiyet hakkı dâhilinde olabilir hem de kendilerine karşı bir saldırı için araç olarak kullanılabilir.

  Bulut bilişim hizmet sağlayıcılarında şeffaflık, birleşik hizmetleri de kapsayacak şekilde, kuruluşların sistemin gizliliği ve güvenliği hakkında tam bir denetim yapabilmesi için hayati önem taşır. Hizmet anlaşmalarının kuruluşun güvenlik denetimlerine ve süreçlerine göre bulut bilişim hizmet sağlayıcısı tarafından görünürlük sağlayacak şekilde yapılması , aynı zamanda prosedür ve politikaların da korunuyor olması önem taşımaktadır.
- **İkincil Veri:** Bulut bilişim hizmet sağlayıcıları uygulama verilerinin yanı sıra müşterilere ait önemli kullanıcı verilerini de saklar. Bulut bilişim hizmet sağlayıcıları aynı zamanda bu verilerin güvenliğini de sağlaması ve herhangi bir güvenlik ihlali durumunda sadece saklanan veriyi değil, verinin aynı bulut altyapısında tutulup tutulmadığından bağımsız olarak, ne hakkında olduğunu da raporlaması faydalı olacaktır.

  Bulut bilişim hizmet sağlayıcılarının müşterileri hakkında tuttuğu etkinlik raporları da ikincil veriler grubuna girer. Bu raporlarda kaynakların tüketimiyle ilgili bilgiler, günlük kayıtları (loglar), denetim kayıtları ve metaveriler olabilir. Sözleşmelerde toplanacak metaveriler ve bunların kullanılmasıyla (üçüncü parti şirketlere satılması ve paylaşılması dahil) ilgili hakların ve sahipliklerin belirlenmesi de göz önünde bulundurulması gereken önemli hususlardandır.

- **Risk Yönetimi:** Risk yönetimi; kurumsal faaliyetler, kurumsal varlıklar veya bir bilgi sisteminin çalışmasından kaynaklanan risklerin belirlenip değerlendirilerek bunun kabul edilebilir bir düzeye indirilmesi için gerekli adımları atma işlemidir. Süreç bilgi sisteminin güvenlik durumunun düzenli takibi için bir risk değerlendirmesinin yürütülmesi, riski azaltma stratejisinin uygulanması ve bunlarla ilgili teknikleri ve prosedürleri içerir. Genel bulut tabanlı sistemlerde de, geleneksel bilgi sistemlerinde olduğu gibi riskin her daim yönetilmesi bir zorunluluktur.

4.4 Mimari

Altyapının fiziksel konumu tasarıma, güvenliğe, kaynak havuzuna, ölçeklenebilirliğe ve başka ihtiyaçlara göre bulut sağlayıcılar tarafından belirlenir. Uygulamalar, internet üzerinden erişilebilen programlama arayüzleri üzerine kurulur. Bu internet tabanlı hizmet genelde birbiriyle iletişimde olan birden fazla bulut bileşenini içerir.

Bulut tabanlı uygulamalarda sunucu tarafını tamamlamak için istemci tarafını da başlatmak ve sürdürmek gerekir. Web tarayıcılar genelde istemci olarak çalışır. İstemcide, sunucuda ve ağ üzerindeki birçok basitleştirilmiş arayüz ve hizmetin arkasında gizlilik ve güvenlikle ilgili oldukça karmaşık bir yapı vardır. Bu nedenle bulut sağlayıcının gizliliği ve güvenliği sağlamak adına kullandığı teknolojilerin anlaşılması önemlidir.

- **Saldırı Tarafı:** Sanal makine takibi (Hypervisor) işletim sistemi ile donanım arasında bulunan ek bir yazılım katmanıdır. Bu uygulama da altyapı hizmetinde (IaaS) yaygın olarak kullanılan çok kiracılı (multi-tenancy) sanal makineler işletilir. Bunun yanı sıra sanal makine takibi ile diğer programlama arayüzleri için başlatma, durdurma, taşıma (migration) gibi yönetimsel işlemler de desteklenir. Ancak bu özellikler, sistemi uygulama programlama arayüzü, kanallar ve veri parçaları gibi bileşenlere yönelik saldırılara açık hale getirir.

  Sanal sunucuların ve uygulamaların güvenliğini sağlamak için fiziksel ve mantıksal ek tedbirler alınması faydalı olacaktır. Sanal makineler yayımlanmadan önce kuruluş politikalarının ve prosedürlerinin, ayrıca işletim sistemi ve uygulamalarının güvenlik açısından sıkılaştırılması başta gelen tedbirlerdir.

- **Sanal Ağ Koruması:** Pek çok sanallaştırma platformu aynı ana bilgisayarda sanal makineleri doğrudan ve verimli bir şekilde birbirine bağlamak için yazılım tabanlı anahtar ve ağ yapılandırmaları oluşturma yeteneğine sahiptir. Örnek olarak sanal makinelerin dışarıya açık olmayan özel bir alt ağda iletişim kurabilmesi verilebilir. Bazı sanal makine takibi araçları ağı izleme olanağı da sağlar ancak bunlar fiziksel ağların izlenmesi için kullanılan araçlar kadar kuvvetli değildir. Burada kuruluşlar trafiği gizlemekle trafiği izlemek arasında bir tercih yapmalıdır.

  Sanallaştırma ortamının bir yan etkisi de yönetimsel hakların geleneksel sistemlerdeki gibi olmaması ve bunun yetkisiz değişikliklerle çökmelere neden olabilmesidir.

- **Sanal Makine İmajları:** IaaS bulut sağlayıcıları ve sanal makine ürünleri üreticileri sanal makine görüntüleri için depolar (repository) oluştururlar. Bir sanal makine imajı bazı yazılımlara ihtiyaç duyar. Buna örnek olarak başlangıçtaki veya belirli bir zamandaki

durumunu önyüklemek için gereken yüklü ve yapılandırılmış uygulamalar verilebilir. Güvenlik problemleriyle karşılaşılmaması için oluşturulan ve paylaşılan imajların kontrol edilmesi ve araçların güncel tutulması gerekecektir. Ayrıca imajı yayımlayanlar için bir diğer risk faktörü de imaj içinde saldırganlara bilgi verebilecek kod ve veri parçacıklarının olması ihtimalidir. Özellikle geliştirme amaçlı kullanılan imajların yanlışlıkla paylaşılmasıyla sistem hakkında bilgi sahibi olan saldırgan, imaj içine zararlı yazılımlar yükleyebilir veya zararlı kodları barındıran imajlar müşterilerin bulut bilişim sistemine yayımlanabilir.

- **İstemci Tarafı Savunma:** İyi bir savunma için hem sunucu tarafında hem de istemci tarafında güvenliğin sağlanması gerekir. Özellikle web tarayıcılar birçok bulut bilişim hizmeti için anahtar bileşenlerdir. İçerdikleri eklentiler ve uzantılar ise otomatik güncelleme sağlanmadığı için bir güvenlik tehdidi oluşturur. Diğer bir tehdit ise akıllı telefonlardır. Bulut sağlayıcıları web tarayıcılarının yanı sıra mobil cihazlara yönelik uygulamalar da geliştirir. Çoğu zaman masaüstü uygulamalara verilen yama ve güncelleme desteği geniş bir platformda yaygınlaşan mobil uygulamalara verilemez veya ancak sınırlı ölçüde verilebilir. Buna ek olarak akıllı telefonların kaybolma riskleri ve ihtiyaç duyulan güvenlik gereksinimlerini karşılayamaması nedeniyle kuruluşlar bu tarz cihazları yasaklayabilir ya da kullanımını kısıtlayabilir.

  Sosyal ağlar, webmail hizmetleri ve buna benzer sitelerin kullanımının artmasıyla sosyal mühendislik saldırıları da artış göstermiştir. Bu tarayıcı güvenliğini ve buna bağlı olarak bulut bilişim hizmetini güvenlik tehdidi altında bırakır. Arka kapı açan bir truva atı, keylogger veya başka çeşit bir zararlı yazılım istemcinin sistemine yerleşmişse genel bulut bilişim hizmetine de saldırıda bulunulabilir.

4.5 Kimlik ve Erişim Yönetimi

Veri duyarlılığı ve bilgi gizliliği kuruluşların en çok endişe duyduğu konulardan biri haline gelmiştir. Kullanıcılardan toplanan verilerin güvenliği ve kullanımı için kimlik yönetimi yapılır. Kimlik ispatı ve denetimi bu adımın bir parçasıdır. Yetkisiz erişimi engellemek önemli bir sorun iken diğer bir sorun da kurumsal kimlik yönetiminin bulut hizmetiyle birleştirilememesidir. Bunun bir çözümü kimlik ittifakıdır. Kimlik ittifakında kuruluş ve bulut sağlayıcı etki alanları arasında dijital kimlikleri ve öznitelikleri paylaşabilmektedir ve bunu tek bir oturum açma ile sağlamaktadır. Başarı için kimlik ve erişim yönetiminin dikkatli, açık talimatlı ve saldırılara karşı koruyacak şekilde yapılandırılması gerekecektir.

- **Kimlik Denetimi:** Kullanıcı kimliklerinin doğruluğunun ve geçerliliğinin saptanmasıdır. Uygulama ve verinin hassasiyetine göre farklı denetim seviyeleri söz konusudur. Birçok bulut sağlayıcı SAML standartlarını destekler. SAML standartları ile uygulama ve verilere erişimden önce kimlik denetimi yapılır. Denetim için kuruluş ve bulut sağlayıcı etki alanlarındaki bilgiler kullanılır.
- **Erişim Denetimi:** SAML tek başına bulut tabanlı kimlik ve erişim yönetimi hizmetleri için yeterli değildir. Bunun için XML tabanlı XACML ile bulut sağlayıcı, bulut kaynaklarına erişim için kullanıcı yetkisine göre denetim sağlayabilir. XACML, SAML'nin yaptığı etki alanlarına erişim işlemine ulaşmayı sağlar.

4.6 Yazılım İzolasyonu

Çok kiracılı mekanizmaların kullanım yoğunluğu nedeniyle bulut bilişim hizmet sağlayıcılarının başarılı olmak için dinamik, esnek ve müşteri kaynaklarının izole edildiği bir yapı sağlaması önem taşımaktadır. IaaS modelinde çok kiracılı yapı kullanımı farklı müşterilerin sanal makinelerinin aynı sistem üzerinde çalıştırılması şeklinde olur. Bu durumda sanal olmayan makineler gibi sanal makineler de saldırıya ve gizlilik ihlaline açık hale gelir.

- **Sanal Makine Takibinin (Hypervisor) Karmaşıklığı:** Hypervisor ile birden fazla sanal makinenin, her biri farklı işletim sistemi ve uygulamaları çalıştıracak ve diğer sanal makinelerle arasında izolasyon sağlanacak şekilde tek bir ana bilgisayar üzerinde çalıştırılması sağlanır. Hypervisorun normal bir işletim sistemine göre daha basit ve güvenli olduğu düşünülebilir ancak pratikte durum bunun tam tersi de olabilir.
- **Saldırı Vektörleri:** Çok kiracılı sanal makine tabanlı sistemler kullandıkları ince teknolojilerle yeni tehditler de oluşturabilir. En kritik tehditlerden biri, sanal makinedeki zararlı kodların hypervisor vasıtasıyla diğer sanal makinelere bulaşmasıdır.

  Bir saldırı örneği olarak IaaS ele alınabilir. Farklı kullanıcılara ait sanal makineler çalıştırılıp ağ araçları, IP adresleri ve etki alanları kullanılarak hizmetin altyapısı hakkında bilgi alınır. Bundan sonra bu bilgilerle istenen belirli bir sanal makineye ait yaklaşık bilgiler elde edilebilir. İkinci adım olarak hypervisor yetkilendirme mekanizması aşılır veya çalışması durdurulur. Bunun dışında belleğe yazma konusundaki zayıflıklar, DoS, ortadaki adam (man-in-the-middle) gibi saldırılarla sistemin ele geçirilmesi de karşılaşılan örneklerdir.

4.7 Veri Koruması

Hassas kuruluş verileri bulut bilişim hizmet sağlayıcısında farklı müşteri verileriyle birlikte tutulur. Bu nedenle verilere erişim kontrol edilir. Alınan bu tedbir riskin tamamen ortadan kaldırılması için yeterli olmaz. Benzer güvenlik tehdidi verinin içeriden veya farklı bulut altyapıları arasında aktarıldığı durumlar için de geçerlidir.

- **Değer Yoğunluğu:** Bütün verinin tek bir yerde saklandığı bulut bilişim sistemi saldırıların en büyük hedefi haline gelmektedir. Örneğin IaaS ve PaaS gibi hizmetlerdeki parola sıfırlama, elektronik posta sisteminde bulunan zafiyetler saldırgana kimlik denetim mekanizmasını aşma imkanı verir. Öte yandan verilerin yüksek profilli bir kuruluşla aynı sistemde olması saldırılardan etkilenme ihtimalini artırır.
- **Veri İzolasyonu:** Veri izolasyonu, verinin kullanıldığı ortama göre çok farklı şekillerde yapılabilir. Erişim denetimi ve şifreleme veriyi yetkisiz kullanıcılardan uzak tutmak için kullanılan yöntemlerdir. Erişim denetimi kimlik bazlı işlem yaparken, şifreleme ile veri depolama ortamı fiziksel olarak kontrol edilemediği için güvenlik konusunda önemli hale gelmektedir.

  Bulut bilişimde kullanılan veritabanları da çeşitlilik gösterir. Bazı bulut bilişim hizmet sağlayıcıları müşterilerine tek sanal makine üzerinde çalışan tek bir veritabanı sunar. Burada tüm kontrol müşteriye verilir. Diğer alternatif ise bulut müşterisine göre tanımlanmış etiketleme sistemiyle öntanımlı bir veritabanı ortamının diğer kiracılara da paylaştırılmasıdır. Çok kiracılı ortamlar için verim ve izolasyon dengesini gözetecek

şekilde farklı ayarlamalar yapılabilir.

Verinin saklanması, işlenmesi ve transfer edilmesi esnasında güvenliğin etkin bir şekilde sağlanması ve erişim sırasında denetlenmesi önemli bir hususdur. İletişim protokolleri için kullanılan standartlar ve sertifikalar ile sağlanan şifreleme metodları IaaS, PaaS, SaaS için de uyarlanabilir.

- **Veri Temizleme (Sanitization):** Bulut bilişim hizmet sağlayıcısının uyguladığı veri temizleme yöntemleri güvenliği doğrudan etkiler. Temizleme işlemi, verinin üstüne yazılması, manyetik ortamının yok edilmesi, diğer yöntemlerle depolama ortamlarından silinmesi veya ortamın bilgi çıkarılamayacak şekilde imha edilmesi gibi yöntemlerle gerçekleştirilir. Bu işlem yedekleme ve geri yükleme sırasında ya da araçların sıfırlanıp yeniden kullanılması için kullanılabilir. Yaşanan olaylar göstermektedir ki ortamlar çalışmaz hale gelse bile çevrimiçi uygulamalar ve çeşitli araçlarla hassas veriler ele geçirilebilir. Veri temizlemesine yönelik hususlara hizmet sözleşmelerinde yer verilmesi, bu hususta yaşanabilecek muhtemel sorunların önüne geçecektir.

4.8 Kullanılabilirlik

Kullanılabilirlik, basit bir ifadeyle bir kuruluşun kaynaklarına ne ölçüde erişebildiğini ve kullanabildiğini ifade eder. Kuruluş; DoS saldırıları, ekipmanlarda yaşanabilecek kesintiler ve doğal felaketlerden geçici veya kalıcı olarak etkilenebilir.

- **Geçici Kesintiler:** Bulut bilişim hizmetleri kullanılabilirliği ve güvenilirliği yüksek olacak şekilde tasarlanmasına rağmen zaman zaman kesintiler ve yavaşlamalar yaşanabilir. Yıllık %99.95 erişilebilirlik ve 4.38 saatlik arıza süresi beklenen değerlerdir. Bulut bilişim hizmet sağlayıcısının kullanılabilirlik seviyesi, yedek alma ve felaket durumlarında geri kurtarma yetenekleri konusunda kuruluşlara planlama yapabilmeleri için bilgilendirme yapması gerekir. Bazı durumlarda ikinci bir bulut sağlayıcı hizmeti birincil sağlayıcıda uzun süreli bozulma ya da felaket durumunda, kritik operasyonların derhal yeniden başlatılması için ya da birincil sağlayıcı tarafından işlenen verileri yedeklemek için kullanılabilir.
- **Uzun Süreli ve Kalıcı Kesintiler:** Bir kuruluş veri depolama ve işleme için bir bulut hizmetine güveniyorsa, bu bulut hizmeti ciddi bir kesinti yaşadığında uzun süre bu hizmeti kullanmadan kritik faaliyetlerini sürdürmeye hazır olmalıdır. Kuruluşun acil eylem planında uzun ve sürekli kesinti durumlarının ve devamlılık için destek sisteminin kapsanması, bu konudaki muhtemel sorunları azaltacaktır.
- **Hizmet Dışı Bırakma:** Bu saldırı türü, bir sistemi sahte isteklerle, asıl isteklere yanıt veremeyecek şekilde çalışmaz hale getirmeyi amaçlar. Bu saldırı herkese açık hizmetlere internet aracılığıyla yapılabileceği gibi dahili olarak erişilen hizmetlere de yapılabilir. Bulut sağlayıcı ağında kaynaklara erişim için kullanılan adresler saldırı vektörü olarak kullanılabilir. Normalde bu adresler dışarıya yönlendirilmeyip sadece dâhili olarak erişime açıktır. Hizmetlerin sadece dahili erişime açık olduğu durumlar için en kötü senaryo çalışanlardan kaynaklanan saldırılardır.

4.9 Olay Müdahale

Olay müdahale, bir bilgisayar sisteminin güvenliğine karşı yapılan bir saldırının sonuçlarıyla başa

çıkmak için planlanmış yöntemler içerir. Bulut sağlayıcının olayın doğrulanması, saldırının analiz edilmesi ve engellenmesi, veri toplanması ve korunması, sorunun iyileştirilmesi ve hizmetin yeniden yapılandırılması dahil olmak üzere çok önemli görevleri bulunmaktadır. Bulut uygulama yığınındaki her katman (uygulama, işletim sistemi, ağ ve veritabanı), yük dengeleyicileri, saldırı tespit sistemleri gibi bileşenlerin olayla ilgili kayıt oluşturması önem arz etmektedir. Kuruluş açısından ise kurumsal bilgi işlem ortamı ile bir bulut bilişim ortamı arasındaki farklılıkları gidermek için bir kuruluşun olay müdahale planını gözden geçirmesi faydalı olacaktır.

- **Veri Kullanılabilirliği:** Güvenlik olaylarının zamanında tespit edilebilmesi için olay takibi sırasında ilgili verilerin kullanılabilirliği önem teşkil etmektedir. Bulut bilişim hizmet sağlayıcıları olay tespiti için sık sık yetersiz kalmaktadır. Sıkça karşılaşılan sorunlar; olay kaynaklarına ve bulut sağlayıcının kontrolü altındaki zafiyet bilgisine yetersiz erişim, otomatik olarak olay verilerine erişime ve işlemeye uygun olmayan arayüzler, bulut altyapısının ek algılama noktası eklemeye uygun olmaması, üçüncü taraftan raporlanan ihlallerin ve olayların doğru müşteriye veya bulut sağlayıcıya iletilmesi sırasındaki sorunlardır. Bu sorunlar bulut hizmet modellerine ve bulut sağlayıcılarına göre değişiklik gösterebilir.
- **Olay Analizi ve Çözümü:** Bir olayın gerçekleştiğinin tasdiki için veya hangi istismar metodunun kullanıldığına karar vermek için yapılan bir analizin hızlı ve yeterli detayları barındıracak şekilde belgelendirilmesi önem arz etmektedir. Ayrıca daha sonra kullanılmak üzere (örneğin adli vakalarda) izlenebilirlik ve bütünlük sağlanması gerekecektir. Bir olayı tam olarak kavramak için hangi ağların, sistemlerin, uygulamaların etkilendiği tespit edilerek saldırı vektörünün ortaya çıkarılması da bu süreçte gerçekleştirilecek bir diğer çalışmadır. Yapılan analizlerde bulut altyapısına dair gerçekleşen olayla alakalı ayrıntılı bilgilerin olmaması, bulut sağlayıcının ilgili olay hakkındaki yetersiz kaynakları, yeterince tanımlanamamış veya belirsiz durumlar için bulut sağlayıcılarının sorumluluktan kaçması ve olayla ilgili kanıt olabilecek bilgileri toplama ve sunmadaki yetersizlikler bulut müşterilerinin karşılaştığı sorunlardır. Olayın ve etkilenen varlıkların kapsamı belirlendikten sonra, olayı çözmek ve sistemi eski güvenli çalışma haline getirmek için önlemler alınabilir. Bir saldırı durumunda, bulut sağlayıcı ve bulut müşterisi arasındaki rol ve sorumluluklar hizmet modeli ve bulut mimarisine göre değişir.

Bir olayın ardından atılacak adımlar zararı sınırlamalı ve geri dönüşüm için gerekli maliyeti ve zamanı en aza indirmelidir. Bulut bilişimde gizlilik ve güvenliğin sağlanması için bir olayın tanımlanması ve gerekli adımların atılması sırasında bulut sağlayıcısı ile müşterisi arasındaki işbirliği hayati önem taşımaktadır.

Olaya müdahale ekibinin verimli olması için özerk ve kararlı bir çalışma içinde olması gerekir. Bir problemin çözümü diğer birçok müşteriyi etkileyebilir. Bulut sağlayıcılarının diğer müşterilerle de gerekli bilgileri paylaşması için olay sırasında ve sonrasında yaptığı işlemlerin şeffaf olması önem arz etmektedir. Olaya müdahaleyle ilgili koşulların ve prosedürlerin hizmet anlaşması yapılmadan önce anlaşılması ve tartışılması faydalı olacaktır.

5. Kontrol Listesi

Bu kontrol listesi, bulut bilişimle ilgili kontrollere genel bir bakış açısı kazandırılmasını amaçlamaktadır. Kolay kullanılabilirliğin temini için dokümanın sayfa sayısının az olması hedeflenmiş, bu nedenle kontrol listesi bileşenleri genel hatlarıyla açıklanarak faydalanılan kaynakla ilişkilendirilmiştir. Bileşenlerle ilgili detaylı bilgi ve açıklamalara ilgili kaynaktan ulaşılabilir.

KISA KONTROL	KONTROL	KAYNAK
1. Uyumluluk		
1.1 Denetim Planlaması	Denetim planlaması yapılmalı, denetim prosedürleri iş süreçlerini aksatmamalıdır.	CSA (CO-01)
1.2 Bağımsız Denetimler	Politika ve regülasyonlara uyumla ilgili bağımsız periyodik değerlendirmeler yapılmalıdır.	CSA (CO-02)
1.3 Üçüncü Parti Denetimleri	Üçüncü parti hizmet sağlayıcıların uyumluluğu periyodik olarak denetlenmelidir.	CSA (CO-03)
1.4 Kontakt / Otoritenin Devamı	Yerel otoriterlerle kontakt noktası kurulmalıdır (böylece teknolojide veya regülasyonda meydana gelen değişiklikler daha kolay takip edilerek mevcut sisteme yansıtılabilir).	CSA (CO-04)
1.5 Bilgi Sistemi Regülasyonel Eşleştirmesi	Tüm sistem bileşenleri için regülatif, hukuki ve sözleşmelerle ilgili gereksinimler tanımlanmalı. Kuruluşun bilinen gereksinimlere karşı yaklaşımı ve yeni zorunluluklara nasıl uyum sağlayacağı açıkça belirlenmeli ve güncel tutulmalıdır.	CSA (CO-05)
1.6 Telif Hakları	Telif hakları ve telif gerektiren yazılımlarla ilgili politika ve prosedürler oluşturulmalıdır.	CSA (CO-06)
2. Veri Yönetimi		
2.1 Sahiplik / İdare	Verilere yönelik sorumluluklar, yönetimle birlikte tayin edilmiş olmalıdır.	CSA (DG-01)
2.2 Sınıflandırma	Veriler kritiklik, veri kaynağı, mevcut konum gibi özelliklerine göre sınıflandırılmalıdır.	CSA (DG-02)
2.3 İşleme ve Etiketleme	Verilerin etiketlenmesi ve işlenmesi için politika ve prosedürler tanımlanmalıdır.	CSA (DG-03)

KISA KONTROL	KONTROL	KAYNAK
2.4 Veri Saklama Politikası	Veri saklama, yedekleme ve yedekli çalışabilme mekanizmaları regülatif vb. gereksinimler dikkate alınarak oluşturulmalı ve periyodik olarak test edilmelidir.	CSA (DG-04)
2.5 Güvenli İmha	Verinin güvenli ve tam olarak silinmesi için mekanizma ve prosedürler oluşturulmalıdır.	CSA (DG-05)
2.6 Üretim Ortamında Olmayan Veri	Üretim verisi, üretim ortamı haricindeki ortamlarda kullanılmamalıdır.	CSA (DG-06)
2.7 Veri Sızması	Veri sızmasını önleyecek güvenlik mekanizmaları oluşturulmalıdır.	CSA (DG-07)
2.8 Risk Değerlendirmeleri	Veri yönetimiyle ilgili risk değerlendirmeleri yapılmalıdır.	CSA (DG-08)
3. Tesis Güvenliği		
3.1 Politika	Güvenli bir çalışma ortamı için politika ve prosedürler oluşturulmalıdır.	CSA (FS-01)
3.2 Kullanıcı Erişimi	Varlık ve fonksiyonlara fiziksel erişim kısıtlanmalıdır.	CSA (FS-02)
3.3 Kontrollü Erişim Noktaları	Fiziksel güvenlik çemberi (duvarlar, bariyerler, kapılar, vb.) oluşturularak hassas verilerin ve bilgi sistemlerinin korunması sağlanmalıdır.	CSA (FS-03)
3.4 Güvenli Alan Yetkisi	Güvenli alanlara giriş ve çıkış fiziksel erişim kontrol mekanizmalarıyla kısıtlanmalıdır.	CSA (FS-04)
3.5 Yetkisiz İnsanların Girişi	Yetkisiz personelin giriş yapabileceği noktalar kontrol altında tutulmalı, bu noktalar veri depolama ve işleme birimlerinden izole edilmelidir.	CSA (FS-05)
3.6 Giriş-Çıkış Kayıtları	Kişilerin tesise giriş-çıkış kayıtları tutulmalı, personelle ilgili kayıtlar sistem üzerinden personel kimlikleriyle eşleştirilerek takip edilebilmelidir.	TSE
3.7 Tesis Dışı Yetkilendirme	Donanım, yazılım ve verilerin tesis dışında bulundurulması ve transferinden önce yetkilendirme yapılmalıdır.	CSA (FS-06)

KISA KONTROL	KONTROL	KAYNAK
3.8 Tesis Dışı Araç-Gereç	Tesis dışında kullanılacak araç-gereçlerin kullanımı ve güvenli imhası için politika ve prosedürler oluşturulmalıdır.	CSA (FS-07)
3.9 Varlık Yönetimi	Kritik varlıkların envanteri, sahiplikleriyle birlikte oluşturulmalı ve güncel tutulmalıdır.	CSA (FS-08)
4. İnsan Kaynakları Güvenliği		
4.1 Arka Plan Koruması	Tüm çalışan adayları, sözleşme yapılanlar ve üçüncü taraflar riskle orantılı şekilde arka plan doğrulamasına tabi olmalıdır.	CSA (HR-01)
4.2 İstihdam Sözleşmeleri	Bireyler tesise, sistemlere ve verilere erişim yetkisi verilmeden önce bilgi güvenliğiyle ilgili sorumlulukları belirleyen hizmet veya iş sözleşmelerini imzalamalıdır.	CSA (HR-02)
4.3 İstihdamın Sona Ermesi	İstihdam prosedürlerindeki değişiklikler veya istihdamın sona ermesiyle ilgili roller ve sorumluluklar belirlenmelidir.	CSA (HR-03)
5. Bilgi Güvenliği		
5.1 Yönetim Programı	Yönetimsel, teknik ve fiziksel güvenliği kapsayan bir Bilgi Güvenliği Yönetim Programı hayata geçirilmelidir.	CSA (IS-01)
5.2 Yönetim Desteği / Katılım	Üst yönetim ve ara yönetim kademeleri, bilgi güvenliğini desteklemek için açıkça dokümante edilmiş bir şekilde görevlendirme ve görevlendirmenin yerine getirildiğinin doğrulanması suretiyle faaliyet yürütmelidir.	CSA (IS-02)
5.3 Politika	Yönetim, liderler ve çalışanlar için rollerin ve sorumlulukların tanımlandığı resmi bir bilgi güvenliği politika dokümanını hayata geçirmelidir.	CSA (IS-03)
5.4 Asgari Gereksinimler	Uygulamalar, veritabanları, sistemler, ağ altyapısı ve bilgi işleme süreçlerini kapsayacak şekilde asgari güvenlik gereksinimleri hayata geçirilmeli ve en azından yıllık olarak yeniden değerlendirmelidir.	CSA (IS-04)
5.5 Politika Gözden Geçirmeleri	Yönetim, bilgi güvenliği politikasını planlanan aralıklarla veya kuruluşta değişiklik meydana geldiğinde yeniden gözden geçirmelidir.	CSA (IS-05)

KISA KONTROL	KONTROL	KAYNAK
5.6 Politika Yaptırımları	Güvenlik politika ve prosedürlerini ihlal eden çalışanlara yaptırım uygulanmalıdır.	CSA (IS-06)
5.7 Kullanıcı Erişim Politikası	Kullanıcı erişim politika ve prosedürleri hayata geçirilmelidir (uygulamalara, veritabanlarına, sunuculara ve ağ altyapısına normal ve özel erişim yetkilerinin verilmesi ve geri alınması, vb.).	CSA (IS-07)
5.8 Kullanıcı Erişim Kısıtlaması	Kullanıcıların uygulamalara, sistemlere, veritabanlarına, ağ konfigürasyonlarına ve hassas veri ve fonksiyonlara erişimi kısıtlanmalı ve yönetimin onayından geçmelidir.	CSA (IS-08)
5.9 Kullanıcı Erişim İptali	Herhangi bir değişim durumunda uygun zamanlamayla kullanıcı erişim yetkilerinin alınması veya değiştirilmesi sağlanmalıdır.	CSA (IS-09)
5.10 Kullanıcı Erişim Gözden Geçirmeleri	Tüm seviyelerdeki kullanıcı erişimleri yönetim tarafından planlanan aralıklarla gözden geçirilmeli, tespit edilen ihlallere yönelik politika ve prosedürler hazır olmalıdır.	CSA (IS-10)
5.11 Eğitim / Farkındalık	Sözleşme yapılanlar, üçüncü parti kullanıcıları ve kuruluş çalışanları için bir güvenlik farkındalık programı hayata geçirilmeli ve uygun olduğu durumlarda zorunlu tutulmalıdır.	CSA (IS-11)
5.12 Endüstri Tecrübesi / Standartlar	Networking, uzmanlaşmış güvenlik forumları ve profesyonel birlikler aracılığıyla endüstri güvenlik tecrübesi ve standartlar sürdürülmelidir.	CSA (IS-12)
5.13 Roller / Sorumluluklar	Sözleşme yapılanlar, çalışanlar ve üçüncü parti kullanıcılarının bilgi varlıkları ve güvenlikle ilgili konularda rolleri ve sorumlulukları belirlenmeli ve dokümante edilmelidir.	CSA (IS-13)
5.14 Yönetim Gözetimi	Yöneticiler, sorumluluk alanlarıyla ilgili güvenlik politika, prosedür ve standartlara uyum sağlamalı ve bunlara ilişkin farkındalık oluşturmalıdır.	CSA (IS-14)
5.15 Görev Ayrımı	Görevlerin belirgin bir şekilde ayrılması için politikalar, süreçler ve prosedürler tanımlanmış olmalıdır.	CSA (IS-15)
5.16 Kullanıcı Sorumluluğu	Kullanıcılar, bilgi güvenliği konusundaki sorumluluklarından haberdar edilmelidir.	CSA (IS-16)

KISA KONTROL	KONTROL	KAYNAK
5.17 Çalışma Alanı	Çalışma alanı boş olduğunda hassas veri barındıran görünür dokümanlar temizlenmeli ve sunucular belirli bir süre işlem yapılmadığında zaman aşımı durumuna geçmelidir.	CSA (IS-17)
5.18 Şifreleme	Hassas veriler depolama ünitesinde (dosya sunucuları, veritabanları, vb.) ve verinin taşınma anında (sistem arayüzleri, açık ağlar, elektronik mesajlaşma, vb.) şifrelenmelidir.	CSA (IS-18)
5.19 Şifreleme Anahtarı Yönetimi	Verinin saklanırken ve transfer esnasında şifrelenmesi için etkin anahtar yönetimi sağlanmalıdır.	CSA (IS-19)
5.20 Açıklık / Yama Yönetimi	Açıklık ve yama yönetimi için mekanizmalar tanımlanmalı; uygulama, sistem ve ağ cihazlarının zafiyetleri değerlendirilmeli ve risk odaklı yaklaşımla riski en fazla olandan başlanarak yamalar kurulmalıdır.	CSA (IS-20)
5.21 Antivirüs / Zararlı Yazılım	Antivirüs programlarının en geç 6 saatte bir güncellemeleri yapılarak bilinen zararlı yazılımlarla mümkün olan en iyi şekilde baş edebilmesi sağlanmalıdır.	CSA (IS-21)
5.22 Olay Yönetimi	Güvenlikle ilgili olaylar önceliklendirilmeli ve doğru zamanda derinlemesine olay yönetimi gerçekleştirilmelidir.	CSA (IS-22)
5.23 Olay Raporlama	Güvenlik olaylarında sözleşme yapılanlar, çalışanlar ve üçüncü parti kullanıcıları sorumluluklarından haberdar edilmeli ve güvenlik olayları önceden tanımlanmış iletişim kanalları üzerinden raporlanmalıdır.	CSA (IS-23)
5.24 Olay Müdahale Resmi Hazırlık	Güvenlik olayı gerçekleştikten sonra uygun adli bilişim yöntemleriyle delil zinciri oluşturulabilmelidir.	CSA (IS-24)
5.25 Olay Müdahale Metrikleri	Güvenlik olaylarının tipini, büyüklüğünü ve yol açtığı zararı değerlendirecek mekanizmalar tanımlanmalıdır.	CSA (IS-25)
5.26 Kabul Edilebilir Kullanım	Bilgi varlıklarının kabul edilebilir kullanımını belirleyen politika ve prosedürler oluşturulmalıdır.	CSA (IS-26)
5.27 Varlık İadeleri	Sözleşmenin sona ermesinin ardından çalışanlar, sözleşme yapılanlar ve üçüncü parti kullanıcıları belirlenmiş bir zamanda kuruluşun tüm varlıklarını iade etmelidir.	CSA (IS-27)

KISA KONTROL	KONTROL	KAYNAK
5.28 e-Ticaret İşlemleri	Açık ağda dolaşan e-ticaretle ilgili veriler uygun şekilde kategorize edilip güvenliği sağlanmalıdır.	CSA (IS-28)
5.29 Denetim Araçlarına Erişim	Kuruluşun bilgi sistemleriyle etkileşimde olan denetim araçları uygun şekilde bölümlere ayrılabilmeli (segmented) ve bunların kullanımı kısıtlanmalıdır.	CSA (IS-29)
5.30 Test / Konfigürasyon Portlarına Erişim	Kullanıcıların test ve konfigürasyon amaçlı portlara erişimi yetki bazında kısıtlanmalıdır.	CSA (IS-30)
5.31 Ağ / Altyapı Hizmetleri	Ağ ve altyapı hizmet seviyesi sözleşmeleri güvenlik kontrollerini, kapasiteyi, hizmet seviyelerini ve müşteri gereksinimlerini dokümante etmelidir.	CSA (IS-31)
5.32 Taşınabilir / Mobil Cihazlar	Taşınabilir cihazlardan (mobil cihazlar, tabletler, vb.) hassas verilere erişim daha sıkı kurallarla yetki bazında kısıtlanmalıdır.	CSA (IS-32)
5.33 Kaynak Kodu Erişim Kısıtlaması	Uygulama veya nesne kaynak koduna erişime, bilmesi gereken prensibine göre izin verilmelidir. Kodda yapılan değişiklikler detaylı olarak kayıt altında tutulmalıdır. Açık kaynak kodlu yazılım kullanılması durumunda bu gereksinim dikkate alınmayacaktır.	CSA (IS-33)
5.34 Yardımcı Uygulamalara Erişim	Sistem, nesne, ağ, sanal makine ve uygulama kontrollerinin yerini alma ihtimali olan yardımcı araçlar kısıtlanmalıdır.	CSA (IS-34)
6. Yasal Yükümlülükler		
6.1 Gizlilik Anlaşmaları	Gizlilik anlaşmaları için gereksinimler dokümante edilmeli ve periyodik olarak yenilenmelidir.	CSA (LG-01)
6.2 Üçüncü Parti Anlaşmaları	Kuruluşun veri ve varlıklarını doğrudan veya dolaylı etkileyen üçüncü parti anlaşmaları, ilgili tüm güvenlik gereksinimlerini kapsamalıdır.	CSA (LG-02)
7. Operasyon Yönetimi		
7.1 Politika	Tüm personelin hizmet operasyon rolünü destekleyebilmesi için politika ve prosedürler tanımlanmalıdır.	CSA (OP-01)

KISA KONTROL	KONTROL	KAYNAK
7.2 Dokümantasyon	Bilgi sistemleri dokümantasyonu (yönetim ve kullanım kılavuzları, mimari diyagramlar, vb.) yetkili personelin erişimine açık olmalıdır.	CSA (OP-02)
7.3 Kapasite / Kaynak Planlaması	Hedeflenen seviyede sistem performansı için kapasite ve sistem kaynakları planlanmalı, ileriye dönük projeksiyonlar yapılmalıdır.	CSA (OP-03)
7.4 Ekipman İdamesi	Operasyonların devamlılığını sağlayacak ekipman idamesi için politika ve prosedürler oluşturulmalıdır.	CSA (OP-04)
8. Risk Yönetimi		
8.1 Program	Kuruluşlar, riski belirli bir seviyede tutmak için kurumsal risk yönetimi geliştirmeli ve sürdürülmelidir.	CSA (RI-01)
8.2 Değerlendirmeler	Asgari yıllık olarak veya planlanan aralıklarla resmi (formal) risk değerlendirme işlemi yürütülmeli, bu esnada risklerin gerçekleşme olasılığı ve etkisi incelenmelidir.	CSA (RI-02)
8.3 Azaltma / Kabul	Riskler kabul edilebilir bir seviyeye indirilmelidir. Kabul seviyeleri oluşturulmalı ve yönetimin onayına sunulmalıdır.	CSA (RI-03)
8.4 İş / Politika Değişimi Etkileri	Risk değerlendirme sonuçları; güvenlik politikaları, prosedürler, standartlar ve kontrollerdeki değişiklikleri de kapsamalıdır.	CSA (RI-04)
8.5 Üçüncü Parti Erişimi	Kuruluşun bilgi sistemlerine ve verilerine üçüncü parti erişimle ilgili risklerin tanımlanması, değerlendirilmesi ve önceliklendirilmesinin ardından koordineli bir şekilde yetkisiz ve uygun olmayan erişimin etkisini düşürecek tedbirler alınmalıdır.	CSA (RI-05)
9. Sürüm Yönetimi		
9.1 Yeni Geliştirme / Temin	Yeni uygulamaların, sistemlerin, veritabanlarının, altyapının, hizmetlerin, tesislerin geliştirilmesi veya temininde Yönetim yetkilendirmesi için politika ve prosedürler oluşturulmalıdır.	CSA (RM-01)
9.2 Üretim Değişiklikleri	Üretim ortamındaki değişiklikler uygulama öncesi dokümante edilmeli, test edilmeli ve onaylanmalıdır.	CSA (RM-02)

KISA KONTROL	KONTROL	KAYNAK
9.3 Kalite Testi	Kuruluş tarafından geliştirilen tüm yazılımlarda kalite standartlarının sağlandığını temin edecek bir sistematik gözlem ve değerlendirme programı oluşturulmalıdır.	CSA (RM-03)
9.4 Dış Kaynaklı Geliştirme	Tüm dış kaynaklı yazılım geliştirmeleri için kalite standartlarının karşılandığından emin olunmasını sağlayacak bir gözlem ve değerlendirme sistematiği kurulmalıdır.	CSA (RM-04)
9.5 Yetkisiz Yazılım Kurulumu	Yetkisiz yazılım kurulumunu kısıtlayacak politika, prosedür ve mekanizmalar oluşturulmalıdır. Sunucu seviyesinde uygulama yönetiminin hizmet alıcıların sorumluluğunda olduğu Altyapı olarak Hizmet modelinde bu gereksinim uygulanmaz.	CSA (RM-05)
10. Dayanıklılık		
10.1 Yönetim Programı	Gerçekleşmesi muhtemel risk olaylarının etkisini kabul edilebilir bir seviyeye indirecek iş sürekliliği ve felaket kurtarma politika, süreç ve prosedürleri oluşturulmalı, ilgili paydaşlara tebliğ edilmelidir.	CSA (RS-01)
10.2 Etki Analizi	Kuruluşça verilen hizmetin aksamasının etkisini değerlendirecek dokümante edilmiş bir metot tanımlanmalıdır.	CSA (RS-02)
10.3 İş Sürekliliği Planlaması	İş sürekliliği planlaması ve plan geliştirme için tutarlı ve bütüncül bir çerçeve oluşturularak dokümante edilmeli ve bu planların test, idame ve bilgi güvenliği gereksinimleriyle uyumlu olması sağlanmalıdır.	CSA (RS-03)
10.4 İş Sürekliliği Testi	İş sürekliliği planlarının etkisinin sürdürülebilir olması için bu planlar belirlenen aralıklarla veya önemli organizasyonel veya çevresel değişikliklerde test edilmelidir.	CSA (RS-04)
10.5 Çevresel Riskler	İnsan eliyle veya doğal olarak gerçekleşen felaketler (yangın, sel, vb.) tahmin edilmeli, tasarlanmalı ve karşı önlemler alınmalıdır.	CSA (RS-05)

KISA KONTROL	KONTROL	KAYNAK
10.6 Ekipman Konumu	Ekipmanın çevresel risk faktörlerinden ve yetkisiz erişim riskinden etkilenmemesi için ekipman bu tür risk ihtimallerinin bulunduğu alanlardan uzakta konumlandırılmalı ve makul uzaklıkta konumlandırılmış yedek ekipmanlarla desteklenmelidir.	CSA (RS-06)
10.7 Ekipman Güç Arızaları	Ekipmanın güç kesintilerinden (güç arızası, ağ kesintisi, vb.) korunması için güvenlik ve yedeklilik mekanizmaları oluşturulmalıdır.	CSA (RS-07)
10.8 Güç / Telekomünikasyon	Telekomünikasyon ekipmanı, kablolama ve relay'ler veya destek hizmetleri çalışmama veya hasar görmeye karşı korunmalı; yedekler, alternatif güç kaynakları ve/veya rotalarla tasarlanmalıdır.	CSA (RS-08)
11. Güvenlik Mimarisi		
11.1 Müşteri Erişim Gereksinimleri	Müşterilere verilere, varlıklara ve bilgi sistemlerine erişim yetkisi verilmeden önce müşterilerin tanımlanmış olan güvenlik, sözleşmeyle ilgili ve regülasyonel tüm gereksinimleri adreslenmeli ve düzenlenmelidir.	CSA (SA-01)
11.2 Kullanıcı Kimliği Kanıtları	Uygulamalar, veritabanları, sunucular ve ağ altyapısı için kullanıcı kimlik ve şifre kontrolleri otomasyon yöntemiyle implemente edilmeli ve zorunlu tutulmalıdır.	CSA (SA-02)
11.3 Veri Güvenliği / Bütünlüğü	Farklı sistem arayüzleri, farklı yargı alanları veya herhangi bir üçüncü parti hizmet sağlayıcılar arasında aktarılan verilerin güvenliği ve bütünlüğünü garanti edecek politika ve prosedürler oluşturulmalı, mekanizmalar hayata geçirilmelidir.	CSA (SA-03)
11.4 Veri Bütünlüğü	Veri giriş ve çıkış bütünlük rutinleri (örneğin çapraz kontroller ve değişiklik kontrolü), verinin işlendiği ve aktarıldığı ortamlar için implemente edilmelidir.	CSA (SA-05)
11.5 Üretim Ortamı ve Diğer Ortamlar	Bilgi varlıklarına yetkisiz erişim veya yetkisiz değişikliklerin önlenmesi için üretim ortamı ve diğer ortamlar birbirinden ayrı olmalıdır.	CSA (SA-06)
11.6 Uzak Kullanıcı Yetkilendirme	Tüm uzak kullanıcı erişimleri için çok aşamalı yetkilendirme kullanılmalıdır.	CSA (SA-07)

KISA KONTROL	KONTROL	KAYNAK
11.7 Ağ Güvenliği	Ağ ortamları güvenli ve güvensiz ağlar arasındaki bağlantıları kısıtlayacak şekilde tasarlanmış ve konfigüre edilmiş olmalı ve planlanan aralıklarla gözden geçirilmelidir.	CSA (SA-08)
11.8 Dağıtık Hizmet Engelleme Koruması	Dağıtık hizmet engelleme saldırılarına yönelik tedbirler alınmalı, belirli bir müşteriye veya müşteri grubuna yönelik saldırılardan diğer müşterilerin etkilenmeyeceği şekilde idari ve teknik önlemler alınmalıdır.	TSE
11.9 Bölümlere Ayırma	Sistem ve ağ ortamları güvenlik duvarlarıyla bölümlere ayrılmalıdır.	CSA (SA-09)
11.10 Kablosuz Güvenliği	Kablosuz ağ ortamlarını korumak için politika ve prosedürler oluşturulmalı ve mekanizmalar hayata geçirilmelidir.	CSA (SA-10)
11.11 Paylaşılan Ağlar	Paylaşılan ağlar üzerinden sistemlere erişim yalnızca yetkili personelin erişimine açık olacak şekilde kısıtlanmalıdır. Harici birimlerle paylaşılan ağlar, kuruluşlar arasındaki ağ trafiğini ayrıştıracak kontrollerin detaylandırıldığı dokümante edilmiş planlara sahip olmalıdır.	CSA (SA-11)
11.12 Saat Senkronizasyonu	Üzerinde mutabakata varılmış, güvenilir bir harici zaman belirleyici kullanılarak kuruluşa ait ilgili tüm bilgi işleme sistemlerinin ve ihtiyaç duyulan diğer güvenlik birimlerinin sistem saatleri senkronize edilmelidir.	CSA (SA-12)
11.13 Ekipman Tanıma	İletişim yetkilendirmesi için otomatize ekipman tanıma kullanılmalıdır. Konumu bilinen cihazlar için lokasyon tespit cihazlarıyla iletişim yetkilendirmesi bütünlüğü sağlanabilir.	CSA (SA-13)
11.14 Ekipman Tasfiyesi	İptal edilmiş ürünlerin, aktif olmayan sanal makinelerin ve anlık durum görüntülerinin (snapshot) silinmesine ilişkin bir politika geliştirilmeli ve uygulanmalıdır.	CloudControls
11.15 Denetim Loglama / Saldırı Tespit	Yetkili kullanıcı erişim eylemleri, yetkili ve yetkisiz erişim girişimleri, sistem istisna hataları ve bilgi güvenliği olaylarının kaydedildiği denetim logları sürdürülmelidir. Denetim logları en azından günlük olarak gözden geçirilmeli ve ağ saldırı tespit cihazları kullanılarak vakitlice tespit ve inceleme gerçekleştirilebilmelidir.	CSA (SA-14)

KISA KONTROL	KONTROL	KAYNAK
11.16 Mobil Kod	Mobil kod, yükleme ve kullanımdan önce yetkilendirilmeli ve yetkilendirilmiş mobil kod konfigürasyonunun açıkça tanımlanmış güvenlik politikasına uygun işlediğinden emin olunmalıdır.	CSA (SA-15)
11.17 Müşteri Bazında Soyutlama	Müşterilerin çalışma ortamını müşteri bazında ayrıştırmak mümkün olmalıdır.	CloudControls
12. Müşteri İlişkileri		
12.1 Müşteri Verisinin ve Donanımının Korunması	Mahkeme çağrısı durumunda, Bulut Hizmet Sağlayıcısı (BHS) yürürlükteki mevzuatın izin verdiği ölçüde diğer müşterilere ait veri ve donanıma el konmaması için ticari açıdan makul karşı önlemleri almalıdır.	CloudControls
12.2 Tek Taraflı Sözleşme Değişiklikleri	BHS, hizmet seviyesi sözleşmesini, iş koşullarını veya diğer anlaşmaları müşterinin isteğine muhalif olarak tek taraflı değiştirmemelidir.	CloudControls
12.3 Kısa Dönemli Sözleşmeler	Kısa dönemli sözleşme yapılabilmesine imkan tanınacaktır.	CloudControls
12.4 Müşteri Verisinin Dışa Aktarımı	Müşteri verisi endüstri standartlarına uygun bir formatta dışa aktarılabilir olmalıdır.	CloudControls
12.5 Risklerin Müşteriye Tebliği	BHS, talep edildiğinde el koyma, hizmet sağlayıcısının faaliyetinin sona ermesi, firma bağımlılığı riski ve BHS sahipliğinin değişmesi risklerine ilişkin bilgi sağlamalıdır.	CloudControls
12.6 Hizmet Seviyesi Sözleşmeleri	Hizmet seviyesi sözleşmesinin gereklerinin nasıl yerine getirileceği tanımlanmalı, takip edilmeli ve müşterilere tebliğ edilmelidir. Bir ihlal durumunda hizmet seviyesi sözleşmesinden uyumluluğa geri dönüş için prosedürler tanımlanmış olmalıdır. HSS tesliminin uyumluluk kapsamı dışında olduğu durumda müşteriler göçün gerçekleşmesini kolaylaştıracak makul bir süre için ücret ödemeksizin göçü gerçekleştirme ve ürünlerini alma avantajına sahip olacaklardır.	CloudControls

KISA KONTROL	KONTROL	KAYNAK
12.7 Hizmet Zamanı İhlali	Sağlam bir hizmet zamanı ihlal tazminat sistemi mevcut olmalıdır. Bir hizmetin ulaşılabilirliği, BHS ağının uç kısmından ulaşılabilirlik anlamına gelir. Asli ürün bileşenlerinin erişilmez olması hizmetin kapalı olduğunu gösterir. Önceden duyurusu yapıldığında, hizmetlerin bakımı hizmet zamanı ihlali olarak değerlendirilmez.	CloudControls
12.8 Standartlara Uyum ve Bilgilendirme	BHS denetim ilkelerini, kontrolleri ve sonuçları yayınlamalıdır. Eğer bir denetim BHS'nin taahhüt ettiği standartlarla uyum sağlamadığını ortaya çıkarırsa, konuyla ilgili müşteriler bilgilendirilmelidir. BHS makul bir sürede standardı tekrar uyumlu hale getirmeli, standart tekrar uyumlu hale getirilmezse müşterilerin zararı tazmin edilmelidir.	CloudControls
12.9 Kaynak Harcama Bilgilendirmesi	Müşteri, kendi ismi kullanılarak yapılan aşırı kaynak talepleri hakkında bilgilendirilmelidir. Müşterilerin bilgisi haricinde harcama limitinin üzerine çıkması mümkündür.	CloudControls
12.10 Faaliyetin Sona Ermesi	BHS'nin beklenmedik bir şekilde faaliyetlerine son vermesi durumunda veri ve varlıklara erişimi garanti altına alacak bir anlaşma mevcut olmalıdır.	CloudControls
12.11 Sözleşme Feshi	BHS, ancak kanuni gereksinim varsa, hizmet alımına karşılık ödeme yapılmıyorsa veya kabul edilebilir kullanım politikası ihlali varsa kısa süreli uyarma ile müşteri sözleşmesini feshedebilir. Bu durumda müşteri mümkünse önceden uyarılmalı ve müşterinin verilerine ulaşabileceği bir prosedüre imkân tanınmalıdır.	CloudControls
12.12 Hizmetlerin Askıya Alınması	BHS bir müşteriye verdiği hizmeti ancak kanuni gereklilik durumunda, hizmetler için ödeme yapılmadığında veya adil kullanım politikası ihlali düzeltilmediği veya diğer müşterilerin hizmetleri tehdit ettiği durumlarda askıya alabilir. Müşteri mümkün olduğu durumlarda önceden uyarılmalı ve hizmetler mümkün olan en kısa sürede tekrar kullanıma sunulmalıdır.	CloudControls
12.13 Veri Konum Bilgisinin Paylaşımı	Müşteri verinin hangi yargı birimlerinin yetki sınırları içinde tutulduğunu kendisine sağlanan arayüz aracılığıyla tespit edebilmelidir. Hangi ülkelerin ve yargı birimlerinin müşteri verisi üzerinde hak iddia edebilecekleri müşteriye bildirilmelidir.	CloudControls

KISA KONTROL	KONTROL	KAYNAK
12.14 Olay Soruşturması İşbirliği	BHS müşterinin her türlü makul olay soruşturmasında işbirliği yapmalıdır. Buna ilgili denetim günlük kayıtlarının teslimi de dahildir (gizlilik taahhütleri dikkate alınacaktır).	CloudControls
12.15 Veri Sahipliği	Müşteri verisi her zaman müşteri sahipliğinde kalmalıdır. BHS hak iddia ettiği her türlü telif hakkına ilişkin bildirimde bulunmalıdır.	CloudControls
12.16 Kanuni Taleplerin İcrası	BHS, ilgili mevzuat çerçevesinde, durdurma ve bırakma ya da mahkeme çağrısına müşterinin gereksinimleri doğrultusunda karşı koymak için ticari açıdan makul bir çaba harcayacağını taahhüt eder. Müşteriyi kanuni bir talep veya istek konusunda bilgilendirmeye izin verilmiyorsa, BHS müşterinin böylesi bir talebe karşı koymak isteyeceğini varsaymalıdır.	CloudControls
12.17 Müşteri Verisi Mahremiyeti	BHS teknik açıdan gerekli olmadığında veya sunmakta olduğu altyapıya karşı bir yanıltma veya saldırıya karşı koymak için olmadığında müşteri verisini araştırmamalı, analiz etmemeli veya kaydetmemelidir. Müşteri verisi müşterinin talebi durumunda imha edilmelidir. Müşteri verisinin soyutlanmasına ilişkin politika müşteriye bildirilmeli ve bu denetlenmelidir. Müşterinin talebi durumunda BHS personelinin erişim hakları ve müşterinin çalışma ortamıyla ilgili işlem logları müşterinin erişimine açılmalıdır. BHS'nin müşterinin çalışma ortamına erişimi engellenebilmelidir (yasal gereksinimler hariçtir).	CloudControls
12.18 Müşteri Erişim Kontrolleri	Müşteri yönetim arayüzleri, sadece bireysel erişime imkân tanıyan usule uygun bir erişim kontrol modeline sahip olmalıdır. Veri bozulmasıyla sonuçlanabilecek eylemler için ilave kontroller yapma imkânı olmalıdır. Müşteri yönetim arayüzüne erişim hakları, müşteri tarafından kolaylıkla değiştirilebilmelidir. Sözleşme bitimi sebebiyle erişim haklarının azaltılması veya müşterinin bir çalışanını ilgilendiren erişim haklarının azaltılması anında ve eksiksiz bir şekilde uygulanmalıdır.	CloudControls
12.19 Erişilebilirlik Bilgi Paylaşımı	Gerekli olduğu durumlarda, felaket kurtarma planları ve erişilebilirlik artırıcı önlemler müşterilerle paylaşılmalıdır.	CloudControls

KISA KONTROL	KONTROL	KAYNAK
12.20 Bilgi Sistemlerindeki Değişiklikler	Bilgi sistemindeki değişikliklerle ilgili bilgi sağlama hakkında prosedürler oluşturulmalı ve uygulanmalıdır. BHS yeni bilgi sistemleri tedariki ve iyileştirmelerle ilgili kontrollerini beyan etmelidir. BHS müşteriler tarafından kullanılan mevcut teknolojileri sürdürmek için gerekli çabayı sarf etmelidir. Bu tür teknolojiler kullanımdan kalkma sürecinde olduğunda geçiş süreci uygulanabilir.	CloudControls
12.21 Müşteri Zafiyet Değerlendirmesi	BHS müşteriler tarafından, müşterilerin sahipliğinde bulunan bileşenlere yönelik zafiyet değerlendirmesi yapılabilmesine imkân tanımalı ve zafiyet değerlendirmesi politikası hakkında bilgi sağlamalıdır.	CloudControls
12.22 İhlal ve Hata Bilgilendirmesi	Müşteriyi etkileyebilecek bir mahremiyet ihlali, güvenlik ihlali veya teknik hata durumunda müşterilerin bilgilendirileceği bir politika mevcut olmalıdır. Hata logları politikası açıkça bildirilmeli ve ilgili loglar müşterinin talep etmesi durumunda erişime açılmalıdır.	CloudControls
12.23 Kullanılan Kaynak Raporlama	HSS performansıyla, kullanılan ve ücretlendirilebilir kaynaklarla ilgili detaylı raporlama imkanı mevcut olmalıdır.	CloudControls
12.24 Ek Hizmet Bilgilendirmesi	BHS, sunduğu ilişkili hizmetlerle ilgili olarak (örneğin kullanılan şifreleme, BHS ile mobil etkileşim hususunda bilgi gibi) açıklama sağlamalıdır.	CloudControls
12.25 Yönetim Arayüzü Erişilebilirliği	Yönetim arayüzü için erişilebilirliği artıracak önlemler mevcut olmalıdır.	CloudControls
12.26 Personel Yetkisi	Müşteri personelinden alınan talepler ancak onun daha önceden tanımlanmış yetki seviyesi dikkate alınarak yetkili olması durumunda yerine getirilmelidir.	CloudControls

Referanslar

NIST, Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards and Technology, Draft Special Publication 800-144, USA.

CSA, Security Guidance, v3, Cloud Security Alliance, November 2011.

CSA, Cloud Controls Matrix, v1.4, Cloud Security Alliance, March 2013.

CloudControls, Cloud Control Framework (Controls, Risks and Customer Questions), Cloud Controls Project, Netherlands, (online) <http://www.cloudcontrols.org> (last accessed on 7th March, 2014).