Ziya Gökalp
Cyber Security Leader & Advisor

‘İşin Sürekliliği’ adına ‘Bilgi Güvenliği’

Mevcut denetim ve kontrol mekanizmaları ile işin ve işin gereği olan operasyonel faaliyetlerin olağanüstü olan veya olmayan durumlarda duraklaması veya faaliyet gösteremez hale gelmesi ile ortaya çıkabilecek finansal kayıplar her işletme için ürkütücü hale gelmiştir.

En yalın hali ile örneklemek gerekirse; Telekom operatörü olarak faaliyet gösteren bir firmanın sistemlerinin durması, bir bankanın internet / mobil bankacılık uygulamasının çalışmaması, otomasyon sistemleri kullanarak üretim yapan bir üreticinin üretim faaliyetlerinin duraksaması, E-Devlet portallerinin hizmet veremiyor olması finansal anlamda milyon dolarlık işlem kaybını ve beraberinde müşteri / kullanıcı güveninin sarsılması ile doğacak müşteri kaybının finansal zararlarını beraberinde getirir. Bu noktada uzun zamandır konuşulan olağanüstü durum eylem planları ve iş sürekliliği yönetimi, işletmelerin ve devletlerin yönetim stratejilerinin en önemli parçası olarak görülmektedir.

İş sürekliliği yönetimi; kritik sistemlerin yedeklenmesi ile birlikte üretimden finansa, hizmetlerden operasyonel faaliyetlere, insan kaynağından satınalmaya kadar tüm fonksiyonların duraklaması ile ortaya çıkabilecek menfi sonuçları, bu sonuçları oluşturabilecek risklerin analiz edilerek ortadan kaldırılmasını hedeflemektedir.

Bu açıdan bakıldığında işin devamını sağlamak, tüm risk faktörlerini ve tehdit unsurlarını tespit edebilmek ve bunlara önlem alabilecek politikaları ve prosedürleri geliştirmek ile mümkün kılınabilir. İş sürekliliği tıpkı Bilgi Güvenliğinde olduğu gibi bitmeyen, sürekli geliştirilmesi, gözden geçirilmesi ve denetlenmesi gereken bir süreçtir.

Farklı seneryolar, farklı çalışma durumları, farklı unsurların değerlendirilmesi ve gerçeğe uygun ayağa kaldırma, devam ettirme politikaları, bu politikaların test edilmesi ve denetlenmesi, işin sürekliliği anlamında yapılan yatırımları anlamlı kılacaktır. Analize başlamadan önce strateji ve planlama, hangi organizasyonun analiz ve planlama amacı ile iş birimlerine bölüneceğini belirler. Finans şirketleri finansal raporlama, çağrı merkezleri, internet tabanlı bankacılık sistemleri gibi operasyonel faaliyetlerini ayrı iş dalları olarak ele alarak değerlendirir ve denetler. Üretim yapan firmalarda ise her bir üretim tesisi veya üretim farklılıkları içeren üretim bandı ayrı iş dalları olarak görülüp değerlendirilmeli ve planlanmalıdır.

Yukarı verdiğim örnekler doğrultusunda dahili ve harici risk unsurlarını ve bu unsurlar ile doğabilecek sonuçları öngörmek, bunlara önlemler alabilmek, sürecin başarısı adına hiç şüphesiz işletmelerin yönetim düzeyinde değerlendirmesi ve her bölümün takım çalışması ile mümkün olabilir. İş sürekliliği; organizasyonların tavanından tabanına kadar her kademeyi ilgilendirir. Bu noktada çalışanları bilinçlendirme ve sürece dahil etme kaçınılmazdır.

İngiliz Standardı Enstitüsü (BSI) tarafından geliştirilen ve daha sonra bir ISO/IEC standardına da dönüşen BS 25999 / ISO 22301– İş Sürekliliği Yönetim Sistemi; uygulama kurallarını ve spesifikasyonları iki ana aşamada düzenlemektedir.

İlki; İş Sürekliliği Yönetim Sistemi'nin geliştirilmesi,

Diğeri; İş Sürekliliği Yönetim Sistemi'nin uygulanması ve işletilmesidir.

BS 25999 / ISO 22301, her bir ana aşama dahilinde standardın uygulanması için başlıca faaliyetler belirtmektedir.

Buna göre "İş Sürekliliği Yönetim Sistemi" nin uygulanması ve işletilmesi aşamasında;

Kurum faaliyetlerinde yaşanan aksamaların etkilerinin belirlenmesi, risk değerlendirmesi ile kritik faaliyetlere karşı tehdit unsurlarının analiz edilmesi, risk azaltma seçeneklerinin belirlenmesi, risklerin hafifletilmesi, faaliyetlerin durması aşamasında geri alınması/ayağa kaldırılması, iş kesintilerine karşılık verebilme ve faaliyetlerin idaresi amaçlı süreçlerin belirlenmesi, planlama yapılarak süreçlerin dokümante edilmesi, tatbikat prosedürü ile kriz durumlarına tepki verebilmenin yaşatılması ve gözlemlenmesi, tüm planın periyodik olarak gözden geçirilmesi, sürecin verimliliğinin ve hedefine ulaştığının kontrol edilmesi sağlanmalıdır.

İş Sürekliliği Yönetimi; Kurum ve kuruluşların yönetim fonksiyonu olarak doğru kişiler tarafından idare ettirilmelidir. Bu bağlamda organizasyonların İş Sürekliliği komitelerine sahip olmaları kaçınılmazdır. Yönetim gerekliliklerini yerine getirebilmek, politika ve prosedürleri oluşturabilmek, riskleri tespit edebilmek ve risk seviyelerini öngörebilmek, süreci idame ve idare ettirmek, tüm faktörleri anlamak ve tasarlamak bir yönetim komitesi ve bu komiteye bağlı takımlar ile mümkün kılınabilir. CIO (Chief Information Officer), COO (Chief Operation Officer), CFO (Chief Finance Officer), CSO (Chief Security Office) gibi pozisyonlarda yer alan kişilerden oluşacak bir komite ve bu komiteye bağlı takımlar sürecin geliştirilmesi ve hayata geçirilmesi ile sürekli kontrol edilmesi ve güncellenmesi anlamında birlikte çalışmanın ötesinde, üst yönetimin konuya hassasiyetini de gösterecektir.

Kurum ve kuruluşlar için 'Bilgi Güvenliği' ne kadar önemli ve stratejik ise aynı şekilde 'İş Sürekliliği Yönetimi' de tüm organizasyonların varlıklarını devam ettirebilmesi adına kaçınılmazdır. Bu bağlamda işin sürekliliği adına 'Bilgi Güvenliği' nin kaçınılmaz olduğunu da ifade etmek mümkündür.

Ziya GÖKALP

Cyber Security Leader & Advisor

MSc.IT, SSCP®, ECSA , CEH, OCOE,
MPM®, ITIL, Certified ISO/IEC 27001 LA,
CIW Security Analyst,
CompTIA Project+,
Senior Certified Leadership Practitioner,
Certified Information Security Executive™