

CAMIŞ MENKUL DEĞERLER A.Ş.

**BİLGİ SİSTEMLERİ ACİL DURUM
MÜDAHALE ve KURTARMA PLANI
BİLGİ SİSTEMLERİ GÜVENLİĞİ**

Yönetici Özeti

CAMIŞ MENKUL DEĞERLER A.Ş. Bilgi Sistemleri Acil Durum Müdahale Planı, CAMIŞ MENKUL DEĞERLER bilgi sistemleri bünyesinde karşılaşılabilecek olan acil durumlar ve alınmış önlemleri içermekte, gerekli ekiplerin dağılımı ile hareket planlarını tanımlamaktadır.

Müdahale Planı çerçevesinde yaşanabilecek olası acil durumlar; doğal afetler, ağ/iletişim teknoloji sorunları, bilişim saldırıları ve ARACI KURUM SİSTEMİ SORUNLARI başlıklarında incelenmiştir. Oluşması muhtemel sorunlar ilgili bölümlerde tanımlanmış, sorun kaynakları ve olası hasar boyutları tahmin edilmiştir.

Acil durumlara müdahale amaçlı olarak özel müdahale ekipleri oluşturulmuştur; Merkez ve Merkez dışı örgütlerde karşılaşılan teknoloji sorunları, iletişim sorunları, bilişim saldırıları ve ARACI KURUM SİSTEMİ SORUNLARINA yönelik olarak özel ekipler oluşturulmuş, sorumluluk alanları ve ekip üyeleri belirlenmiştir. Ayrıca her ekibin görevleri, müdahale planlarının ilgili yerlerinde net çizgilerle tanımlanmıştır.

Oluşması muhtemel tüm acil durumlar için ayrı müdahale planları hazırlanmış, her müdahale planı, sorumlu ekipler, görev tanımları ve görev adımları net olarak ifade edilmiştir. Hazırlanan yönergeler doğrultusunda tanımlanmış ekiplerin hangi durumlara doğrudan müdahale edebileceği, hangi durumlarda ise dış ürün/hizmet sağlayıcı kurum ile irtibata geçeceği tanımlanmıştır.

CAMIŞ MENKUL DEĞERLER, hazırlanmış olduğu Acil Durum Müdahale Planı ile oluşabilecek acil durumlar nedeniyle bilişim sistemlerinde karşılaşılabilecek olan sorunlara yönelik her türlü önlemi almış, görev ve olay tanımlarını yapmıştır.

İçindekiler

YÖNETİCİ ÖZETİ	2
İÇİNDEKİLER	3
1 OLASI AFET VEYA SORUN TANIMLARI	4
1.1.SİSTEM SORUNLARI	4
1.1.1 MERKEZ’DE YAŞANAN SİSTEM SORUNLARI.....	4
1.1.2 MERKEZ DIŞI ÖRGÜT SORUNLARI.....	5
1.1.3 ARACI KURUM SİSTEMİ SORUNLARI	6
1.1.4 İLETİŞİM ALTYAPISI SORUNLARI	7
1.1.5 DIŞ HİZMET SAĞLAYICILARIN HİZMETLERİNDE KARŞILAŞILABİLECEK SORUNLAR.....	7
1.2 DEPREM	7
1.3 YANGIN	8
1.4 TERÖR	8
1.5 BİLİŞİM SALDIRILARI	9
1.5.1 DAHİLİ SALDIRILAR	9
1.5.2 HARİCİ SALDIRILAR	9
2 SORUN MÜDAHALE EKİP TANIMLARI	10
3 MERKEZİ AĞ ALTYAPISI SORUN PLANI	10
4 MERKEZ AĞ SUNUCULARI SORUN PLANI	10
5 MERKEZ DIŞI ÖRGÜT SİSTEM SORUN PLANI	10
6 ARACI KURUM SORUN PLANI	10
7 İLETİŞİM ALT YAPISI SORUN PLANI	10
8 BİLİŞİM SALDIRISI SONRASI DAVRANIŞ PLANI	11
9 3. PARTİ KURULUŞLAR HİZMET SORUN PLANI	11
9.1 AĞ SERVİS SAĞLAYICILARI HİZMET SORUN PLANI	11
9.2 SUNUCU SERVİS SAĞLAYICILARI HİZMET SORUN PLANI	11
9.3 İLETİŞİM SERVİS SAĞLAYICILARI HİZMET SORUN PLANI	12
9.4 VERİ YAYINI SAĞLAYICILARI HİZMET SORUN PLANI	13
10 BİLGİ SİSTEMLERİ GÜVENLİĞİ	13

1 Olası Afet veya Sorun Tanımları

Kurumumuz bünyesinde devamlılık arzemesi gereken iş süreçleri ve bilişim altyapısına yönelik olarak karşılaşılabilecek sorunların tanımları aşağıda aktarılmaktadır. Doğal afetler, terör, sistem arızaları veya bilişim suçlarından kaynaklanan, sistemin devamlılığının aksaması, kritik sistemlerin işleyiş dışına çıkması veya gizlilik arzeden bilgilerin ifşa edilmesi sonuçları doğurabilecek durumlardan kurumumuzu etkileyebilecek olaylar aşağıda tanımlanmıştır. Listede yer almayan olaylara yönelik olarak özel önlem alınmamakla beraber, genel önlemler ölçeğinde tanımlanmamış özel durumlara da müdahale edilmektedir.

Oluşma ihtimali bulunan sorunlar aşağıda tanımlanmış, sorunların kaynakları ve iş süreçlerini etkileme düzeyleri her bir olası sorun için tahmin edilmiştir. Sorunların bazıları kısıtlı olarak “Merkez” de veya “Merkez Dışı Örgütlerde” hizmet aksamalarına neden olabilirken bazı özel durumlarda iş süreçlerinde uzun süreli aksamalar oluşabileceği ön görülmekte, önlemler bu doğrultuda şekillendirilmektedir.

1.1.Sistem Sorunları

1.1.1 Merkez’de Yaşanan Sistem Sorunları

Kaynağı kurum merkez yapısında bulunan bileşenler olan sorunları kapsamaktadır. Oluşabilecek sistem sorunu ağ temelli veya sunucu temelli olarak gerçekleşebilecektir, bu doğrultuda alınacak önlemler ve tanımlamalar için gruplama yapılacaktır, her bir sorun türü ayrıca değerlendirilecektir.

Madde I. Ağ Altyapısı Sorunları

Bölüm 1.01 Dahili Ağ Altyapısı Sorunları

Kurum merkezinde bulunan ve yerel ağda bulunan ağ bileşenlerinden kaynaklanabilecek sorunları kapsamaktadır. Yerel ağda bulunan anahtar (switch), yönlendirici (router), tekrarlayıcı (repeater), güvenlik duvarı, sanal özel ağ sistemi ve kablolu altyapısı nedeniyle oluşabileceği öngörülmektedir.

Dahili ağ sorunları oluşması durumunda yerel ağın bir bölümü kullanılamayacaktır. Kullanılmayan bölüm nedeniyle kritik önem arzedecek Aracı Kurum hizmetleri, iletişim hizmetleri ve diğer bilgi işlem hizmetleri kısmi olarak veya tamamen aksayacaktır. Oluşacak sorun nedeniyle “Merkez dışı örgüt”lerin “Merkez’e bağlantısı veya aldığı hizmetlerin devamlılığında aksamalar oluşacaktır.

Bölüm 1.02 Harici Ağ Altyapısı Sorunları

Kurum merkezinde bulunan, Merkez dışı örgüt bağlantılarını sağlayan veya iletişim altyapısı için kullanılmakta olan ağ hizmetlerinde dış kaynaklı hizmetler nedeniyle oluşabilecek olan sorunlardır. Sorun kaynağı, ağ hizmeti alınan hizmet sağlayıcı ile kurum arasında bulunan ağ bağlantılarının geçici veya kalıcı olarak kesilmesi durumudur. Ağ bağlantılarının kesilmesi, hizmet sağlayıcı kurumun ağ hizmetlerinin aksaması, taşıyıcı kurumların altyapısının aksaması veya kurum ile hizmet sağlayıcı arasında kullanılmakta olan yönlendiricilerin uyumsuzluk ortaya çıkarması sonucu oluşabileceği öngörülmektedir.

Harici ağ sorunları oluşması durumunda “Merkez dışı örgüt”ler ile “Merkez” arasında bulunan bağlantılarda aksama olacak, “Merkez dışı örgüt”lerin “Merkez” üzerinden kullanmakta olduğu hizmetler geçici olarak aksayacak, iletişim altyapısı ile Aracı Kurum hizmetlerinde aksamalar oluşacaktır.

Madde II. Sunucu Sorunları

Bölüm 1.01 Donanımsal Sorunlar

Merkez’de bulunan, temel ağ hizmetleri, Aracı Kurum hizmeti, iletişim altyapısı veya dış kaynaklı hizmet sağlayıcıların hizmetlerinin üzerinde çalışmakta olduğu sunucularda oluşabilecek donanımsal sorunları kapsamaktadır. Donanımsal sorunlar, sunucu üzerinde bulunan donanımların fiziksel zarar görmesi, kullanım ömrünün tükenmesi, uyumsuzluk, işletim sistemi tarafından kural dışı kullanım, aşırı ısınma/soğuma veya elektrik düzeyi düzensizliği sebeplerinden kaynaklanabilmektedir.

Donanım sorunları oluşması durumunda, sunucu üzerinde sorun kaynağı donanım ile eş değer özelliğe sahip, yedek olarak tanımlanmış ve sorunsuz olarak çalışması devam eden bir donanım bulunmuyor ise sunucu devre dışı kalacaktır. Elde sorun çıkardığı tespit edilen donanımdan bulunmuyor ise temin süresi kadar, bulunuyor ise ilgili donanımın sunucuya kurulması süresi kadar sunucu hizmet dışı kalacaktır. Hizmet dışı kalan sunucunun görevi doğrultusunda “Merkez dışı örgüt” ve “Merkez” hizmetlerinden bazılarında aksama olabilecektir.

Bölüm 1.02 Yazılımsal Sorunlar

Merkez’de bulunan, temel ağ hizmetleri, Aracı Kurum hizmeti, iletişim altyapısı veya dış kaynaklı hizmet sağlayıcıların hizmetlerinin üzerinde çalışmakta olduğu sunucularda oluşabilecek yazılımsal sorunları kapsamaktadır. Yazılımsal sorunlar yapılandırma hataları, yönetim hataları, yazılım güncelleme uyumsuzlukları, programlama hataları veya dış kaynaklı bir yazılımın olağan dışı işlemler yapması sonucu oluşabilmektedir.

Yazılım sorunları oluşması durumunda, sorunu oluşturan yazılımın sunucuda kullanım amacı doğrultusunda “Merkez dışı örgüt” ve “Merkez” hizmetlerinde aksama olabilecektir. Yazılımın sunucudan kaldırılması, yeniden yüklenmesi, yapılandırma hatasının düzeltilmesi veya sorunlu yazılımın bazı özelliklerinin devre dışı bırakılması süresince sorun devam edebilecektir.

1.1.2 Merkez dışı örgüt sorunları

Kaynağı kurum Merkez dışı örgütlerinde bulunan ağ veya sunucu bileşenleri olan sorunları kapsamaktadır. Merkez dışı örgütlerde yaşanabilecek sistem sorunlarının oluşturabileceği aksamalar doğrudan ilgili Merkez dışı örgütün eriştiği hizmetlerin aksamasını sağlayacaktır, merkez yapıda bulunan hizmetlerde bir aksama oluşturması beklenmemektedir. Değerlendirmeler bu bilgi ışığında sorunun Merkez dışı örgüt ile kısıtlı kalacağı varsayımı ile yapılmıştır.

Madde I. Ağ Altyapısı Sorunları

“Merkez dışı örgüt”lerin sahip olduğu, dahili haberleşme ve hizmetler için kullanmakta olduğu ağ altyapısında veya “Merkez”in sunduğu hizmetler için kullanılan bağlantıyı sağlayan ağ altyapısında oluşabilecek sorunlardır. Sorun kaynağı yerel ağ cihazları veya kablolama altyapısı olabileceği gibi “Merkez”e bağlantıyı sağlayan dış hizmet sağlayıcının hizmetlerinin aksaması da olabilmektedir.

Dahili ağ sorunları oluşması durumunda “Merkez dışı örgüt” içinde kullanılmakta olan hizmetlerde kısıtlı aksamalar olacaktır, ancak harici ağ sorunları yaşanması durumunda “Merkez dışı örgüt” ile “Merkez” arasında bulunan bağlantı aksayabilir ve çok sayıda hizmet söz konusu aksamadan etkilenebilir.

Madde II. Sunucu Sorunları

“Merkez dışı örgüt”lerin sahip olduğu, temel ağ hizmetleri, Aracı Kurum hizmetleri, “Merkez” ile paylaşılan hizmetler ve yerel paylaşım hizmetlerini sunan sunucularda oluşabilecek olan sistem sorunlarını kapsamaktadır. Bir sunucu veya sunucu ailesinde ortaya çıkabilecek sistem sorunları yazılımsal veya donanımsal olabilmektedir. Yazılımsal sorunlar yapılandırma hataları, yönetim hataları, yazılım güncelleme uyumsuzlukları, programlama hataları veya dış kaynaklı bir yazılımın olağan dışı işlemler yapması sonucu oluşabilmektedir. Donanımsal sorunlar, sunucu üzerinde bulunan donanımların fiziksel zarar görmesi, kullanım ömrünün tükenmesi, uyumsuzluk, işletim sistemi tarafından kural dışı kullanım, aşırı ısınma/soğuma veya elektrik düzeyi düzensizliği sebeplerinden kaynaklanabilmektedir.

Bir veya birden fazla sunucuda karşılaşılabilecek sorunlar nedeniyle sadece kısıtlı sayıda hizmetlerin aksaması beklenmektedir ; ancak sunucu temel ağ servislerini sunmakta ise bu durum çok sayıda hizmeti etkileyebilecektir. Aracı Kurum sürecinin parçası olabilecek bir sunucuda karşılaşılabilecek sorun ise söz konusu sürecin aksamasına neden olabilecektir. Yazılımın sunucudan kaldırılması, yeniden yüklenmesi, yapılandırma hatasının düzeltilmesi veya sorunlu yazılımın bazı özelliklerinin devre dışı bırakılması süresince sorun devam edebilecektir. Donanım sorunları oluşması durumunda, sunucu üzerinde sorun kaynağı donanım ile eş değer özelliğe sahip, yedek olarak tanımlanmış ve sorunsuz olarak çalışması devam eden bir donanım bulunmuyor ise sunucu devre dışı kalacaktır. Elde sorun çıkardığı tespit edilen donanımdan bulunmuyor ise temin süresi kadar, bulunuyor ise ilgili donanımın sunucuya kurulması süresi kadar sunucu hizmet dışı kalacaktır.

1.1.3 ARACI KURUM SİSTEMİ SORUNLARI

Kurumsal Aracı Kurum sisteminde karşılaşılabilen, Aracı Kurum yazılımı, uygulama sunucusu, veritabanı sunucusu ve ağ altyapısından oluşan sorunları kapsamaktadır. Aracı Kurum yazılımı sorunları, uygulama sunucusu yazılımsal ve donanımsal sorunları, veritabanı sunucusu yazılımsal ve donanımsal sorunları ile Aracı Kurum sisteminde kullanılan ağ kablolama altyapısı ile ağ cihazlarından kaynaklanan sorunlar nedeniyle oluşabilmektedir.

Aracı Kurum sisteminde sorunlar oluşması durumunda “Merkez”de yatırım işlemleri aksaması, “Merkez dışı örgüt”lerden yatırım işlemi yapılamaması ve çeşitli Aracı Kurum süreçlerinde kısa süreli aksamalar oluşabileceği tahmin edilmektedir. Cihaz değişimi veya donanımsal sorunların oluşması durumunda ise değişim ve cihaz temin sürelerince uzun süreli sorunlar yaşanabileceği ön görülmektedir.

1.1.4 İletişim Altyapısı Sorunları

Kurumsal iletişim altyapısında karşılaşılabilen iletişim cihazları, santral bağlantıları ve kablolama altyapısından oluşan sorunları kapsamaktadır. Kablolama altyapısının zarar görmesi, iletişim altyapısının sonlandırılmasında kullanılan cihazlarda karşılaşılan yazılımsal ve donanımsal sorunlar, iletişim cihazları ile santral arasında oluşabilecek uyumsuzluk sorunları nedeniyle oluşabilmektedir.

İletişim altyapısında sorunlar oluşması durumunda “Merkez” ve “Merkez dışı örgüt”ler arasında veya dış hatlar ile yapılacak haberleşmelerin kısa süreli olarak aksayabileceği tahmin edilmektedir. Dış hizmet sağlayıcı tarafından iletişim altyapısı cihazlarında veya kablolama altyapısında yapılabilecek değişiklik süresince haberleşmelerde kısa süreli aksamalar oluşabileceği tahmin edilmektedir. Cihaz değişimi veya donanımsal sorunların oluşması durumunda ise değişim ve cihaz temin sürelerince uzun süreli haberleşme sorunları yaşanabileceği ön görülmektedir.

1.1.5 Dış Hizmet Sağlayıcıların Hizmetlerinde Karşılaşılabilecek Sorunlar

Dış hizmet sağlayıcı kurumların sunmuş oldukları, veri sağlama , ağ altyapısı, sunucu yönetim altyapısı ve iletişim altyapısında karşılaşılabilecek sorunları kapsamaktadır. Dış hizmet sağlayıcılardan alınan ağ altyapısı hizmetlerinin aksamaması, kablolama altyapısından, hizmet sağlayıcının yönetiminde olan ağ cihazlarının donanımsal veya yazılımsal sorunlarından kaynaklanabilmektedir. İletişim altyapısı sorunları, dış hizmet sağlayıcılarca iletişim altyapısına entegre edilmiş cihazlarda oluşabilecek donanımsal veya yazılımsal problemler ile iletişim kablolama altyapısından kaynaklanabilmektedir. Veri sağlamada yaşanan sorunlar, veri sağlayıcı kurumun veri aktarım yazılımında, ağ altyapısında veya sunucularda yaşanabilecek yazılımsal veya donanımsal sorunlardan kaynaklanabilmektedir. Sunucu altyapısı sorunları, hizmet sağlayıcı kurumun yönetiminden sorumlu olduğu sunucularda donanımsal ve yazılımsal nedenlerle oluşabilmektedir.

Kurum bilgi akışı ve süreçlerince kullanılma durumları doğrultusunda dış hizmet sağlayıcılardan kaynaklanan sorunlar nedeniyle ağ ve iletişim servislerinin aksamaması beklenmektedir. Temel ağ servislerinin ve bağlantılarının aksamaması, ağda bulunan tüm servis ve Merkez dışı örgütler arası iletişimlerini aksatacağı, sürece özel servislerin aksamaması durumunda ise bölümsel aksamalarla karşılaşılması beklenmektedir. İletişim altyapısında oluşabilecek sorunlar nedeniyle Merkez dışı örgütler arası iletişim ve dış müşteriler ile iletişimde aksamalar oluşacağı tahmin edilmektedir.

1.2 Deprem

“Merkez” veya “Merkez dışı örgüt”lerde doğal etkenler sonucu oluşabilecek olan yer sarsıntılarını ve beraberinde oluşabilecek hasarı kapsamaktadır. Sadece bir “Yerleşim”in etkilenmesi gibi çok sayıda “Yerleşim”in etkilenmesi de mümkün olabilecektir. Karşılaşılan deprem tehlikesi şiddeti ve etki alanı değerlendirmelere esas teşkil edecektir.

Deprem sonucunda personel kaybı, yapısal hasar, yazılımsal hasar, donanımsal hasar ve süreç durması sorunları oluşabileceği düşünülmektedir. Hasar boyutlarına bağlı olarak öncelikle kısa süreli süreç aksamaları oluşacağı, sonrasında ise hasar tanımlamaları doğrultusunda değişken sürelerde aksamalar oluşacağı tahmin edilmektedir. Kısa süreli ve düşük şiddetli depremlerde süreçlerdeki aksamaların kısa süreli olacağı, nispeten şiddetli depremler oluşması durumunda hasar olmasa dahi personel gerektiren süreçlerin uzun süreli aksayacağı tahmin edilmektedir.

Deprem sonucu personelin zarar görmesi durumunda ilgili süreçlerin personelin konumu doğrultusunda değişken sürelerce aksayacağı tahmin edilmektedir. Personelin uzun süreli veya kalıcı olarak kaybı durumunda ilgili görevin devir alınması süresince iş süreçlerinin aksayacağı veya tamamen duracağı tahmin edilmektedir. Yapısal hasar ile karşılaşılması durumunda ise ilgili bölümde bulunan sistemlerin ve personelin durumu doğrultusunda süreçlerde aksama oluşacağı düşünülmektedir. Özellikle şiddetli depremlerden çok sayıda “Yerleşim”in etkileneceği ve bu nedenle çok sayıda sürecin büyük ölçüde aksayacağı tahmin edilmektedir.

Donanımsal hasardan etkilenen sunucular, ağ kablolama altyapısı ve çalışanlar doğrultusunda çalışma süreçlerinin ilgili “Yerleşim” için büyük ölçüde aksayacağı düşünülmektedir. Ayrıca kayıtlı veri kaybı, sistemde bulunan süreç verilerinin kaybı veya süreçlerin devamlılığının aksaması, ilişkili diğer süreçleri aksatabilecek, ek olarak kayıp bilgiler doğrultusunda yedekten geri dönüş süresi kadar temel ağ servisleri aksayacaktır. Depremden etkilenen “Yerleşim” ile “Merkez” veya “Merkez dışı örgüt”ler arasında bulunan iletişimin büyük ölçüde aksayacağı düşünülmektedir.

1.3 Yangın

“Merkez” veya “Merkez dışı örgüt”lerde karşılaşılacak elektrik, ısı veya gaz patlamaları nedeniyle oluşabilecek olan yangınları kapsamaktadır. Kurum çalışanlarının hareketi, dış hizmet sağlayıcıların çalışanlarının hareketi, elektrik altyapısında bulunan sorunlar, dış etkiler nedeniyle oluşan ısınma veya gaz dolaşım altyapısında bulunan sorunlar nedeniyle karşılaşılabilir. Dikkatsizlik veya kasıt unsuru içeren hareketlere ek olarak dış etkenlerden kaynaklanması da mümkün olabilmektedir.

Yangın sonucunda personel kaybı, yapısal hasar, yazılımsal hasar, donanımsal hasar ve süreç durması sorunları oluşabileceği düşünülmektedir. Hasar boyutlarına bağlı olarak öncelikle kısa süreli süreç aksamaları oluşacağı, sonrasında ise hasar tanımlamaları doğrultusunda değişken sürelerde aksamalar oluşacağı tahmin edilmektedir.

Yangın sonucu personelin zarar görmesi durumunda ilgili süreçlerin personelin konumu doğrultusunda değişken sürelerce aksayacağı tahmin edilmektedir. Personelin uzun süreli veya kalıcı olarak kaybı durumunda ilgili görevin devir alınması süresince iş süreçlerinin aksayacağı veya tamamen duracağı tahmin edilmektedir. Yapısal hasar ile karşılaşılması durumunda ise ilgili bölümde bulunan sistemlerin ve personelin durumu doğrultusunda süreçlerde aksama oluşacağı düşünülmektedir.

Donanımsal hasardan etkilenen sunucular, ağ kablolama altyapısı ve çalışanlar doğrultusunda çalışma süreçlerinin ilgili “Yerleşim” için büyük ölçüde aksayacağı düşünülmektedir. Ayrıca kayıtlı veri kaybı, sistemde bulunan süreç verilerinin kaybı veya süreçlerin devamlılığının aksaması, ilişkili diğer süreçleri aksatabilecek, ek olarak kayıp bilgiler doğrultusunda yedekten geri dönüş süresi kadar temel ağ servisleri aksayacaktır. Yangından etkilenen “Yerleşim” ile “Merkez” veya “Merkez dışı örgüt”ler arasında bulunan iletişimin büyük ölçüde aksayacağı düşünülmektedir.

1.4 Terör

Bir dış grup veya kişi tarafından kuruma yönelik olarak yapılan şiddet eylemlerini kapsamaktadır. Şiddet eylemleri kurum iş süreçlerinin aksatılması, kurum taşınmazlarına veya çalışanlarına zarar verilmesi biçiminde gerçekleşebilmektedir.

Şiddet eylemi sonucunda personel kaybı, yapısal hasar, yazılımsal hasar, donanımsal hasar ve süreç durması sorunları oluşabileceği düşünülmektedir. Hasar boyutlarına bağlı olarak öncelikle kısa süreli süreç aksamaları oluşacağı, sonrasında ise hasar tanımlamaları doğrultusunda değişken sürelerde aksamalar oluşacağı tahmin edilmektedir.

Şiddet eylemi sonucu personelin zarar görmesi durumunda ilgili süreçlerin personelin konumu doğrultusunda değişken sürelerce aksayacağı tahmin edilmektedir. Personelin uzun süreli veya kalıcı olarak kaybı durumunda ilgili görevin devir alınması süresince iş süreçlerinin aksayacağı veya tamamen duracağı tahmin edilmektedir. Yapısal hasar ile karşılaşılması durumunda ise ilgili bölümde bulunan sistemlerin ve personelin durumu doğrultusunda süreçlerde aksama oluşacağı düşünülmektedir.

Donanımsal hasardan etkilenen sunucular, ağ kablolama altyapısı ve çalışanlar doğrultusunda çalışma süreçlerinin ilgili “Yerleşim” için büyük ölçüde aksayacağı düşünülmektedir. Ayrıca kayıtlı veri kaybı, sistemde bulunan süreç verilerinin kaybı veya süreçlerin devamlılığının aksaması, ilişkili diğer süreçleri aksatabilecek, ek olarak kayıp bilgiler doğrultusunda yedekten geri dönüş süresi kadar temel ağ servisleri aksayacaktır. Şiddet eyleminden etkilenen “Yerleşim” ile “Merkez” veya “Merkez dışı örgüt”ler arasında bulunan iletişimin büyük ölçüde aksayacağı düşünülmektedir.

1.5 Bilişim Saldırıları

1.5.1 Dahili Saldırıları

Kurum kaynaklarının izinsiz kullanımı, kurumun sahip olduğu gizlilik derecesi bulunan bilgilere izinsiz erişim sağlanması, kurumsal bilgilerin dış kaynaklarca paylaşımı, iş süreçlerinin aksatılması, kurumsal kaynaklar ile kişisel menfaat elde edilmesi ve kurum itibarının zedelenmesi biçiminde gerçekleştirilebilecek, yerel sistemler üzerinden yapılan bilişim saldırılarını kapsamaktadır. Kurum çalışanları, dış hizmet sağlayıcı çalışanları veya kurum dışı kişiler tarafından yapılabileceği düşünülmektedir.

Kurum içinden gelen bir saldırı oluşması durumunda saldırı türü doğrultusunda iş süreci aksamaları oluşabileceği tahmin edilmektedir. Servis engelleme biçiminde gerçekleşen ve ağ altyapısı veya sunuculara yönelik saldırılar sonucunda ilgili ağ iletişimi veya sunucunun sunduğu servisleri ilgilendiren iş süreçlerinin kısa süreli olarak aksayacağı tahmin edilmektedir. Saldırının sunucu ele geçirme ve veri kaybı ile sonuçlanması durumunda, sunucu verilerinin yedekten geri yükleme süresi kadar iş süreçlerinin aksaması beklenmektedir. Veri çalınması veya geçici veri değişiklikleri yaratılması durumunda, saldırı tanımlama süresince iş süreçlerinde kısa süreli aksamalar oluşabileceği tahmin edilmektedir. Gizlilik derecesi içeren verilerin açığa çıkması durumunda maddi kayba ek olarak itibar kaybı da söz konusudur. Finansal işlemleri kapsayan bir dahili saldırı oluşması durumunda ise maddi kayıp ve itibar kaybı, sadece itibar zedelemeye yönelik görünüm değişimi temelli saldırılar sonucunda ise itibar kaybı oluşabilmektedir.

1.5.2 Harici Saldırıları

Kurum kaynaklarının izinsiz kullanımı, kurumun sahip olduğu gizlilik derecesi bulunan bilgilere izinsiz erişim sağlanması, kurumsal bilgilerin dış kaynaklarca paylaşımı, iş süreçlerinin aksatılması, kurumsal kaynaklar ile kişisel menfaat elde edilmesi ve kurum itibarının zedelenmesi biçiminde gerçekleştirilebilecek, dış ağlarda bulunan sistemlerden yerel sistemlere yönelik yapılan bilişim saldırılarını kapsamaktadır. Ağırlıklı olarak kurum dışı

kişiler, daha sonra ise kurum çalışanları veya dış hizmet sağlayıcı çalışanları tarafından yapılabileceği düşünülmektedir.

Kurum dışından gelen bir saldırı oluşması durumunda saldırı türü doğrultusunda iş süreci aksamaları oluşabileceği tahmin edilmektedir. Servis engelleme biçiminde gerçekleşen ve ağ altyapısı veya sunuculara yönelik saldırılar sonucunda ilgili ağ iletişimi veya sunucunun sunduğu servisleri ilgilendiren iş süreçlerinin kısa süreli olarak aksayacağı tahmin edilmektedir. Saldırının sunucu ele geçirme ve veri kaybı ile sonuçlanması durumunda, sunucu verilerinin yedekten geri yükleme süresi kadar iş süreçlerinin aksaması beklenmektedir. Veri çalınması veya geçici veri değişiklikleri yaratılması durumunda, saldırı tanımlama süresince iş süreçlerinde kısa süreli aksamalar oluşabileceği tahmin edilmektedir. Gizlilik derecesi içeren verilerin açığa çıkması durumunda maddi kayba ek olarak itibar kaybı da söz konusudur. Finansal işlemleri kapsayan bir dahili saldırı oluşması durumunda ise maddi kayıp ve itibar kaybı, sadece itibar zedelemeye yönelik görünüm değişimi temelli saldırılar sonucunda ise itibar kaybı oluşabilmektedir.

2 Sorun Müdahale Ekip Tanımları

Camiş Menkul Değerler A.Ş. Türkiye Şişe Cam Fabrikaları A.Ş. Teknik altı yapısını kullanmaktadır. Bu nedenle Bilgisayar altyapısı ve iletişim alt yapısında tanımlanmış sorunlar adı geçen Şirketin Bilgisayar Destek Hizmet Müdürlüğü ve Enformasyon Teknolojileri Müdürlüğüne tanımlanmış ekipler ve prosedürler dahilinde yürütülecektir. Camiş Menkul Değerlerde Teknik alt yapı konusunda koordinasyonu sağlayan yetkili bu hususlarda da gerekli koordinasyonu sağlayacaktır.

3 Merkezi Ağ Altyapısı Sorun Planı

Türkiye Şişe Cam Fabrikaları A.Ş. Bilgisayar Destek Hizmet Müdürlüğü ve Enformasyon Teknolojileri Müdürlüğüne tanımlanmış prosedürler dahilinde yürütülecektir

4 Merkez Ağ Sunucuları Sorun Planı

Türkiye Şişe Cam Fabrikaları A.Ş. Bilgisayar Destek Hizmet Müdürlüğü ve Enformasyon Teknolojileri Müdürlüğüne tanımlanmış prosedürler dahilinde yürütülecektir

5 Merkez dışı örgüt Sistem Sorun Planı

Türkiye Şişe Cam Fabrikaları A.Ş. Bilgisayar Destek Hizmet Müdürlüğü ve Enformasyon Teknolojileri Müdürlüğüne tanımlanmış prosedürler dahilinde yürütülecektir

6 Aracı Kurum Sorun Planı

Aracı Kurum Programını Kiraladığımız Geneks International Yazılım ve İletişim Teknolojileri Limited Şirketi ve Türkiye Şişe Cam Fabrikaları A.Ş. Bilgisayar Destek Hizmet Müdürlüğü ve Enformasyon Teknolojileri Müdürlüğüne tanımlanmış prosedürler dahilinde Şirketimizin Teknik alt yapıdan sorumlu yetkilisinin koordinasyonunda yürütülecektir

7 İletişim Alt Yapısı Sorun Planı

Türkiye Şişe Cam Fabrikaları A.Ş. Bilgisayar Destek Hizmet Müdürlüğü ve Enformasyon Teknolojileri Müdürlüğüne tanımlanmış prosedürler dahilinde yürütülecektir.

8 Bilişim Saldırısı Sonrası Davranış Planı

Türkiye Şişe Cam Fabrikaları A.Ş. Bilgisayar Destek Hizmet Müdürlüğü ve Enformasyon Teknolojileri Müdürlüğüne tanımlanmış prosedürler dahilinde yürütülecektir.

9 3. Parti Kuruluşlar Hizmet Sorun Planı

9.1 Ağ Servis Sağlayıcıları Hizmet Sorun Planı

Ağ altyapısı ile ilgili hizmetlerin alındığı dış hizmet sağlayıcılarının hizmetlerinde saptanan sorunlar için aşağıda tanımlanan yönergeler izlenecektir;

- Uzak veya kurum içi ağ bağlantısı hizmetleri sağlayan kurumların ağ iletişimlerinde ortaya çıkabilecek olan sorunlarda ilgili dış hizmet sağlayıcıya sorun bildirim yapılacaktır.
- Dış hizmet sağlayıcı kurumun hizmet sözleşmelerinde tanımlı olan devamlılık taahhütleri incelenecek ve oluşan sorunun devamlılık taahhütleri dahilinde kaldığı doğrulanacaktır. Devamlılık taahhüdü dahilinde bulunan sorunlarda ;
 - İlgili kurumun devamlılık taahhüdü doğrultusunda yapmış olduğu ağ bağlantı yedekleme altyapısının devreye alınıp alınmadığı kontrol edilecektir.
 - Sorun giderim süre taahhütlerinin geçerliliği sorun giderim süresi içinde göz önünde bulundurulacaktır.
 - Ağ bağlantısı amacıyla dış hizmet sağlayıcı tarafından sağlanan cihazların etkinliği analiz edilecek ve sorun kaynağı olan cihazlarda;
 - § Yazılımsal veya yapılandırmadan kaynaklanan sorunların dış hizmet sağlayıcı tarafından çözülmesi istenecektir.
 - § Donanımsal sorunlarda dış hizmet sağlayıcının sözleşme taahhütleri dahilinde ilgili ağ cihazını değiştirmesi talep edilecektir.
- Devamlılık taahhüdü bulunmayan ağ altyapısı sorunlarında dış hizmet sağlayıcının sağladığı bağlantının sorunlu bölümü dış hizmet sağlayıcı ile eş güdümlü analizler ile tespit edilecek ve çözülecektir.
- Kablolama altyapısının değişmesi gereken durumlarda ilgili dış hizmet sağlayıcıya sorun bildirim yapılır ve kablolama değişim süre bilgisi talep edilir.
- Bağlantı amaçlı kullanılan ağ cihazlarından kaynaklanan sorunlarda dış ürün sağlayıcı kurum ile irtibata geçilerek ağ cihazının donanımsal ve yazılımsal sorunlarının giderilmesi talep edilir ve sorun giderim süresi istenir.
- Uzak alan ağ bağlantılarında kesinti oluşması durumunda, uzak alan ağının yedeği olarak kullanılan ağ altyapısının devreye alınması ilgili dış hizmet sağlayıcıdan talep edilir. Eğer yedek ağ altyapısı aynı dış hizmet sağlayıcı tarafından sunulmuyor ve farklı bir hizmet sağlayıcıdan hizmet alınıyor ise irtibata geçilerek yedek bağlantı devreye alınır.

9.2 Sunucu Servis Sağlayıcıları Hizmet Sorun Planı

Sunucular ile ilgili hizmetlerin alındığı dış hizmet sağlayıcılarının hizmetlerinde saptanan sorunlar için aşağıda tanımlanan yönergeler izlenecektir;

- Sunucu hizmetleri sağlayan kurumların hizmetlerinde ortaya çıkabilecek olan sorunlarda ilgili dış hizmet sağlayıcıya sorun bildirim yapılacaktır.

- Dış hizmet sağlayıcı kurumun hizmet sözleşmelerinde tanımlı olan devamlılık taahhütleri incelenecek ve oluşan sorunun devamlılık taahhütleri dahilinde kaldığı doğrulanacaktır. Devamlılık taahhüdü dahilinde bulunan sorunlarda ;
 - İlgili kurumun devamlılık taahhüdü doğrultusunda yapmış olduğu sunucu yedekleme altyapısının devreye alınıp alınmadığı kontrol edilecektir.
 - Sorun giderim süre taahhütlerinin geçerliliği sorun giderim süresi içinde göz önünde bulundurulacaktır.
 - Sunucuda oluşan donanımsal sorunların giderimi için ilgili donanımın değiştirilmesi talep edilecektir.
 - Sunucuda oluşan yazılımsal sorunların giderimi için soruna bağlı olarak yama yükleme, yapılandırma yükleme veya işletim sistemi yükleme hizmetleri talep edilecektir.
 - Kümelenmiş sunucularda dış ürün sağlayıcısının hizmet sınırları dahilinde kümeleme bozulmadan sorun gideriminin sağlanması talep edilecektir.
- Devamlılık taahhüdü bulunmayan donanımsal sunucu sorunlarında dış ürün sağlayıcı ile irtibata geçilecek ve ilgili donanımın değişimi ürün değişim taahhütleri doğrultusunda talep edilecektir.
- Devamlılık taahhüdü bulunmayan yazılımsal sunucu sorunlarında dış ürün sağlayıcı ile irtibata geçilecek, sunucunun yazılımsal sorunlarının giderilmesi ve ilgili yüklemelerin yapılması talep edilecektir.

9.3 İletişim Servis Sağlayıcıları Hizmet Sorun Planı

İletişim altyapısı ile ilgili hizmetlerin alındığı dış hizmet sağlayıcılarının hizmetlerinde saptanan sorunlar için aşağıda tanımlanan yönergeler izlenecektir;

- Uzak veya kurum içi iletişim bağlantısı hizmetleri sağlayan kurumların iletişim altyapısında ortaya çıkabilecek olan sorunlarda ilgili dış hizmet sağlayıcıya sorun bildirimini yapılacaktır.
- Dış hizmet sağlayıcı kurumun hizmet sözleşmelerinde tanımlı olan devamlılık taahhütleri incelenecek ve oluşan sorunun devamlılık taahhütleri dahilinde kaldığı doğrulanacaktır. Devamlılık taahhüdü dahilinde bulunan sorunlarda ;
 - İlgili kurumun devamlılık taahhüdü doğrultusunda yapmış olduğu iletişim bağlantı yedekleme altyapısının devreye alınıp alınmadığı kontrol edilecektir.
 - Sorun giderim süre taahhütlerinin geçerliliği sorun giderim süresi içinde göz önünde bulundurulacaktır.
 - İletişim bağlantısı amacıyla dış hizmet sağlayıcı tarafından sağlanan cihazların etkinliği analiz edilecek ve sorun kaynağı olan cihazlarda;
 - § Yazılımsal veya yapılandırmadan kaynaklanan sorunların dış hizmet sağlayıcı tarafından çözülmesi istenecektir.
 - § Donanımsal sorunlarda dış hizmet sağlayıcının sözleşme taahhütleri dahilinde ilgili ağ cihazını değiştirmesi talep edilecektir.
- Devamlılık taahhüdü bulunmayan iletişim altyapısı sorunlarında dış hizmet sağlayıcının sağladığı bağlantının sorunlu bölümü dış hizmet sağlayıcı ile eş güdümlü analizler ile edilecek ve çözülecektir.
- Kablolama altyapısının değişmesi gereken durumlarda ilgili dış hizmet sağlayıcıya sorun bildirimini yapılır ve kablolama değişim süre bilgisi talep edilir.
- Bağlantı amaçlı kullanılan iletişim cihazlarından kaynaklanan sorunlarda dış ürün sağlayıcı kurum ile irtibata geçilerek iletişim cihazının donanımsal ve yazılımsal sorunlarının giderilmesi talep edilir ve sorun giderim süresi istenir.

- Uzak alan ağ bağlantılarında kesinti oluşması durumunda, uzak alan ağının yedeği olarak kullanılan iletişim altyapısının devreye alınması ilgili dış hizmet sağlayıcıdan talep edilir. Eğer yedek iletişim altyapısı aynı dış hizmet sağlayıcı tarafından sunulmuyor ve farklı bir hizmet sağlayıcıdan hizmet alınıyor ise irtibata geçilerek yedek bağlantı devreye alınır.

9.4 Veri Yayını Sağlayıcıları Hizmet Sorun Planı

Veri yayını ile ilgili hizmetlerin alındığı dış hizmet sağlayıcılarının hizmetlerinde saptanan sorunlar için aşağıda tanımlanan yönergeler izlenecektir;

- Veri yayını hizmetleri sağlayan kurumların veri iletim altyapısında ve veri içeriğinde ortaya çıkabilecek olan sorunlarda ilgili dış hizmet sağlayıcıya sorun bildirimi yapılacaktır.
- Dış hizmet sağlayıcı kurumun hizmet sözleşmelerinde tanımlı olan devamlılık taahhütleri incelenecek ve oluşan sorunun devamlılık taahhütleri dahilinde kaldığı doğrulanacaktır. Devamlılık taahhüdü dahilinde bulunan sorunlarda ;
 - İlgili kurumun devamlılık taahhüdü doğrultusunda yapmış olduğu veri iletimi yedekleme altyapısının devreye alınıp alınmadığı kontrol edilecektir.
 - Sorun giderim süre taahhütlerinin geçerliliği sorun giderim süresi içinde göz önünde bulundurulacaktır.
 - Veri iletim bağlantısı amacıyla dış hizmet sağlayıcı tarafından sağlanan cihazların etkinliği analiz edilecek ve sorun kaynağı olan cihazlarda;
 - § Yazılımsal veya yapılandırmadan kaynaklanan sorunların dış hizmet sağlayıcı tarafından çözülmesi istenecektir.
 - § Donanımsal sorunlarda dış hizmet sağlayıcının sözleşme taahhütleri dahilinde ilgili veri iletim cihazını değiştirmesi talep edilecektir.
- Devamlılık taahhüdü bulunmayan veri iletim altyapısı sorunlarında dış hizmet sağlayıcının sağladığı bağlantının sorunlu bölümü dış hizmet sağlayıcı ile eş güdümlü analizler ile tespit edilecek ve çözülecektir.
- Veri iletim altyapısının değişmesi gereken durumlarda ilgili dış hizmet sağlayıcıya sorun bildirimi yapılır ve kablolama değişim süre bilgisi talep edilir.
- Bağlantı amaçlı kullanılan veri iletim cihazlarından kaynaklanan sorunlarda dış ürün sağlayıcı kurum ile irtibata geçilerek veri iletim cihazının donanımsal ve yazılımsal sorunlarının giderilmesi talep edilir ve sorun giderim süresi istenir.
- Uzak alan ağ bağlantılarında kesinti oluşması durumunda, uzak alan ağının yedeği olarak kullanılan veri iletim altyapısının devreye alınması ilgili dış hizmet sağlayıcıdan talep edilir. Eğer yedek veri iletim altyapısı aynı dış hizmet sağlayıcı tarafından sunulmuyor ve farklı bir hizmet sağlayıcıdan hizmet alınıyor ise irtibata geçilerek yedek bağlantı devreye alınır.
- Veri yayını içeriğinde meydana gelen değişimden kaynaklanan sorunlarda dış hizmet sağlayıcı ile irtibata geçerek yayının iletimi için kullanılan cihaz ve yazılımlarda gerekli değişimlerin yapılması talep edilecek ve çözülecektir.

10 Bilgi Sistemleri Güvenliği

Türkiye Şişe Cam Fabrikaları A.Ş. Bilgisayar Destek Hizmet Müdürlüğü ve Enformasyon Teknolojileri Müdürlüğünce tanımlanmış prosedürler dahilinde yürütülecektir