BULUT SERVİSLERİ GÜVENLİĞİ POLİTİKASI
(Doc # ACT-ISM-POL-13)

REVISION DATE: 02.02.2024
REVISION NO: 00

ADDRESS	Yenisehir Mh. Mustafa Akyol Sokak No:7 A Blok Kat 3-4 Arwen – Merlin Ofis , 34912 Pendik Istanbul / TURKEY
PHONE	+ 90 216 588 10 20
FAX	+ 90 216 588 10 19
WEB	www.actairlines.com
E – MAIL	info@actairlines.com

İÇİNDEKİLER

1. AMAÇ 5
2. KAPSAM 5
3. SORUMLULUKLAR 5
4. UYGULAMA 5
4.1 BULUT SERVİSLERİ ÖZELLİKLERİ 5
4.2 BULUT SERVİS ÇEŞİTLERİ 6
4.3 BULUT SERVİS DAĞITIM MODELLERİ 6
4.4 BULUT SERVİSLERİ GEREKSİNİMLERİ 6
4.4.1 STRATEJİ VE POLİTİKA 6
4.4.2 AĞ SEGMENTASYONU 6
4.4.3 KİMLİK VE ERİŞİM YÖNETİMİ İLE AYRICALIKLI ERİŞİM YÖNETİMİ 7
4.4.4 BULUT ÖRNEKLERİ VE VARLIKLARI 7
4.4.5 ŞİFRE KONTROLÜ (AYRICALIKLI VE AYRICALIKSIZ ŞİFRELER) 7
4.4.6 GÜVENLİK AÇIĞI YÖNETİMİ 7
4.4.7 ŞİFRELEME (ENCRYPTION) 7
4.4.8 OLAĞANÜSTÜ DURUM KURTARMA 7
4.4.9 İZLEME, UYARI VE RAPORLAMA 7
4.5 BULUT SERVİSLERİ GÖREV VE SORUMLULUKLAR 8
4.5.1 SİSTEM YÖNETİMİ EKİBİ 8
4.5.2 SİBER GÜVENLİK EKİBİ 8
4.6 BULUT SERVİSLERİ GÜVENLİK TEHDİTLERİ 8
4.7 BULUT SERVİSLERİ RİSKLERİ 10
4.7.1 KURUMSAL VE STRATEJİK RİSKLER 10
4.7.2 TEKNİK RİSKLER VE GÜVENLİK RİSKLERİ 10
4.7.3 HUKUKSAL RİSKLER 10
4.8 BULUT SERVİSLERİ ÇIKIŞ STRATEJİSİ 11

REVİZYONLAR

REV.NO	REVİZYON KONUSU	TARİH	UYGULAYAN
00	İlk Yayın	02.02.2024	Bilgi Güvenliği Uzmanı
01			
02			
03			
04			
05			
06			
07			
08			
09			
10			
11			
12			
13			
14			

Kopya No/Format	Dağıtım Listesi
00-pdf	Master (Bilgi Güvenliği Müdürlüğü)
01-pdf	ACT Airlines Intranet Sistemi

1. AMAÇ

Bu politikanın amacı bulut hizmetlerinin edinilmesi, kullanılması, yönetimi ve bulut hizmetlerinden çıkış süreçleri, kuruluşun bilgi güvenliği gerekliliklerine uygun yönetilmesinin sağlanmasıdır.

2. KAPSAM

Bu politika tüm bilgi sistemleri altyapısı ve tedarikçiler üzerinden sağlanan bulut hizmetlerini kapsar.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından ve altyapı gereksinimlerinin sağlanmasından Bilgi Teknolojileri, sürecin bilgi güvenliği kriterleri açısından değerlendirilmesi ve denetlenmesinde Bilgi Güvenliği ve tüm personel belirlenen politikaya uygun kullanımdan sorumludur.

4. UYGULAMA

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) özel yayınına göre “bulut bilişim, minimum yönetim çabası veya hizmet sağlayıcı etkileşimi ile hızlı bir şekilde sağlanabilen ve piyasaya sürülebilen, yapılandırılabilir bilgi işlem kaynaklarından oluşan paylaşılan bir havuza her yerde, uygun, isteğe bağlı ağ erişimini sağlamak için bir modeldir." Bu tanıma göre bulut bilişim ile bilgi işlem kaynaklarına ve tesislerine her zaman ve her yerden erişim sağlanabilmektedir. Merkezi bulut güvenliğinin amacı, BT ekiplerine ortak bir tehdide ilişkin anında bildirim göndermektir. Bu proaktif yaklaşım ile şirketlerin, hem DDoS gibi yıkıcı saldırılardan hem de veri ihlalleri gibi daha büyük tehditlerden korunabilmesi amaçlanmaktadır. Bir bulut güvenlik stratejisini uygulamaya koymadan önce, güvenlik ekiplerinin mevcut tüm bulut denetimlerini değerlendirmesi ve bunların merkezileştirilmiş olup olmadığına karar vermesi gerekmektedir:

4.1 BULUT SERVİSLERİ ÖZELLİKLERİ

Bulut bilişimin beş ana özelliği bulunmaktadır: kaynak havuzu, geniş ağ erişimi, hızlı esneklik, isteğe bağlı self servis ve ölçülen hizmet.

- **Paylaşılan kaynaklar:** istemciler, ağlar, sunucular, depolama, yazılım, bellek ve işleme gibi kaynakları aynı anda paylaşabilir. Sağlayıcılar, talepteki dalgalanmalara göre kaynakları dinamik olarak tahsis edebilir ve müşteri bu hizmetlerin fiziksel konumlarından tamamen habersizdir.
- **Geniş ağ erişimi:** bulut, herhangi bir cihazdan İnterneti kullanarak ağa geniş erişim sağlar.
- **Esneklik:** bulut esnektir ve yapılandırılabilir. Müşteriler, kaynakların sınırsız olduğunu hissederler.
- **İsteğe bağlı self servis:** gerekirse herhangi bir müşteri, servis teknisyenlerinin müdahalesi olmadan bulutu otomatik olarak yapılandırabilir. Müşteriler zamanlamayı gerçekleştirir ve gerekli depolama ve bilgi işlem gücüne karar verir.
- **Ölçülen hizmet:** farklı bulut hizmetleri, farklı metrikler kullanılarak ölçülebilir. Müşterilerin ve sağlayıcıların haklarını korumak için detaylı kullanım raporları oluşturulur.

4.2 BULUT SERVİS ÇEŞİTLERİ

Hizmet Olarak Yazılım (SaaS)
Bulut hizmet sağlayıcısının; bulut uygulama yazılımını geliştirip koruduğu, otomatik yazılım güncellemeleri sağladığı ve müşterileri için İnternet üzerinden kullandıkça ödeme olanağına sahip yazılımlar sunduğu bir hizmet modelidir.

Hizmet Olarak Platform (PAAS)
Müşterilerin mevcut altyapıya yatırım yapmadan veya altyapıyı muhafaza etmeden oluşturmaya ihtiyaç duydukları geliştirici araçlarına erişmesine, mobil ve web uygulama yazılımlarını yönetmesine olanak tanır. Kuruluşların altyapı (genelde donanım ve işletim sistemleri) yönetimi ihtiyacını ortadan kaldırarak uygulama dağıtma ve yönetim alanlarına odaklanmasını sağlamaktadır.

Hizmet Olarak Altyapı (IAAS)
Müşterilerin internet üzerinden altyapı servislerine istedikleri zaman erişmelerini sağlar. bulut BT sistemi için temel yapı taşlarını içerir ve genelde ağ özelliklerine, bilgisayarlara (sanal veya tahsis edilmiş donanımda) ve veri depolama alanına erişim sunmaktadır.

4.3 BULUT SERVİS DAĞITIM MODELLERİ

Özel Bulut (Private Cloud)
Şirket içinde, intranet üzerinde, güvenlik duvarının arkasında bulunur ve genellikle onu kullanan aynı kuruluş tarafından yönetilmektedir. Özel bir iç ağ üzerinden yapılan kısıtlamalarla belirli kullanıcılara sunulan bilgi işlem hizmetidir..

Genel Bulut (Public Cloud)
Şirket dışında, internet üzerinden bulunmaktadır ve genellikle bir bulut hizmeti sağlayıcısı tarafından yönetilmektedir. Özel buluttan daha az güvenlidir. Elektronik postalara para ödemeden üçüncü bir şirket üzerinden kiralanacak kaynaklar üzerinden çeşitli özellikleri kullanılabilmektedir.

Hybrit Bulut
Public (Genel) ve Private Cloud (Özel Bulut)'un tüm özelliklerinin birleşiminden ortaya çıkmıştır. Bu hibrit bulut özelliği sayesinde güvenlik ve gizlilik ön plandadır.

Topluluk Bulut (Community Cloud)
Bulut'un üzerinde alınan herhangi bir hizmetin birkaç şirket ile ortak kullanılması durumuna denmektedir. Birden çok firması olan işletme sahipleri için uygun bir bulut teknolojisidir.

4.4 BULUT SERVİSLERİ GEREKSİNİMLERİ

4.4.1 STRATEJİ VE POLİTİKA

Bütünsel bir bulut güvenlik programı, bulut güvenlik risklerinin sahipliğini ve sorumluluğunu, koruma kap-samındaki boşlukları hesaba katmalıdır. Program, bulut bilişim güvenliği sisteminin güvenilirliğini olgunlaştırmak ve istenen son duruma ulaşmak için gereken kontrolleri tanımlamalıdır.

4.4.2 AĞ SEGMENTASYONU

Ağ segmentasyonu, bulut bilişim sisteminin erişilebilir bölgeleri arasında hangi hizmetlere izin verildiğine ilişkin katı kurallar belirlemenize olanak tanıyan kanıtlanmış bir güvenlik stratejisidir. Bu sistem bölgeler içinde hassas verilerin ve kaynakların belirlenmesi, yalnızca belirlen-miş ana bilgisayarların ve diğer onaylanmış bölgelere ait kullanıcıların bunlara ulaşmasını sağlar. Bu sayede ağ boyunca hareketler zorlaştırılarak saldırılar kısıtlanabil-mektedir. Bilgisayar korsanları ve kötü amaçlı yazılımlar, veri sızdırmak için sisteme erişemez, ayrıca engellenen kötü amaçlı bağlantılar kritik varlıkları tespit etmek için bağlantı noktası taraması da yapamaz.

4.4.3 KİMLİK VE ERİŞİM YÖNETİMİ İLE AYRICALIKLI ERİŞİM YÖNETİMİ

Kimlik ve erişim yönetimi (Identity and Access Management -IAM), elektronik veya dijital kimliklerin yö-netimini kolaylaştıran iş süreçleri, politikalar ve bunları destekleyen teknolojilerden oluşan bir yapıdır. BT yöne-ticileri IAM çerçevesi ile kuruluşlarındaki kritik bilgilere kullanıcı erişimini kontrol edebilmektedir.

Yalnızca yetkili kullanıcıların bulut ortamına, uy-gulamalara ve verilere erişmesini sağlamak için güçlü kimlik yönetimi ve kimlik doğrulama süreçlerinden ya-rarlanılması büyük fayda sağlayacaktır. Bulut bilişimin güvenliğinin sağlanabilmesi için ayrıcalıkların rol tabanlı olduğundan ve ayrıcalıklı erişimin oturum izleme yoluyla denetlenip kaydedildiğinden emin olunması gereklidir.

4.4.4 BULUT ÖRNEKLERİ VE VARLIKLARI

Bulut örnekleri, hizmetler ve varlıklar keşfedilip gruplan-dırıldıktan sonra, bunların yönetilmesi için aksiyon alın-ması gereklidir. Bulut bilişim yönetim sistemlerinin en önemli bile-şenlerinden biri olan bulut varlıkları Bulut Varlık Yönetimi (Cloud Asset Management -CAM) adı verilen bir bile-şenle kontrol edilmektedir. Bulut varlık yönetimi, bulut ortamını oluşturan tüm varlıkların ve altyapının görünür-lüğünü ve kontrolünü sağlamaktadır. Daha iyi optimize edilmiş, daha güvenli bir bulut için bu bileşen çok önemli bir ilk adımdır.

4.4.5 ŞİFRE KONTROLÜ (AYRICALIKLI VE AYRICALIKSIZ ŞİFRELER)

Paylaşılan parolaların kullanımına asla izin verilmemeli-dir. Hassas alanlar için parolalar, diğer kimlik doğrulama sistemleriyle birleştirilerek daha güçlü bir savunma sağ-lanabilir. Parola yönetimi için gerekli şartlar onaylandık-tan sonra uygulamaların kullanılması önerilmektedir.

4.4.6 GÜVENLİK AÇIĞI YÖNETİMİ

Güvenlik açığı yönetimi, bulut bilişim güvenliğinde önemli bir rol oynamaktadır. Şirket içi ana bilgisayarların güvenlik açığı yönetimi, bulut ortamlarına uygulanamaz. Bu sebeple hızla değişen bulut ortamlarının güvenliği için, güvenlik açığı yönetiminin yeni bir yaklaşıma ihti-yacı vardır.

4.4.7 ŞİFRELEME (ENCRYPTION)

Bulut şifreleme, verilerin buluta aktarılmadan ve bulutta depolanmadan önce orijinal düz metin biçiminden şifreli metin biçimine dönüştürülme işlemidir.

4.4.8 OLAĞANÜSTÜ DURUM KURTARMA

Bulut hizmeti sağlayıcıları için veri yedekleme, saklama ve kurtarma ilkeleri ile süreçlerinden haberdar olunmalı-dır. Yedekleme sistemlerinin şirket içi standartları karşıla-ması gerekir. Bu sayede herhangi bir durumda yaşanan veri kaybı sonrası işletmenin tekrar faaliyete geçmesi kolaylaşmaktadır. Yedeklemenin periyodik olarak tekrar-lanması ve iş modeline göre bu periyotların belirlenmesi de bir diğer önemli konudur.

4.4.9 İZLEME, UYARI VE RAPORLAMA

Tüm ortamlarda ve sistemlerde sürekli güvenlik ve kullanıcı etkinliği izlenmelidir. Bulut sağlayıcıları gelen verileri kurum içi ve dışından gelen verilerle entegre etmeye ve merkezileştirmeye çalışmalıdır. Bu şekilde bulut bilişim ortamında neler olup bittiğine dair bütünsel bir resme sahip olunabilir.

4.5 BULUT SERVİSLERİ GÖREV VE SORUMLULUKLAR

4.5.1 SİSTEM YÖNETİMİ EKİBİ

- ✓ Bir bulut stratejisi geliştirme ve uygulama
- ✓ Harici bulut çözümlerini ve hizmetlerini araştırma ve seçme
- ✓ Bulut projelerinin yönetilmesi
- ✓ Bulut altyapısını ve servislerinin işlevselliğini sağlamak
- ✓ Güvenlik ve uyumluluğun sağlanması
- ✓ Operasyonel ve performans problemlerinde teknik destek sağlamak
- ✓ Kaynakların ve bütcenin yönetilmesi
- ✓ Sektör trendleri ve gelişmeleri ile güncel kalmak

4.5.2 SİBER GÜVENLİK EKİBİ

- ✓ Bulut sistemlerinin güvenlik gereksinimlerini analiz etme ve tanımlama
- ✓ Bulut sistemlerinden gelen ilgili güvenlik uyarılarını analiz etme ve yanıtlama
- ✓ Bulut güvenliği standartlarının tanımlanması
- ✓ Kuruluşun faaliyetlerindeki değişiklikleri ve en son güvenlik tehditlerini yansıtmak için güvenlik politikalarının düzenli olarak gözden geçirilmesi ve güncellenmesi.
- ✓ Güvenlik operasyonları ve destek faaliyetleri ile ilgili metriklerin izlenmesi
- ✓ Uyumluluk ve yasal şartların uygunluğun takip edilerek iyileştirilmesi
- ✓ Bulut güvenliğine yönelik zafiyet takiplerini yapmak ve gereken implementasyonları gerçekleştirmek

4.6 BULUT SERVİSLERİ GÜVENLİK TEHDİTLERİ

Artan Saldırı Yüzeyi
Bulut bilişim sistemlerinin güvenliğinde yaşanan en büyük zorluk yapılandırma ve konfigürasyon eksikliklerinden kaynaklı hataların doğurduğu açıklardır. Bulut bilişim sisteminin dışarıda kullanımına izin verdiği yazılımla, servis ve uygulamalar güvenlik açıklarının temelini oluşturmaktadır.

Görünürlük ve Takip Eksikliği
IaaS modelinde, bulut sağlayıcılar altyapı katmanı üzerinde tam kontrole sahiptir. Ancak görünürlük ve kontrol eksikliği, PaaS ve SaaS bulut modellerinde daha da ge-niş bir alana hitap etmektedir. Bulut müşterileri genellikle bulut varlıklarını etkili bir şekilde tanımlayamaz ve ölçe-mez veya bulut ortamlarını görselleştiremez.

Sürekli Değişen İş Yükleri
Bulut varlıkları, dinamik olarak çeşitli ölçekte ve hızda sağlanabilmektedir. Geleneksel güvenlik araçları, sürekli değişen ve kısa ömürlü iş yükleriyle esnek ve dinamik bir ortamda koruma ilkelerini uygulamak için yetersiz kalabilir.

Granüler Ayrıcalık ve Anahtar Yönetimi
Bulut kullanıcı rolleri genellikle çok gevşek bir şekilde yapılandırılmaktadır. Bu roller ile kullanıcılara amaçlanan veya gerekenin ötesinde kapsamlı ayrıcalıklar sağlana-bilmektedir. Bulut sistemi ile ilgili yeterli eğitimi olmayan kullanıcılara veritabanı silme veya yazma izinleri verilmesi bu durumun en büyük örneklerinden biridir. Bu ve benzeri uygulama düzeyinde yanlış yapılandırılmış anahtarlar ve ayrıcalıklar, genel anlamda oturumları güvenlik risklerine maruz bırakır.

Karmaşık Ortamlar
Küresel ölçekte işletmeler geliştikçe bulut ortamları daha karmaşık hâle gelmeye devam etmektedir. Çoğu işlet-me günümüzde en az bir genel bulut ve bir özel bulut hizmeti kullanmaktadır. Yapılan araştırmalar çoğu işletmenin üç ila dört bulut sistemini bir arada kullanmaya başladığını göstermektedir. Bu karmaşık bulut ortamının yönetiminin zor olduğu kanıtlanmıştır. Karmaşıklık arttıkça bu durum daha da zorlaşacaktır.

Bulut Uyumluluğu ve Yönetim
Bulut bilişim yönetişimi ve uyumluluğu, önemli bir nedenden dolayı kritik öneme sahiptir. Bulut bilişim, iş ve kişisel yaşamın pek çok yönünü etkilemektedir. Bulut bilişim, müşteriler için büyük verimlilik kazanımları ve maliyet avantajları sunmaktadır. Ancak bir bulut bilişim stratejisini tanıtmak basit bir işlem değildir. Bulut yönetiminin devreye girdiği yer burasıdır. Basitlik, entegrasyon ve maliyet kontrolü için birden çok bulut bilişim hizmeti-ni yönetme süreci bulut yönetimini oluşturan en önemli alanlardır. Bulut yönetiminin mevcutta kullanılan bütün sistemler ve yazılımlarla uyumlu olması ve güvenliği ak-satmadan bağlantı kurması gereklidir.

Hizmet Hırsızlığı
Bu saldırıda, bir sistem değişkeni sıfırlanarak daha az ödeme ile sanal makinenin daha uzun süre kullanılmasına izin verilir.

Hizmet Aksatma
Bu saldırı türünde saldırgan bulut platformunu hedef alarak bulut müşterilerine sağlanan hizmetlerin kullanımını engellemektedir.

Veri Temizleme
Veri temizleme saldırısında kullanıcı, kendisine ait veriyi bulut deposundan silerken dosya sistemleri veriyi tamamen yok etmemektedir. Böylece silinen veri, saldırganlar tarafından ele geçirilerek kullanılabilmektedir.

Müşteri Veri Manipülasyonu
Bulut platformuna dışardan erişim sağlayan herhangi bir kullanıcı, uygulama bileşeninden sunucu uygulamasına gönderilen verileri değiştirerek web uygulamalarına sal-dırabilmektedir. Bulut bilişim sistemlerine SQL enjeksiyonu, komut enjeksiyonu ve siteler arası her türlü yazılı (betik) çalıştırma saldırılarıyla veri manipülasyonu kolay-lıkla gerçekleştirilebilmektedir.

Veri Sızıntısı
Verinin transferi, depolanması, denetimi ve işlenmesi sırasında veri sahibinin yetki verdiği kullanıcılar dışında farklı kişiler tarafından verilerin ele geçirilmesi işlemine veri sızıntısı denilmektedir.

Buluta Kötücül Yazılım Enjekte Etme
Buluta enjekte edilen kötücül yazılım aracılığı ile bulut verileri ele geçirilip değiştirilebilir ve verilere erişim engellenebilir hatta veri üzerinde istenilen tüm haklara sahip olunabilir. Bu saldırıda düşman kendi kötücül hizmet uygulama modelini (SaaS ya da PaaS) ya da sanal makine örneğini (IaaS) oluşturur ve buluta ekler. Daha sonra bu sistemlerin düşman tarafından saldırıya uğramış bazı özel hizmetler için geçerli örnekler arasında olduğunu ve bazı yeni hizmet uygulama örnekleri olduğunu bulut sistemine inandırır. Eğer bu davranış başarılı olursa bulut otomatik olarak geçerli kullanıcının isteklerini kötücül hizmet uygulamasına yönlendirir ve kötücül kod çalıştırılır.

Hedeflenmiş Paylaşılan Hafıza
Bu saldırı türünde saldırganlar hem fiziksel hem de sanal makinelerin paylaşılmış hafızalarından yararlanarak, çalışan işlem sayısı, belirli bir süre içerisinde oturum açan

kullanıcı sayısı ve hafızada bulunan geçici çerezler gibi bulutun iç yapısını ortaya çıkaran bilgilere yetkisiz erişim sağlayabilmektedir.

Kimlik Avı
Kimlik avı saldırısı, kişisel bilgilere yetkisiz olarak erişilme-sine, kullanıcı bilgisayarına kötücül bir kod indirilmesine, bulut bilişim yapısının normalden farklı bir şekilde dav-ranmaya zorlanmasına ve son kullanıcı için sunucunun erişilemez olmasına yol açmaktadır. Ayrıca bu saldırı sadece kullanıcıları değil aynı zamanda elektronik bankalar ve elektronik ödeme sistemleri gibi destekleyici finansal kurumları da savunmasız hâle getirebilmektedir.

Botnet'ler
Açık bir bulut ortamı göz önüne alındığında, yönlendir-me ve şaşırtma açısından uzaktan yönetilen zombi bilgisayarların en tehlikeli gruplarından biri olan botnet'ler aracılığıyla bulut kaynaklarına yetkisiz erişim yapılabilmektedir. Ayrıca bulut sisteminin anormal bir şekilde çalışması sağlanabilmekte, hassas bilgiler ve kullanıcı verileri çalınmaktadır. Teknoloji geliştikçe botnet'lerin ağlardaki kamuflajını anlamak zorlaşmaktadır. Ayrıca yeni nesillerin de algılanması için kendilerini ağ içerisinde nasıl gizlediğini öğrenmek gerekmektedir.

4.7 BULUT SERVİSLERİ RİSKLERİ

4.7.1 KURUMSAL VE STRATEJİK RİSKLER

- Yönetim ve kontrol kaybı
- Bulut hizmeti sonlandırması veya arızası
- Servis sağlayıcı bağımlılığı
- Üçüncü parti tedarikçi hatası
- Bulut sağlayıcı kuruluşun satın alınması
- Uyum sorunları
- Sağlayıcının diğer müşterileri nedeniyle itibar kaybı

4.7.2 TEKNİK RİSKLER VE GÜVENLİK RİSKLERİ

- Dış Kaynaklı Saldırılar
- Verilerin güvensiz veya etkisiz silinmesi
- Nakil halindeki veiyi yakalama
- Bulut sağlayıcı tarafında kötü amaçlı giriş
- Kaynak tükenmesi
- Şifreleme
- Kaynak izolasyonu eksikliği
- Hizmet kesintisi veya bozulması
- Kötü amaçlı araştırma ve taramalara girilmesi
- Müşteri gereksinimleri ve bulut ortamı arasındaki anlaşmazlık
- Şifreleme anahtarlarının kaybı
- Hizmet motorunun hacklenmesi

4.7.3 HUKUKSAL RİSKLER

- Yargi değişiminden kaynaklı riskler
- Mahkeme celbi ve e-keşif
- Veri sansürü
- Lisans riskleri
- Veri koruma riskleri

4.8 BULUT SERVİSLERİ ÇIKIŞ STRATEJİSİ

Genellikle tersine geçiş olarak adlandırılan buluttan çıkış stratejisi, bir işletmenin bir bulut sağlayıcısından diğerine daha büyük bir kesinti olmadan etkili bir şekilde geçiş yapabilmesini sağlamak için bir plan geliştirme sürecidir. Bu, buluta geçmek isteyen tüm işletmeler için odak noktası olmalıdır.
Çoğu bulut hizmet sağlayıcısı olağanüstü çalışma süresi ve güvenilirliğe sahip hizmetler sunsa da, pazar liderleri bile son zamanlarda önemli kesintilerle karşı karşıya kalmaktadır. Aynı şekilde, işletmelerin karşılaştığı ve iş performanslarına zarar verebilecek bulut endişeleri, bütçe/maliyet kontrolleri ve yönetişim vb. gibi önceki kararları yeniden düşünmek için birçok başka neden vardır, Bu nedenle çıkış stratejisine sahip olmak öem arz etmektedir.

Buluttan çıkışı planlamak için etkili bir çıkış stratejisi, yeri doldurulamaz verileri güvende tutmak ve başarılı bir geçiş sağlamak için önemli bir parçadır. İşletmeler Buluttan Çıkışa hazırlanırken aşağıdaki anketle testleri yaparak gerekli çıkış yöntemine ön hazırlık yapılmış olunur:

- Mevcut CSP (Bulut Hizmet Sağlayıcısı) ile iş yüklerini çalıştırmanın zorlukları nelerdir?
- Mevcut maliyetlendirme nasıl görünüyor? Her zaman yukarı yönlü bir fiyatlandırma modeli mi?
- Satıcı kilitlenmesi işletmenin ilerlemesini engelliyor mu?
- Diğerlerine göre rekabet avantajı sunuyor mu? Hedeflediğim duruma ulaşmak için mevcut CSP ile bir sonraki önemli şey nedir?
- Dijital çözümler açısından ne kadar yenilikçi?
- Mevcut CSP ile düzenleyicilerin modeli nedir? Sektör kılavuzunu uyarlıyor ve güncelliyor mu? Ve hangi sıklıkta?
- Mevcut zorlukları ele alma açısından genel yetenekleri nelerdir? Örneğin, Güvenlik, Uyumluluk, Operasyonel Esneklik vb,
- Kurumsal yönetişim buluttan çıkışın gerçekleştirilmesine yardımcı oluyor mu?
- Kullandığınız belirli hizmet/hizmetlerle ilgili kesintiler ne sıklıkta yaşanıyor?
- Müşteri desteğine yönelik deneyiminiz nasıl?

Yukarıdaki aşamalar ışığında aşğıdaki adımlar izlenerek uygun çıkış stratejisi belirlenir ve uygulamaya alınır.