Denetci.org

REFERANS İLKELERİ

İş Sürekliliği İlkeleri

Rİ-DAY-2

Sürüm 1.0 · 11.08.2026

www.denetci.org

İş Sürekliliği İlkeleri

İş sürekliliği, kesinti veya kayıp koşullarında kuruluşun önemli hizmet ve sonuçlarını kabul edilebilir düzeyde sürdürebilmesini ve gerektiğinde güvenilir biçimde yeniden kurabilmesini ele alır. Amaç her sistemin kesintisiz çalışacağını iddia etmek değil; hangi kayıpların kabul edilebilir olduğunu, kritik hizmetlerin hangi bağımlılıklara dayandığını ve bu bağımlılıklar kaybedildiğinde nasıl davranılacağını anlamaktır.

İlke 1: Süreklilik bütün sistemleri aynı ölçüde korumayı hedeflememelidir.

Kuruluşun bütün faaliyetleri aynı kayıp sonucuna sahip değildir. Süreklilik öncelikleri teknik görünürlükten veya sistem büyüklüğünden çok kuruluş açısından korunması gereken gerçek sonuçlara dayanmalıdır.

İlke 2: Kritik hizmet, onu sunan tek bir uygulamayla eşit kabul edilmemelidir.

Bir hizmet veri, kimlik, ağ, insanlar, fiziksel ortam ve dış taraflar dahil birçok unsura bağlı olabilir. Görünen uygulamanın çalışması bütün hizmetin sürdürülebildiğini göstermeyebilir.

İlke 3: Dolaylı bağımlılıkların kritikliği kendi görünür işlevlerinden anlaşılmayabilir.

Kimlik, ad çözümleme, sertifika, iletişim veya yönetim gibi ortak hizmetler doğrudan iş çıktısı üretmese de çok sayıda kritik faaliyetin ön koşulu olabilir. Kritiklik, bir unsurun kaybının başka sonuçlara ne ölçüde yayıldığıyla anlaşılmalıdır.

İlke 4: Kabul edilebilir kesinti ve veri kaybı işin gerçek toleransını yansıtmalıdır.

Kurtarma beklentileri yalnızca teknik ekibin hedefleri olmamalıdır. Bir hizmetin ne kadar süre veya hangi veri kaybıyla devam edebileceği, o hizmetin gerçek iş sonuçlarıyla ilişkilendirilmelidir.

İlke 5: Süreklilik hedefleri gerçek kapasitenin üzerinde kâğıt üzerinde güvence üretmemelidir.

Bir hedefin tanımlanması o hedefe ulaşılabildiğini göstermez. İnsan, teknoloji, veri hacmi ve bağımlılıklarla birlikte gerçek kurtarma kapasitesi hedeflerle uyumlu olmalıdır.

İlke 6: Yüksek erişilebilirlik ile iş sürekliliği aynı şey değildir.

Yedek bileşenler bazı teknik arızaları azaltabilir; ancak veri bozulması, kimlik kaybı, kötü niyetli değişiklik veya ortak bağımlılık kaybı bütün aktif ortamları birlikte etkileyebilir. Süreklilik yalnızca hizmetin başka bir çalışan kopyasının bulunmasına dayanmamalıdır.

İlke 7: Yedeklilik yalnızca bağımsız başarısızlık alanları oluşturduğu ölçüde değer taşır.

Farklı cihazlar veya bölgeler aynı yönetim, kimlik, ağ, sağlayıcı ya da başka ortak bağımlılıklara sahip olabilir. Görünürde çoğaltılmış bileşenler aynı olayda birlikte kaybedilebiliyorsa sağladıkları süreklilik sınırlıdır.

İlke 8: Ortak bağımlılıklar ölçüsüz geniş kesinti alanları oluşturmamalıdır.

Tek bir merkezi hizmetin kaybı bütün kritik faaliyetleri durduruyorsa bu durum tasarımın gerçek süreklilik sınırıdır. Merkezileştirme kolaylığı bu ortak kaybı görünmez hale getirmemelidir.

İlke 9: Süreklilik yalnızca fiziksel veya teknik arıza senaryolarına dayanmamalıdır.

Siber saldırı, veri bozulması, insan kaybı, tedarikçi sorunu, yanlış değişiklik ve başka olaylar da hizmetin güvenilir biçimde sunulmasını engelleyebilir. Süreklilik yaklaşımı arızanın tek bir türünü varsaymamalıdır.

İlke 10: Çalışan ancak güvenilemeyen bir hizmet devam ediyor sayılmamalıdır.

Sistem teknik olarak erişilebilir olsa bile verisi bozuk veya güvenlik durumu bilinmiyorsa hizmet sonucu güvenilir olmayabilir. Süreklilik kullanılabilirliğin yanında bütünlük ve gerekli güvenlik özelliklerini de korumalıdır.

İlke 11: Yedekleme iş sürekliliğinin tamamı olarak görülmemelidir.

Veri geri getirilebilse bile uygulama, yapılandırma, kimlik, sertifika, dış hizmet veya gerekli insan bilgisi mevcut değilse hizmet devam edemeyebilir. Süreklilik gerçek hizmet zincirini kapsamalıdır.

İlke 12: Kurtarma sırası hizmetlerin gerçek bağımlılıklarına dayanmalıdır.

En önemli görünen uygulamayı ilk açmak, ihtiyaç duyduğu temel hizmetler hazır değilse anlamlı olmayabilir. Güvenlik ve kimlik altyapıları da dahil olmak üzere hangi unsurun diğerinin ön koşulu olduğu kurtarma kararında karşılık bulmalıdır.

İlke 13: Olağanüstü çalışma biçimi temel güvenlik gereksinimlerini kendiliğinden ortadan kaldırmamalıdır.

Kesinti sırasında normal süreçlerden farklı çalışma yolları gerekli olabilir. Ancak süreklilik amacı, kimlik, yetki, veri bütünlüğü ve hesap verebilirlik gibi temel güven sınırlarının gereksiz biçimde kaldırılmasına dönüşmemelidir.

İlke 14: Acil erişim gerçekten kullanılabilir olmalı ancak normal erişimin kolay alternatifi haline gelmemelidir.

Kriz anında ana kimlik veya yönetim altyapısı kullanılamayabilir. Alternatif erişim bu durumda bağımsızlık sağlayabilmeli, fakat günlük kullanımda olağan güvenlik sınırlarını aşan kalıcı bir yol oluşturmamalıdır.

İlke 15: Alternatif çalışma yöntemi teknik faaliyet değil gerçek iş sonucunu sürdürebilmelidir.

Manuel veya geçici bir süreç sistemin bazı işlevlerini taklit edebilir; fakat kuruluşun ihtiyaç duyduğu sonucu üretemiyorsa gerçek süreklilik sağlamaz. Alternatif yöntemler korunan iş sonucuyla ilişkilendirilmelidir.

İlke 16: Manuel süreklilik insan kapasitesini gerçekçi biçimde dikkate almalıdır.

Otomasyonun yerini geçici olarak insanların alabilmesi bazı durumlarda mümkün olabilir; ancak büyük hacim, uzun süre veya karmaşık kararlar manuel yaklaşımı sürdürülemez hale getirebilir. Kâğıt üzerinde mümkün görünen süreç gerçek olayda insan kapasitesini aşmamalıdır.

İlke 17: İnsanlar ve kurumsal bilgi temel süreklilik bağımlılıklarıdır.

Kritik karar, erişim veya teknik bilgi tek bir kişide toplanmışsa sistemlerin tamamı çalışsa bile hizmet sürdürülemeyebilir. Süreklilik yalnızca teknoloji bileşenlerinin mevcudiyetiyle değerlendirilmemelidir.

İlke 18: İletişim altyapısı da süreklilik kapsamındaki bir bağımlılıktır.

Olay sırasında normal iletişim kanalları kullanılamayabilir. Alternatif iletişim, koordinasyon sağlayabilmeli ancak güvenilirlik ve gizlilik ihtiyaçlarını bütünüyle terk etmemelidir.

İlke 19: Alternatif çalışma alanı yalnızca farklı fiziksel konumda olduğu için bağımsız sayılmamalıdır.

Farklı tesisler aynı enerji, ulaşım, telekomünikasyon, insan kaynağı veya bölgesel olaydan etkilenebilir. Fiziksel çeşitlilik gerçek ortak hata nedenleriyle birlikte değerlendirilmelidir.

İlke 20: Dış hizmet kullanımı süreklilik sorumluluğunu ortadan kaldırmamalıdır.

Sağlayıcıların dayanıklılık iddiaları kuruluşun kendi kritik hizmetinin gerçekten sürdürülebileceğini otomatik olarak göstermez. Kuruluş, dış bağımlılık kaybolduğunda kendi sonuçlarının ne olacağını anlayabilmelidir.

İlke 21: Birden fazla sağlayıcı yalnızca gerçek geçiş yeteneği varsa bağımsızlık sağlar.

İkinci bir sağlayıcıya sözleşmesel erişim bulunması iş yükünün, verinin veya işletimin gerçekten oraya taşınabileceğini göstermeyebilir. Çeşitlilik kâğıt üzerindeki alternatif sayısından çok fiilî geçiş kapasitesiyle anlam kazanır.

İlke 22: Küçük görünen dolaylı unsurlar kurtarmayı durdurabilecek bağımlılıklar oluşturabilir.

Lisanslar, sertifikalar, anahtarlar, yapılandırmalar ve benzeri unsurlar sistemin yeniden çalışabilmesinin ön koşulu olabilir. Kurtarma planı yalnızca ana uygulama ve veriye odaklanarak bu gereksinimleri görünmez bırakmamalıdır.

İlke 23: Normale dönüş sürekliliğin ayrı bir güvenlik aşaması olarak görülmelidir.

Geçici süreçlerde oluşan işlemler, veriler ve yetkiler normal ortama taşınırken kayıp, tekrar veya güvenlik zayıflığı oluşabilir. Hizmetin kriz modundan çıkması kendi başına yeni bir kesinti veya güven kaybı üretmemelidir.

İlke 24: Süreklilik kabiliyeti dokümanların varlığıyla değil gerçek davranışla doğrulanabilmelidir.

Planlar ve hedefler önemli olabilir; ancak kritik hizmetlerin gerekli bağımlılıklarla birlikte gerçekçi kesinti koşullarında sürdürülebildiği veya kabul edilebilir sürede güvenilir duruma getirilebildiği sınanabilmelidir. Gerçek olaylar ve tatbikatlar önceki süreklilik varsayımlarını yeniden değerlendirebilmelidir.