İŞ SÜREKLİLİĞİ YÖNETİMİ

Güvenlik sürecinin en önemli kavramlarından biri iş sürekliliği yönetimidir. Büyük çaplı sistem çökmeleri, arızalar ya da doğal felaketler gibi durumlarda, kritik işlerin devamını sağlayabilmek üzere gerekli önlemler alınmalıdır. Bu konuda önlem ve çözümlere karar vermek üzere, öncelikle iş devamlılık ve etki analizi yapılmalıdır (donanım arızası, sel, yangın gibi durumlarda oluşacak zararların boyutları saptanır vb.). Belirlenen risklerin gerçekleşmesi durumunda, işin belli seviyede devamı için yapılacaklar, sorumluluklar, iletişim bilgileri, operasyon detayları, acil durumu ortadan kaldırmak üzere yapılması gerekenler belirlenerek belgelenmelidir. Yapılan acil durum planları düzenli aralıklarla test edilmeli ve doğrulanmalıdır; test sonuçlarına göre gerektiğinde yeniden düzenlenmelidir.

Fiziksel güvenlikle yakından ilgisi bulunan bu alan kesintilere karşı iş süreçleri ve teknik altyapı konusunda yapılacak hazırlık, eğitim ve testleri kapsar. Özellikle büyük ve karmaşık iş süreçlerine sahip kurumların bilgi teknolojileri bağımlılığı artmış, bu durum BT hizmetlerinin kesintisini daha kritik öneme kavuşturmuştur. İş sürekliliği ve felaket kurtarma kritik iş süreçlerinin analizini, süreçlerin bağımlı bulunduğu fonksiyonların ve teknolojik altyapının tespitini, maksimum kesinti dayanma süresinin tespiti, hedeflenen kurtarma süresinin tespiti, kesinti durumunda uğranılacak zararın boyutuna ve kurtarma zaman hedefine göre gerekli devamlılık ve kurtarma yatırımlarının seçilmesini, etkin bir planlama, eğitim, iletişim ve test döngüsünün uygulanmasını ve kesintiye karşı hazırlıklı kalınmasını, kesinti durumunda kritik süreçlerin kabul edilebilir süre ve seviyede devam ettirilebilmesi için gerekli prosedürlerin hazırlanmasını, kesinti sırasında biriken bilgi ve işlerin bilgi sistemleri ayağa kaldırıldıktan sonra sistem ile senkronizasyonunu, soğuk, ılık veya sıcak kurtarma merkezlerinin oluşturulmasını içerir. Bilgi teknolojileri veya başka bir fonksiyonun hizmetinin kesintiye uğraması kuruma para ve itibar kaybettirebilir. Belli bir süreden sonra kurum faaliyetlerine hiç devam edemeyecek hale gelebilir.

1. İŞ SÜREKLİLİĞİ YÖNETİMİNİN BİLGİ GÜVENLİĞİ BOYUTU

İş Sürekliliği Yönetim Sürecinin Bilgi Güvenliğini İçermesi

- Kurum bünyesinde iş sürekliliği için geliştirilmiş bir süreç olmalıdır.
- Bu süreç bilgi güvenliği ihtiyaçlarına yer vermelidir.
- Süreç iş sürekliliği ile ilgili olarak şu konulara değinmelidir; Kuruluşun yüz yüze olduğu riskler, kritik iş süreçleri ile ilgili varlıklar, bilgi güvenliği olayları yüzünden gerçekleşebilecek kesintilerin etkisi, ilave önleyici tedbirlerin belirlenmesi ve uygulanması, bilgi güvenliğini de içeren iş sürekliliği planlarının belgelenmesi.

İş Sürekliliği ve Risk Analizi

- İş süreçlerinde kesinti yaratan veya yaratabilecek olaylar, kesintilerin yaratacağı etki, gerçekleşme olasılıkları ve bilgi güvenliği açısından sonuçları ile birlikte belirlenmiş olması gerekmektedir.
- Bu tür kesintilerin etkisini belirlemek için risk analizi yapılmış olmalıdır.
- Risk analizi, bilgi güvenliği ile ilgili sonuçları içermekle birlikte sadece bilgi işlem değil tüm iş süreçlerini göz önünde bulundurarak ve tüm süreçlerin sahipleri ile birlikte gerçekleştirilmiş olması gerekmektedir.
- Risk analizinin sonuçları uyarınca iş sürekliliği ile ilgili geniş kapsamlı strateji belirlenmiş olması gerekmektedir.

Bilgi Güvenliğini İçeren İş Sürekliliği Planlarının Geliştirilmesi ve Uygulanması

- Kritik süreçlerin kesintiye uğramasının ardından kurum tarafından belirlenmiş zaman aralığı içinde iş sürecinin onarılması ve belli bir seviyedeki bilgiye ulaşılabilmesi için planlar geliştirilmiş olması gerekmektedir.

- Plan, sorumlulukların belirlenmesi ve anlaşılması, kabul edilebilir hasarın belirlenmesi, onarım prosedürünün belirlenmesi, prosedürün düzenli aralıklarla test edilmesi ve belgelenmesine değiniyor olması gerekmektedir.

İş Sürekliliği Planlama Çerçevesi

- Tüm planların tutarlı olması, bilgi güvenliği ihtiyaçlarının tutarlı olarak sağlanması, test ve bakımla ilgili önceliklerin belirlenmesi için iş sürekliliği planları tek bir çerçeve uyarınca hazırlanıyor ve güncelleniyor olmalıdır.
- İş sürekliliği planı bilgi sistemleri erişilebilirliği ile ilgili yaklaşımını, kurtarma planı ve planın harekete geçirilmesi için gereken şartları, planın bölümlerini yerine getirmekle sorumlu kişileri ve planın sahibini açıkça belirtiyor olmalıdır.
- Yeni ihtiyaçlar ortaya çıktığında prosedürler gerektiği gibi güncellenmelidir.
- Prosedürlere kuruluşun değişiklik yönetimi programı içerisinde yer verilerek iş sürekliliği yönetiminin her zaman uygun şekilde ele alınması sağlanmalıdır.

İş Sürekliliği Planlarının Test Edilmesi, Bakımı ve Yeniden Değerlendirilmesi

- İş sürekliliği planları güncellik ve etkinliklerinin sınanması açısından düzenli olarak test ediliyor olmalıdır.
- Testler aracılığı ile onarım ekibinin üyeleri ve diğer ilgili personelin planlardan ve iş sürekliliği ile ilgili sorumluluklarından haberdar olduğu ve plan devreye sokulduğu zaman üstlenecekleri rolün ne olduğunu bilip bilmedikleri sınanıyor olmalıdır.