DuneMount

DuneMount
Kurumsal Dayanıklılık Hizmetleri

2023

HİZMETLERİMİZ

Bölüm 1
Kurumsal Dayanıklılık

Kurumsal Dayanıklılık (1/2)

Sürekli değişen bir dünyada, değişimlere hızlıca uyum sağlayabilmek ve bu değişiklikler karşısında firmamızın olabildiğince dayanıklı kalabilmesini sağlamak kritik bir öneme sahiptir.

Kurumsal Dayanıklılık Hizmetlerimiz, kuruluşların öngörülemeyen olaylara karşı hazırlıklı olmalarını ve dayanıklılıklarını artırmayı amaçlamaktadır.

Kurumsal Dayanıklılık hizmetlerimiz dört ana başlık altında toplanmıştır. Bunlar sırasıyla; kriz yönetimi, fiziksel güvenlik, iş ve bilgi teknolojileri sürekliliği ve üçüncü taraf yönetimidir.

Bütün hizmetlerimiz ve bu hizmetlerle ilişki olan çözümlerimiz uluslararası en iyi uygulama örneklerine dayanmakta ve müşterilerimizin ihtiyaçları doğrultusunda onlara en faydalı hizmeti vermeyi hedeflemektedir.

i) Kriz Yönetimi

Kuruluşların birçok alanda yaptıkları çalışmalarla her ne kadar krizi önlemeye çalışsalar da bu her zaman mümkün olamamaktadır. Zira öngörülemeyen riskler, öngörülemeyen olayları, öngörülemeyen olaylar ise öngörülemeyen krizleri meydana getirebilir. Ancak kriz anında doğru adımları atarak ve hızlı ve etkili bir müdahale yöntemi belirleyerek krizin etkilerini azaltmak mümkündür.

Kriz Yönetimi hizmetlerimiz, krizlerin etkisini etkin bir şekilde yönetme ve azaltma konusunda kuruluşların iç süreçlerini analiz etmek ve farkındalığı arttırmak için uçtan uca bir çözüm sunmak için geliştirilmiştir.

Kritik bileşenler ve hizmetler:

- Krize hazırlık değerlendirmesi
- Kriz simülasyonları, masa başı simülasyonu ve tatbikat çalışmaları
- Kriz senaryo tasarımı
- Kriz yönetimi çerçevesi ve yönetişim yapısı tasarımı
- Kriz yönetimi planı ve şablonu geliştirme
- Kriz sonrası değerlendirme

ii) Fiziksel Güvenlik

Kurumsal Dayanıklılık anlayışı sadece dijital tehditlere karşı değil, aynı zamanda fiziksel tehditlere karşı da önlemler almayı gerektirir. Bu doğrultuda süreç tasarımı, güvenlik değerlendirmeleri ve fiziksel güvenlik çözümleri özelinde müşterilerimize geniş bir hizmet yelpazesi sunmaktayız.

Kritik bileşenler ve hizmetler:

- Fiziksel güvenlik değerlendirmeleri
- Fiziksel güvenlik çerçevesi, politika, standart ve prosedür tasarımı
- Fiziksel saha güvenlik çözümleri

Kurumsal Dayanıklılık (2/2)

iii) İş ve Bilgi Teknolojileri Sürekliliği

İş ve Bilgi Teknolojileri Sürekliliği hizmeti, beklenmedik aksaklıklar veya felaketler karşısında bile işinizin ve bilgi teknolojileri sistemlerinizin kesintisiz çalışmasını sağlamak için tasarlanmış kapsamlı bir çözümdür.

Dünyadaki ekonomik, coğrafik ve kültürel engellere rağmen, bugün sektörlerinde öncü kuruluşlar tarafından teknoloji ve insan yedekli sistemler kurgulanıyor. Bu kurguların ön planında ise genellikle "teknolojiyi" görüyoruz. Ancak her ne kadar "teknolojiyi" donanım ve yazılımlar besliyor olsa da o teknolojiyi kullanacak "insanı" da hem gerçek hem de mecaz anlamda "besleyecek"; gıda, hijyen, elektrik ve aile bireylerinin güvenliği gibi unsurlar olduğunu da unutmamamız gerekiyor.

Hedefimiz; stratejik planlama, teknoloji dayanıklılığı ve proaktif önlemleri bir araya getirerek, geleneksel süreklilik ve afet anlayışından tamamen bağımsız bir yaklaşım sunmak ve kuruluşunuzun en zor olaylarda bile kritik işlevleri sürdürmesini ve kesinti süresini en aza indirmesini sağlamaktır.

Kritik bileşenler ve hizmetler:

- İş ve bilgi teknoloji sürekliliği stratejisi (ISO22301 uyumlu), çerçeve, süreç ve belge geliştirme
- İş ve bilgi teknoloji sürekliliği testleri, simülasyonları, denetimleri ve fark analizleri
- Süreklilik risk değerlendirmeleri
- Süreklilik alanında çözüm desteği
- Afet Master Planı analizi ve geliştirilmesi

iv) Üçüncü Taraf Yönetimi

Kuruluşların Kurumsal Dayanıklılığı sağlayabilmek için yalnızca kendi iç süreçlerinde değil aynı zamanda iş ortakları ve tedarikçileri ile ilgili iş süreçlerinde de dayanıklılığı sağlaması gerekmektedir. Aksi durumda üçüncü taraf kaynaklı olaylar kolaylıkla kuruluşlar için yıkıcı etkiler oluşturabilir.

Üçüncü Taraf Yönetiminin amacı çalıştığınız üçüncü tarafların kuruluşunuzun operasyonel, güvenlik ve uyumluluk standartları ile uyumlu olup olmadıklarını kontrol etmektir.

Kritik bileşenler ve hizmetler:

- Üçüncü Taraf Risk Değerlendirmesi
- Güvenlik ve Uyum Kontrolleri
- Acil Durum Planlaması
- İletişim Kanalları
- Üçüncü taraf yönetimi; çerçeve, süreç ve belge geliştirme

İLETİŞİM

İletişim

Serdar Karaman || CDPSE, ISO27001/ISO22301 LA, D1&D2 LA

DuneMount Kurucu

Serdar Karaman 2011 yılında Bahçeşehir Üniversitesi Bilgisayar Mühendisliği Bölümünden mezun oldu.

Mezuniyeti sonrasında ise sırasıyla TAC A.Ş., Akbank T.A.Ş., Avea Telekomünikasyon A.Ş., Türk Telekomünikasyon A.Ş. ve Deloitte firmalarında iş sürekliliği, bilgi teknolojileri sürekliliği, kriz yönetimi, operasyonel risk yönetimi, siber dayanıklılık, siber güvenlik ve bilgi güvenliği gibi başlıca alanlarda görev aldı ve danışmanlık kariyeri boyunca sektörde +200 firmaya danışmanlık verdi.

2023 yılında güvenlik danışmanlığı hizmetlerini odak noktasına alan DuneMount danışmanlık firmasını kurmuştur.

İletişim
Mobile: 0 555 479 72 31
E-Mail: serdar.karaman@dunemount.com

DuneMount