FELAKET KURTARMA MERKEZİ HİZMETİ REHBERİ

1. KAPSAM VE AMAÇ

1.1. Felaket kurtarma merkezi hizmeti nedir?

Kurumun kendi felaket kurtarma merkezini kurması yerine bu hizmetin dışarıdan alınmasını kapsamaktadır.

1.2. Genel bilgilendirme

1.2.1. Felaket ve felaket kurtarma nedir?

Kurumlar tarafından belirlenmiş, kritik iş süreçlerini destekleyen, BT hizmetlerinin kullanılamayacak şekilde uzun süreli kesintiye uğraması felaket olarak tanımlanır. Kurumlar için yaşamsal derecede önemli olacak bu BT altyapı unsurlarının, sistemlerin ve yazılımların tekrar çalışır hale gelmesini sağlamak için gerçekleştirilen tüm çalışmalar felaket kurtarma olarak adlandırılır.

Felaketler genel olarak "insan kaynaklı felaketler" ve "doğal felaketler" olarak iki temel kategoride ele alınır. Yaşanması muhtemel bazı felaketler şunlardır;

Yapılan bazı araştırmalara göre ülkemizde doğal felaketlerin %60'a yakınını depremler, %15'ini ise sel ve heyelanlar oluşturmaktadır. Bu nedenle BT altyapısının çalışacağı ortamların (veri merkezleri, sistem odaları, vb.) depreme dayanıklı, yükseltilmiş taban gibi özelliklerde olması; felaket kurtarma amacıyla kullanılacak merkezlerin de altyapısı sağlam binalardan seçilmesi gerekmektedir.

İnsan faktörü de önemli felaketlere neden olabilmektedir. Özellikle yurdumuzda yaşanması muhtemel terör saldırıları, darbe teşebbüsleri gibi nedenlerle kurumların veri merkezleri ve sistem odaları tehlike altındadır. Kuruma yapılacak herhangi bir saldırıdan kurum BT altyapısı etkilenebilir. Bu nedenle BT altyapısının yer aldığı ortamlar korunmalı ve bu gibi durumlar için önlem alınmalıdır.

Kurum çevresinde bulunabilecek benzin istasyonu, askeri binalar, emniyet güçlerine ait binalar, araç

otoparkları felaket oluşturabilecek diğer unsurlar arasındadır. Kurumların BT altyapı unsurlarını, mümkün oldukça bu gibi tehdit unsurlarından uzak bölgelere konumlandırmaları önerilir.

1.2.2. FKM hizmeti nedir?

Felaket Kurtarma Merkezi (FKM), kurumun bir felaket yaşaması durumunda, mevcut BT hizmetlerinin en az kayıp ile tekrar çalışabilmesini sağlayacak şekilde hazırlanmış bir merkezdir.

Kurumların özelikle kritik iş süreçlerini destekleyen BT hizmetlerini, herhangi bir nedenden dolayı sunamaz duruma gelmeleri önemli sorunlara yol açabilmektedir. Bu nedenle, oluşabilecek sorunlar için önceden tedbirler almak gerekmektedir.

Kurum öncelikli olarak, kritik iş süreçlerini ve bu süreçlerin çalışmasını sağlayan BT hizmetlerini (sistemlerinin, yazılımlarının, vb.) belirlemelidir. İş birimleri ile BT ekiplerinin katılımında gerçekleştirilecek bu iş etki analizi çalışması ile kurum için kritik BT hizmetleri (sistemleri, yazılımları, vb.) ortaya çıkarılır. Felaket durumunda bu öncelikli olarak bu kritik BT hizmetlerinin çalışır hale getirilmesi hedeflenir.

Bir sonraki adım, kritik BT hizmetlerine yönelik risklerin yönetilmesidir. Öncelikli BT hizmetlerinin uzun süreli çalışamamasına neden olacak risk unsurları belirlenir, bu riskleri kontrol altına almak (riskleri ortadan kaldırmak, risklerin gerçekleşme olasılığını ya da etkilerini azaltmak) için alınması gereken tedbirler üzerinden çalışılır. Her türlü tedbire rağmen, söz konusu risklerin gerçekleşmesi durumunda hizmetin aksamadan nasıl sürdürüleceği çözümlenmelidir. Bu nedenle bir proje kapsamında, olası bir felaket durumunda kurumun bilişim hizmetlerini kesintisiz yürütebilmesini sağlamak amacı ile (eğer varsa kurum iş sürekliliği yaklaşımı ile uyumlu) bir Felaket Kurtarma Planı hazırlanmalı, bu projenin bir parçası olarak, felaket durumunda devreye girecek bir FKM oluşturulmalıdır.

FKM kapsamında hedef kurumun bir felaket yaşaması durumunda, minimum kaynak ile maksimum personelin kullanabileceği şekilde BT hizmetlerinin çalıştır hale getirilebileceği bir alternatif ortam oluşturmaktır. Bir felaket durumunda, kurum BT personeli çalışmalarını FKM'de gerçekleştirebilecektir.

Kurumun herhangi bir felaket yaşaması veya kurum tarafından kullanılmakta olan BT altyapısının hizmet veremez duruma gelmiş olması ve bu duruma kısa sürede çözüm bulunamayacağının belirlenmesi durumunda, kurum felaket kurtarma planını yürütmeli, kesintiye uğrayan BT hizmetini (veya BT hizmetlerini) FKM'de tekrar çalışır duruma getirmelidir.

1.2.3. Felaket Kurtarma ve iş Sürekliliği arasındaki ilişkiler ve farklar nelerdir?

İş Sürekliliği, bir kurumun, herhangi bir felaket, yaşamını etkileyebilecek her türlü kesinti durumunda, işin devamlılığını sağlayabilmesi için uygulaması gereken süreç, kural, karar ve etkinliklerden oluşur. Felaket Kurtarma ise daha çok BT ile ilişkili olarak kullanılan bir kavramdır. İş Sürekliliği'ni etkileyen,

BT hizmetlerinin kullanılamayacak şekilde uzun süreli kesintiye uğramasına neden olacak durumlarda, kurumlar için yaşamsal derecede önemli BT altyapı unsurlarının, sistemlerin ve yazılımların tekrar çalışır hale gelmesini sağlamak için gerçekleştirilen tüm çalışmalar felaket kurtarma olarak adlandırılır. Felaket Kurtarma, İş Sürekliliği kapsamında, İş Sürekliliği'nin bir parçası olarak ele alınması gereken bir konudur. Kurumlarda genellikle İş Sürekliliği ile Felaket Kurtarma kavramlarının karıştırıldığı gözlenmektedir. İş Sürekliliği her türlü kesinti durumunda (BT yardımı ile veya BT yardımı olmaksızın) işin devamlılığının sağlanabilmesi ile ilgilidir. Felaket Kurtarma ise uzun süreli BT kesintilerine odaklanmaktadır. Bu yüzden İş Sürekliliği için kullanılabilecek bazı yöntemler Felaket Kurtarma kapsamına girmemektedir. Örneğin, İş Sürekliliği kapsamında, bir felaket anında BT hizmetlerinin devre dışı kalması durumunda, belirli faaliyetlerin BT yardımı olmaksızın, el ile gerçekleştirilmesi planlanabilir. Ya da kuruma ait BT altyapısının yedekli olarak çalışması sağlanabilir. Bu yapılarda birincil altyapıda bir sorun olduğunda anlık birkaç düzenleme ile diğer altyapı çalışır hale getirilebilmektedir.

Yaşanabilecek daha geniş çaplı bir felaket durumunda sadece bu tür bir yedekleme ile iş sürekliliğinin sağlanması mümkün olmayabilir. BT hizmeti durabilir, veri kaybı yaşanabilir. Yaşanabilecek bu tür felaket senaryolarında, kurumun en az hasarla kurtulabilmesi için alması gereken bazı önlem ve faaliyet planları olmalıdır.

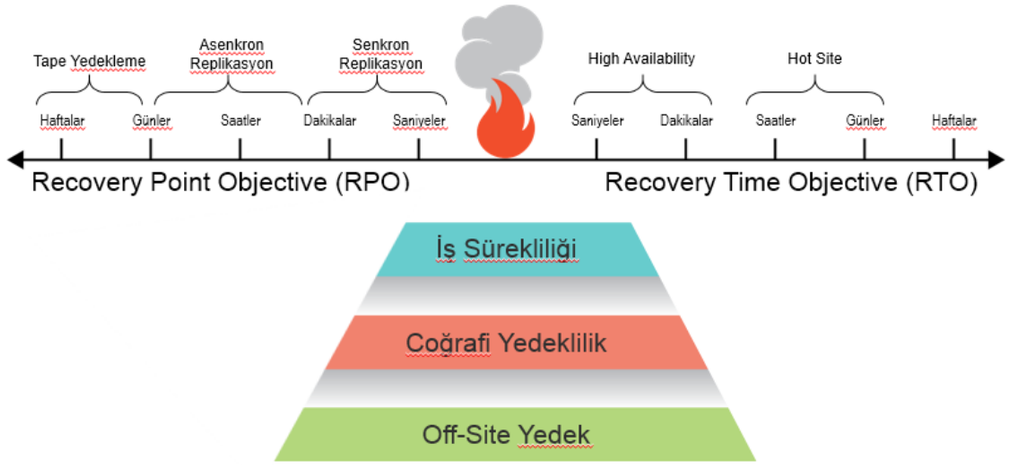
FKM felaket durumunda (ya da uzun süreceği belirlenmiş kesintilerde) devreye alınır. FKM kuruma ait kritik BT hizmetlerinin, sistemlerinin ve yazılımlarının genellikle kurum veri merkezi/sistem odasına uzak bir yerleşimde barındırılması, asenkron bir veri transferi ile verilerin FKM'ye aktarılması/yedeklenmesi mantığına göre tasarlanır. Felaket durumunda, daha önce hazırlanmış bir felaket kurtarma planı üzerinden kurum sunucuları, yazılımları sırası ile devreye alınır ve FKM'ye en son aktarılmış veri üzerinden BT hizmetinin sunulması sağlanır.

Dolayısı ile bir çok kurumun kritik BT hizmetleri, sistemleri ve yazılımları için kendi imkanları ile bir süreklilik planı planlamalı ve ilave olarak FKM ile felaket durumlarına hazırlıklı olmalıdır.

Kurumların, bir FKM yatırımı yapsın veya yapmasın, kritik BT hizmetlerine ilişkin verilerin yedeklerini farklı bölgelerde de saklaması önerilir. Sadece bu konuda hizmet veren kuruluşlar bulunmaktadır.

2. YAPILACAK İŞİN TANIMI

2.1. Replikasyon çözümleri nedelerdir?



FKM çözümlerinde farklı yöntemlerle veriler FKM'ye taşınabilir. Bu yöntemler seçilirken çözümün maliyeti ve performansı yanı sıra, iş birimleri ihtiyaçları doğrultusunda RPO-RTO değerleri göz önünde bulundurulmalıdır.

RPO (Recovery Point Objective – Kurtarma Noktası Hedefi) değeri, kurumun kabul edebileceği veri kaybı ile ilişkili bir değerdir. Veriler veri merkezinden (veya sistem odasından) belirli aralıklarla FKM'ye transfer edilir. Herhangi bir felaket durumunda, son transfer süresinden felaket anına kadar geçen sürede bir veri kaybı yaşanacaktır. RPO, kurumun kabul edebileceği maksimum veri kaybını süre olarak ifade eder. Örneğin, bir kritik BT hizmeti için RPO değerinin 1 saat olması, BT hizmetinin en fazla 1 saatlik bir veri kaybı ile tekrar çalıştırılması hedeflendiği anlamına gelir. Herhangi bir felaket ile karşı karşıya kalındığında veya herhangi bir nedenle veri kaybı yaşandığında, BT hizmeti en azından 1 saat önceki durumunda (veri açısından) çalışır hale getirilebilmelidir.

RTO (Recovery Time Objective – Kurtarma Zaman Hedefi) değeri, kurumun kabul edebileceği kesinti süresi ile ilgili bir değerdir. Bir felaket yaşanması durumunda, kesintiye uğrayan BT hizmeti, FKM'de devreye alınacaktır. RTO, kesintiye uğrayan BT hizmetinin ne kadar süre içerisinde çalışır hale getirileceğine dair hedef süredir. Örneğin bir BT hizmeti için RTO değerinin 4 saat oluşu, hizmetin herhangi bir nedenle çalışama hale gelmesi durumunda en geç 4 saat sonra içerisinde çalıştırılması gerektiği anlamına gelir.

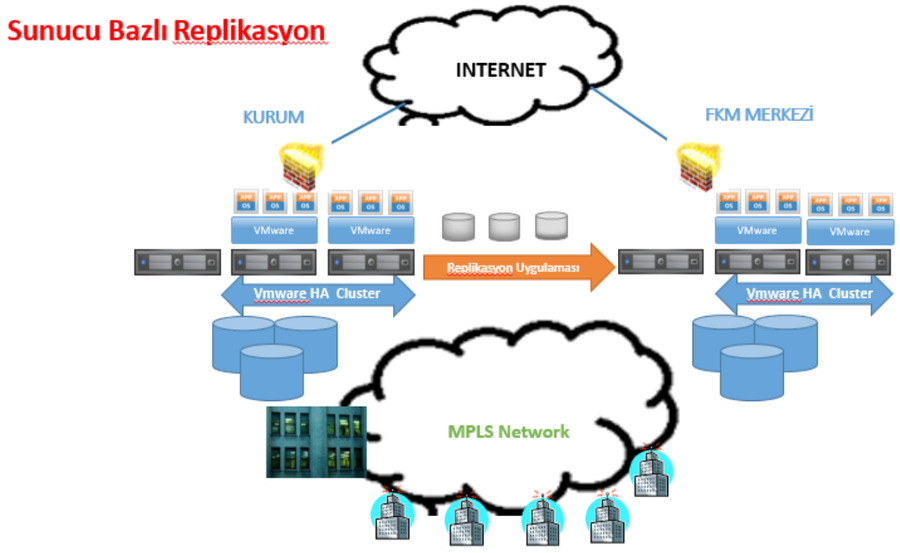
Her ne kadar kurumlar bir felaket durumunda bile kesintisiz (veya minimum RPO ve RTO sürelerinde) hizmet almak isteseler de, bu durum veri merkezi ile FKM arasında bulunan hat altyapısının, kullanılacak donanım ve yazılım unsurlarının maliyetlerini arttıracaktır. Bu nedenle kurumların (ilgili iş birimlerinin ve BT ekiplerinin bir araya gelmesi ile) kesinti ve veri kaybından kaynaklanacak iş kaybını göz önünde

bulundurarak RTO ve RPO değerlerini iyi hesap etmeleri, ihtiyaca uygun bir FKM altyapısı planlanmasına katkı sağlamaları önerilir.

2.1.1. Sunucu tabanlı replikasyon

Kurum altyapısında bulunan sanal sunucuları FKM'ye taşımak için sunucu tabanlı taşıma yönteminden yararlanabilir. Bu yöntemde, kurum tarafından kullanılan sanallaştırma platformuna göre farklı yardımcı uygulamalar kullanılarak (VMware için SRM (Site Recovery Manager), Microsoft Hyper-V için SCVMM (System Center Virtual Machine Manager) veya sanallaştırma platformundan bağımsız yazılımlar, Veeam Enterprise, Veritas, DoubleTake, vb.), sanal sunuculara ait imajların FKM'ye taşınması sağlanabilir.

Bu tür bir taşıma yönteminden yararlanılacaksa, yardımcı uygulamaların lisanslarının tam olarak temin edilmiş olmasına dikkat edilmelidir. Kullanılan yardımcı yazılım ve bu yazılımın yapılandırılma biçimine göre değişmekle birlikte genellikle RPO değerlerinin yüksek olduğu çözümler için daha uygun görünmektedir.

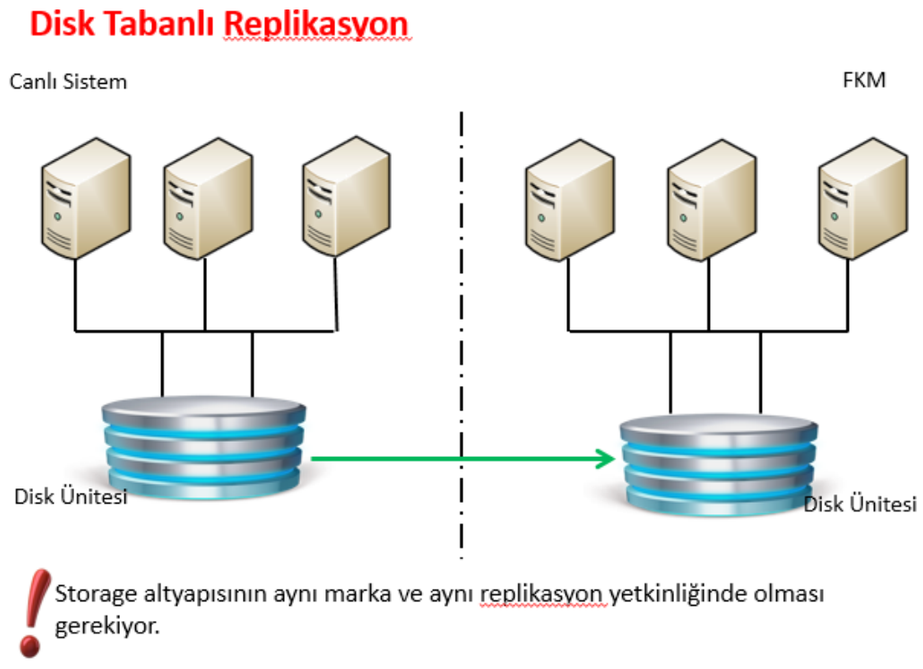


2.1.2. Disk tabanlı replikasyon

Kurum tarafından kullanılan depolama birimleri özelliklerine göre disk tabanlı veri taşıma sağlanabilir. Bu yöntemde veri depolama birimleri arasında taşınacağı için, FKM'de yer alan sunucuların çalışır durumda olması gerekmemektedir. Fakat bu tür bir taşıma yönteminin kullanılabilmesi veri merkezinde/sistem odasında ve FKM'de kullanılan depolama birimlerinin aynı üreticiye ait olmalarını ve aynı taşıma yetkinliğinde olmalarını (kullanılacak yazılımı/yöntemi desteklemelerini) gerektirir. Üreticilerin kendilerine özel taşıma (replikasyon) yazılımları kullanılarak veri taşıma sağlanabilir. Örneğin kurum EMC firması tarafından üretilmiş depolama birimleri kullanıyor ise Recover Point, MirrorView, VNX Replicator, SRDF, VPLEX yazılımlardan yararlanılabilir. Bu yazılımların her birinin farklı özellikleri ve bu özellikler ile doğru

orantılı değişen maliyetleri bulunmaktadır. Recover Point kısa aralıklar ile taşıma gerçekleştiren maliyeti yüksek bir yazılım iken MirrorView uzun aralıkla ile taşıma gerçekleştiren daha ekonomik bir çözüm sunabilmektedir. Taşıma için kullanılacak yazılım seçilmeden önce detaylı bilgi tedarikçilerden talep edilmelidir. Kurum tarafından kullanılan depolama birimlerine göre taşıma için yararlanılacak yazılım da farklı olacaktır. Örneğin Netapp depolama birimleri için SnapMirror, HP için 3PAR Replication Software Suite, vb. kullanılabilir.

Gerek veri merkezi/sistem odası ve FKM'de yer alan depolama birimlerinin aynı üretici firma ürünleri olma zorunluluğu, gerekse bu tür bir taşıma yönteminden istenilen RTO ve RPO değerlerinin sağlanabilmesi için kullanılacak taşıma yazılımı nedeniyle bu taşıma yöntemi ek bir yatırımı gerektirebilir.



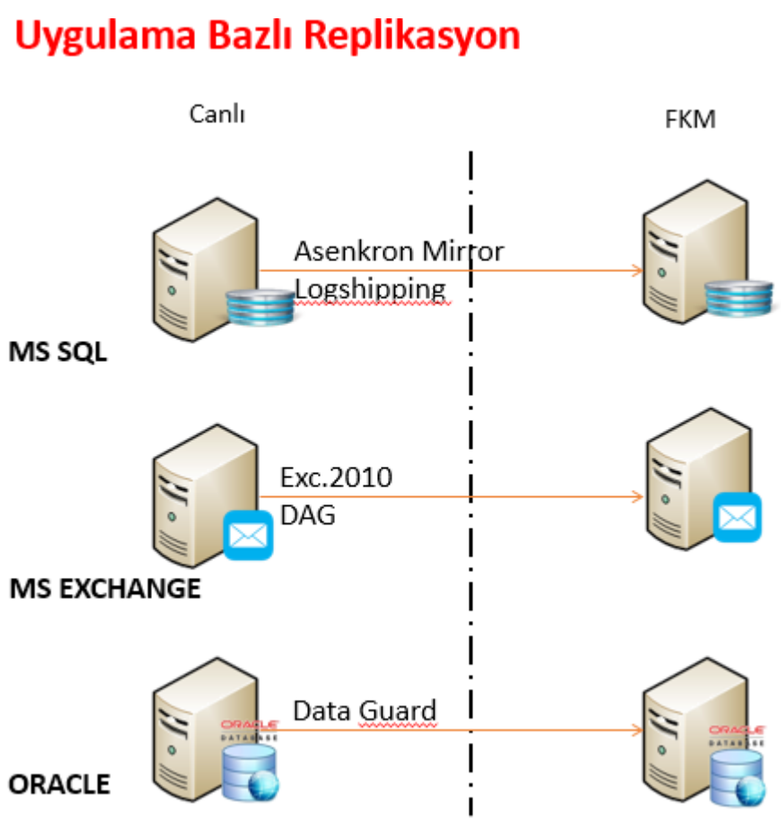
2.1.3. Uygulama tabanlı replikasyon

Veri merkezinde/sistem odasında yer alan verilerin, FKM ortamına taşınması amacı ile kullanılan yöntemler içerisinde en ekonomik görünen ancak yazılım lisansları ve kurulum/yönetim için gerekecek personel gücü nedeni ile o kadar ekonomik sonuçlar doğurmayan bir taşıma yöntemidir. Bu yöntem ile uygulamaların ve veri tabanlarının içeriğinde bulunan özellikler aracılığı ile replikasyon sağlanmaktadır.

Microsoft SQL Server (LogShipping, Always On Availability Groups), Oracle Database (Data Guard), Microsoft Exchange Server (DAG) gibi sunucu uygulamaları ve veri tabanı yazılımları içerisinde yer alan özellikler sayesinde replikasyon sağlanabilir. Ancak kullanılacak özelliğe bağlı olarak, uygulamaların farklı lisanslama

modelleri ile kullanılması gerekebilir. Örneğin SQL Server 2012 Standart sürümü ile Log Shipping özelliğini kullanarak (asenkron bir biçimde) replikasyon gerçekleştiren bir kurum, daha düşük RPO ve RTO değerleri ile replikasyon için Always On Availability Groups özelliğinden yararlanmayı isteyebilir. Böyle bir durumda, kurumun SQL Server 2012 Standart sürümünü Enterprise sürümüne yükseltmesi gerekecek, bu da ek ilave bir lisans maliyetini beraberinde getirecektir.

Uygulama tabanlı replikasyonun planlanıp devreye alınması sonrası, FKM'de yer alan uygulamalar belirli aralıklarla takip edilerek replikasyonun sağlıklı bir şekilde gerçekleştiği güvence altına alınmalıdır. Felaket durumunda FKM'de yer alan uygulamalara hızlı bir biçimde erişimi sağlamak için uygulanması gereken ek adımlar (IP ve DNS değişiklikleri, vb.) planlanmalıdır. Bu modelde veri merkezinde/sistem odasında yer alan sunucular ile birlikte FKM'de yer alan sunucular da çalışır durumda olmalıdır. Replikasyon sırasında ve felaket durumunda FKM'de yer alan uygulama devreye aldığında herhangi bir sorun yaşanmaması için FKM'de kullanılacak sunucuların veri merkezinde/sistem odasında yer alan sunucular ile benzer özelliklerde olması gerekmektedir.



2.2. FKM hizmeti alınacak uygulamaların/hizmetlerin değerlendirmesi yapıldı mı?

Felaket durumunda tüm altyapının birebir çalışması öngörülmemelidir. Beklenti belirlenen sürede, iş sürekliliğini sağlayacak hizmetlerin, sistemlerin, yazılımların çalışır hale getirilmesi olmalıdır. Bu nedenle her hizmetin, sistemin, uygulamanın FKM ortamına replikasyonu düşünülmemelidir.

Rehberin önceki bölümlerinde anlatıldığı şekilde, iş birimleri ile BT ekiplerinin katılımında gerçekleştirilecek bir iş etki analizi çalışması ile kurum için kritik BT hizmetleri (sistemleri, yazılımları, vb.) ortaya çıkarılmalı, söz konusu BT hizmetlerinin uzun süreli çalışamamasına neden olacak risk unsurları belirlenmeli, bu riskleri kontrol altına almak için alınması gereken tedbirler üzerinden çalışılmalıdır. Her türlü tedbire rağmen, söz konusu risklerin gerçekleşmesi durumunda hizmetin aksamadan nasıl sürdürüleceği çözümlenmelidir.

Öncelikli BT hizmetleri her kurum için farklılık gösterebilir. Ayrıca bir felaket durumunda, öncelikli BT hizmetlerinin en kısa sürede çalışabilir duruma getirilmesi için ortak kullanılan bazı BT bileşenlerinin işin en başında başlatılması da gerekebilir. Öncellikli olarak göz önünde bulundurulması gereken sistemler aşağıda ki gibi sıralanabilir:

- DNS Sunucusu
- Domain Denetçisi (kimlik doğrulama ve güvenlik için)
- Veri Tabanı Sunucusu (veriler için)
- Uygulama Sunucusu
- EBYS Sunucusu
- Terminal Sunucusu
- Muhasebe Yazılımı
- Mail Sunucusu

Bu sunucular hizmet vermeye başladıktan sonra aşağıdaki sunucular gibi hassasiyeti düşük sunucular devreye alınabilir:

- Doküman Yönetim Sistemi
- İnsan Kaynakları Sistemi
- Antivirüs ve Windows Güncelleme Sunucu
- SSL – VPN Sistemi
- Fax Sunucu
- Anti – Spam Sistemi

FKM'de mevcut veri merkezi/sistem odası içerisinde yer alan tüm unsurların bire bir kopyalarının barındırılması düşünülmemelidir. Örneğin bazı hizmetler/uygulamalar birden fazla sunucu ile hizmet verebilir. Hizmet/uygulama için canlı ortam, test ortamı, geliştirme ortamı gibi farklı ortamlar oluşturulmuş, bu ortamlarda farklı sunucular yer alıyor olabilir. Bir felaket durumunda test ve geliştirme yapılmayacağı düşünülerek, FKM'de bu ortamlarda yer alan sunucuların bulunmasına gerek görülmeyebilir.

2.3. Felaket kurtarma planı hazırlandı mı?

Felaket kurtarma planı, kurumun bir felaket yaşanması durumunda, gerçekleştirilecek faaliyetleri içeren planlardır. Bu plan içerisinde, kurum için önemli hizmetlerin ve bu hizmetleri oluşturan bileşenlerin bir felaket durumunda (genellikle bir Felaket Kurtarma Merkezi) içerisinde nasıl çalışır hale getirileceği detaylı bir şekilde tarif edilir. Bu planlar içerisinde kurum ve hizmet sağlayıcının sorumlulukları belirlenmeli ve felaket durumunda tarafların hızlıca bu sorumlulukları yerine getirebilmesi için gerekli bilgilendirmeler, eğitimler düzenlenmelidir. Aksi durumda felaket anında acele ile verilen kararlar yanlışlıklara neden olabilir ve altyapının sağlıklı olarak devreye girmesi aksayabilir.

Felaket kurtarma planı, ilgili iş birimleri ile birlikte hazırlanmalı, mümkün olduğunca kapsamlı olmalı, kritik iş süreçlerinin felaket sonrası devamını, diğer önemli süreçlerin en kısa sürede başlatılabilmesini ve devamında kurumun normal işleyişe dönebilmesini sağlamalıdır.

Kurum içerisinde, ilgili bölümlerden belirli kişiler seçilip eğitilmeli ve yetkilendirilmeli, bu kişiler bir felaket anında sorumlu oldukları sistemlere erişerek, kısmen de olsa hizmetleri çalışır hale getirebilmelidir. Örneğin söz konusu kişilerin, tanımlanacak SSL VPN hesapları aracılığı ile bir felaket durumunda Internet üzerinden FKM'ye erişmesi sağlanabilir. Eğer mümkünse, kurumun FKM sağlayıcıdan bir felaket durumunda kullanılacak ofis alanı kiralaması, bu alanda çalışacak önceden belirlenmiş personelin ve en kısa sürede FKM ortamına ulaşması sağlanabilir. Bu nedenle FKM'nin ulaşımı kolay bölgelerde seçilmesi önerilir. Bir felaket durumunda FKM'ye nasıl erişileceği (hava alanı ulaşım, uçuş ve FKM'ye varış süreleri hesaba katılarak) planlanmalıdır.

Felaket kurtarma planının doğruluğu ve güncelliği, belirli aralıklarla, kapsamlı testlerle denenmelidir. Kurumlarda yaşanan değişikliklerin, planı etkilemesi durumunda, plan değişikliklere göre uyarlanmalı ve yeniden test edilmelidir. Bu plan yalnızca felaket anında kullanılan bir belge değil, aynı zamanda kurumun iş ve hizmet sürekliliği ile ilgili işleyişinde ve süreçlerinde aksaklık ve eksiklerin tespit edilmesini sağlayan, felaketlerin önlenmesi ve etkilerinin azaltılması yönünde iyileştirmeleri de mümkün kılan bir belge olmalıdır.

2.4. Hizmet alınacak sağlayıcıların değerlendirmesi yapıldı mı?

Alınacak hizmet kapsamı belirlendikten sonra, FKM hizmeti sağlayabilecek kurumlar hakkında detaylı bir değerlendirme yapılması gerekmektedir. Bu değerlendirmede altyapı, yönetim ve süreç unsurları göz önünde bulundurulmalıdır.

FKM hizmet sağlayıcının daha önce benzer altyapılara sahip kurumlara nasıl hizmet verdikleri ve söz konusu kurumların memnuniyetleri değerlendirilmelidir. Bu aşamada hizmet sağlayıcıdan bir referans listesinin istenmesi, verilen referans listesinden kurum altyapısına en uygun diğer kurumlar (veya firmalar) ile referans görüşmesi yapılması önerilir. Alınan hizmetin kritikliğine göre referans ziyaretleri yapılarak sağlanan FKM hizmeti hakkında detaylı bilgi edinilebilir.

FKM hizmet sağlayıcının sektörün öncü firmalarından olmasına özen göstermesi gerekmektedir. İrili ufaklı birçok sağlayıcı FKM hizmetlerini sağlayabilmektedir. Ancak kurumun mümkün olduğunca köklü sağlayıcıları seçmesi önerilir. Bunun sebebi benzer hizmetleri uzun süredir veren firmaların daha tecrübeli firmalar olması ve bünyesinde yetkin personeller barındırmasıdır.

Çalışılacak firmaların ekonomik güçlerinin yüksek olması da önemli kıstaslardandır. FKM hizmet sağlayıcının ekonomik bir kriz içerisine girmesi, maliyetlerini azaltarak hizmet kalitesinden ödün vermesine ve olası bir iflas durumunda taahhüt edilen hizmetlerin sunulamaması nedeniyle kurumun mağdur durumda kalmasına neden olabilir.

Hizmetin alınacağı firmanın seçiminde, FKM hizmet sağlayıcısının:

- Finansal durumu.
- Organizasyonel yapısı, FKM projesinde, proje sürecini ve kapsamını belirlenen süre içinde yürütebilecek yeterlilikte olup olmadığı.
- Sektördeki tanınırlığı, FKM hizmet sağlayıcıya sektörde duyulan güven.
- Ortaklık ilişkisinde olduğu şirketler.
- Birlikte çalıştığı donanım ve yazılım üretici firmalar.
- Geçirdiği denetimlere ilişkin raporlar.
- Hizmet sunumu ve yönetimi için kullanılan teknolojiler.
- Personelinin teknik yeterliliği.
- Referansları.
- Sunduğu hizmetin bedeli.
- Kalite belgeleri ve hangi standartlarla uyumlu oldukları.

göz önünde bulundurulabilir.

2.5. FKM'nin altyapı değerlendirmesi yapıldı mı?

Bir üst maddede belirtilen genel değerlendirme dışında, FKM hizmet sağlayıcının belirli altyapı yeterliliklerini sağlamış olması beklenmektedir.

- Fiziksel Altyapı Yeterliliğini Ölçmek İçin Sorulabilecek Sorular:
  - FKM kaç metre karelik bir alana kurulmuş, bu alanın ne kadarı veri merkezi olarak kullanılıyor?
  - Hizmet sağlayıcının kaç adet veri merkezi var, veri merkezleri arasında bulunan mesafe kaç kilometre? (Birden fazla veri merkezi olan ve veri merkezleri arasında en az bir tanesi uzak mesafede olan veri merkezi hizmet sağlayıcıları, felaket kurtarma ve iş sürekliliği açısından tercih sebebidir.)
  - FKM ile ulaşım alanları (hava alanı, otogar, tren istasyonu... vb.) arasındaki mesafe nedir?
  - FKM ile tehlike arz edebilecek kamu kurumları (emniyet, polis, itfaiye... vb.) arasındaki mesafe nedir?
  - FKM yakınında yanıcı veya patlayıcı bir imalathane veya benzin istasyonu bulunuyor mu?
  - FKM ile otopark alanı arasındaki mesafe nedir?
  - Yangın, sel, deprem gibi doğal afetler için alınan tedbirlerin neler? (Örneğin sel felaketine karşın

eğimli bir arazide mi konumlanmakta, yangın için erken uyarı sistemi var mı? Kaç ölçeğe kadar bir deprem dayanıklılığına sahip?)

- Teknik Altyapı Yeterliliğini Ölçmek İçin Sorulabilecek Sorular:
  - Uluslararası veri merkezi değerlendirme standartlarından herhangi birine uygunluğu var mı? (Bu standartlar veri merkezinin kesintisiz hizmet vermesi için belirlenmiş standartlardır. Örneğin Uptime Institute tarafından belirlenen Tier standartları değerlendirilebilir. Bu standartlar genel olarak altyapı yedekliliği baz alınarak hazırlanmıştır.)
  - Enerji yedekliliği var mı?
  - Farklı trafolardan yedekli elektrik sağlanıyor mu?
  - UPS, akü, jeneratör gibi besleme ürünleri yedekli olarak sağlanabiliyor mu?
  - Enerji kesintisi durumunda jeneratör aracılığı ile kaç gün beslemesiz hizmet sağlanabilir?
  - İklimlendirme altyapısı yedekliliği sağlanıyor mu?
  - Yangın söndürme altyapısı mevcut mu?
  - Altyapı bakımı için kesinti süresi gerekmekte mi? Gerekiyor ise ne kadar?

3. İŞ MODELİ

3.1. Fiyat performans değerlendirmesi yapıldı mı?

Kurum gerekli değerlendirmeleri yaptıktan sonra birden fazla hizmet sağlayıcıdan teklif talep etmelidir. Tekliflerin iletilen şartnameye uygunluğu kontrol edilmeli ve hizmet sağlayıcıların tekliflerinin şartnameyi birebir karşılaması sağlanmalıdır. FKM hizmet sağlayıcıların hizmet sağladıkları altyapının kurum tarafından kullanılmakta olan BT hizmetleri, sistemleri ve yazılımları için uygun olmasına dikkat edilmeli ve kıyaslama yapılırken kullanılan platformların güncel ve endüstri standartlarını karşıladığından emin olunmalıdır. Alınan hizmet bedelleri ile hizmet sağlayıcının kalitesi karşılaştırılarak değerlendirilmesi ve hizmeti uygun şekilde verebilecek olan sağlayıcı ile sözleşme aşamasına geçilmelidir.

Fiyat değerlendirmesi yaparken replikasyon modeli ve RPO-RTO değerleri konusunda titiz olunmalıdır. Benzer replikasyon yöntemleri arasında değerlendirme yapılmalı, teklif aşaması öncesinde ihtiyaçlar aday FKM hizmet sağlayıcılara iletilmeli ve hizmet sağlayıcıdan bu özelliklerde bir altyapı sağlaması talep edilmelidir. Kritik uygulamaların belirlenmesi konusunda hizmet sağlayıcından destek istenebilir ve hizmet sağlayıcıdan uygun replikasyon çözümü önermesi talep edilebilir.

3.2. Hizmet sözleşmesi, gizlilik sözleşmesi ve görev dağılımı yapıldı mı?

Kurum ve hizmet sağlayıcı arasında hizmetin verileceği süre zarfında uyulacak kuralların ve hizmetin kapsamının belirlenmesi için hizmet sözleşmesi yapılır. FKM hizmet sağlayıcı tarafından sunulacak tüm hizmetlere ilişkin detaylar bu sözleşmeye eklenmeli ve karşılıklı görev tanımları ve sınırları net olarak belirlenmelidir.

Kurum, veri merkezi hizmet sağlayıcı ile sözleşme aşamasına geldiğinde, hizmet kapsamı içerisinde olan tüm kalemleri kontrol etmeli, teklifte olan ancak sözleşmede olmayan bir hizmet kalemi var ise ilgili hizmet sağlayıcı temsilcisine bu durumu iletmelidir. Teklifte bulunan envanter de aynı şekilde kontrol edilmeli ve sunulan envanterin, sözleşme maddelerinde yazan envanter ile aynı kapsamı sağladığından emin olunmalıdır. Kurum hizmet alacağı sağlayıcı ile bir gizlilik sözleşmesi yapmalıdır. Gizlilik sözleşmesi hem kurumun hem de hizmet sağlayıcının haklarını belirleyen önemli bir sözleşmedir. Gizli bilgi ifşa eden tarafın kendisi, işçileri, şubeleri ya da çalışanlarınca, diğer tarafın işçileri, şubeleri ya da çalışanlarına açıklanan her türlü fikir, buluş, iş, metot, ilerleme ve patent, telif hakkı, marka, ticari sır ya da diğer yasal korumaya konu olan ya da olmayan her türlü yenilik; tarafların arasındaki ticari ilişki esnasında öğrenecekleri yazılı veya sözlü tüm ticari, mali, teknik bilgiler, taraflardan herhangi birinin diğerine verdiği tüm teklif ve/veya talepler ve bunların içerikleri, nihai müşteri bilgileri ve konuşma bilgileri sır olarak kabul edilmelidir. Bu gizli bilgileri tarafların koruması ve kesinlikle 3. şahıslar ile paylaşmaması sağlanmalıdır.

Kurum FKM hizmet sağlayıcı dışında, farklı hizmet sağlayıcılar ile çalışıyor olabilir. Böyle bir durumda, kurumun aldığı hizmetlerin aksamaması için farklı hizmet sağlayıcıları ile yapılan sözleşmeler içerisinde sınırlar net olarak belirlenmelidir. Örneğin kurum, FKM hizmetleri için bir hizmet sağlayıcıdan, uygulama destek hizmeti için farklı bir hizmet sağlayıcıdan yararlanıyor olabilir. Bu durumda kurumun bu iki sağlayıcı ile yapacağı sözleşmelerde, hizmet sağlayıcı görev ve sorumluluklarını net olarak belirtmesi gerekir. Görev ve sorumlulukların net olarak belirtilmediği durumlarda, hizmet sağlayıcılar yaşanan sorunlarda sorumluluğun kendilerinde olmadığını belirtip, suçu diğer hizmet sağlayıcıya atabilir, sorunun kaynağı olarak diğer sağlayıcıyı gösterebilir. Böyle bir durumda kurumun almakta olduğu hizmette aksaklık yaşanmasına neden olacaktır. Görev ve sorumluluklar belirlenirken, kurum üzerine düşen görevler de değerlendirilmelidir. Kurum, alınacak hizmete ilişkin hizmet seviyesi beklentilerini FKM hizmet sağlayıcı ile paylaşmalı, FKM hizmet sağlayıcının hizmet sunumuna ilişkin bu beklentileri karşılayacak taahhütler vermesini sağlamalıdır. Sözleşme içerisinde yer alan, hizmet kalitesi ile ilgili madde iyi değerlendirilmeli ve özellikle RTO ve RPO ile ilgili servis seviyesi anlaşması (SLA- Service Level Agreement) maddelerinin sözleşmede olmasına özen gösterilmelidir.

3.3. Kurumun tabi olduğu kanuni düzenleme olup olmadığı kontrol edildi mi?

Kurumun uyum sağlaması gereken yasal düzenlemeler FKM hizmet sağlayıcı seçiminde önemli bir etkendir. BTK ve BDDK gibi kurumların hazırlamış oldukları bilgi teknolojileri hizmet düzenlemelerine uyan kurumlar dikkate alınmalıdır. Genellikle yasal düzenlemeler veri güvenliği ile ilgili konuları içermektedir. Örneğin; kişisel bilgiler veya kredi kartı bilgileri saklayan bir kurum, diğer kurumlara oranla daha yüksek güvenlik içeren bir altyapı gereksinimine sahip olabilir. Bu gibi düzenlemeler maliyetleri ciddi bir şekilde değiştirdiğinden teklif aşaması öncesinde bu ve benzeri durumlar hizmet sağlayıcılara bildirilmeli, hizmetin alımı sırasında da hizmet sağlayıcının ilgili düzenlemelere uygunluğu takip edilmelidir.

Kurumun uyması zorunlu bazı yasal düzenlemeler içerisinde FKM'nin veri merkezine/sistem odasına

uzaklığı, FKM özellikleri, güvenlik önlemleri, vb. net olarak belirlenmiş olabilir. Bu durumda ilgili düzenleme ile belirtilen şartlara uymayan sağlayıcıları kurum dikkate almamalı, ihale kapsamına dâhil etmemelidir. Kurum gerekmesi durumunda FKM ortamını gidip ziyaret ederek düzenlemelere uygunluğunu kontrol etmelidir.

4. ÇIKTILAR

4.1. Elektrik tüketim raporu talep edildi mi?

Kurum özellikle Hibrit Bulut, Özel Bulut veya Barındırma hizmeti alınması durumunda konumlandırılan donanımların kullandığı enerji tüketimin ölçülüp faturalanmasını isteyebilir. Bu ölçümler aylık olarak fatura gününden önce kuruma bildirilmeli ve harcanan enerji tutarınca fatura düzenlemesi yapılması talep edilebilir.

4.2. Yedekleme raporu talep edildi mi?

Altyapı sağlayıcı vermiş olduğu yedekleme hizmeti kapsamında kuruma alınan yedeklerin boyutlarını paylaşmalı ve her ay değişen veri boyutuna göre kuruma faturalama yapmalıdır.

4.3. Replikasyon raporu talep edildi mi?

Kurum hizmet aldığı Felaket Kurtarma Merkezi'ni verilerin ne kadar sürede replike edildiği ve replikasyonun tamamlanma durumunu kontrol etmek için replikasyon sonuç raporu talep edebilir.

4.4. Replikasyon hattı raporu talep edildi mi?

Kurum replikasyon hattının ne kadar yoğunlukla kullanıldığını öğrenmek amacı ile replikasyon hattı çıktısı talep edebilir. Bu rapor doğrultusunda hattın arttırılması veya düşürülmesi gibi kararları verebilir.

TÜBİTAK-BİLGEM-YTE