

Doküman Kodu: BGYS-0010

VERİ YEDEKLEME KILAVUZU

SÜRÜM 1.00

24.1.2008

Hazırlayan: Ali Dinçkan

ÖNSÖZ

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nin misyonu, "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile, bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulaşılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuvarlarında temel ve uygulamalı araştırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sağlanmaktadır.

Bu doküman, BGYS (Bilgi Güvenliği Yönetim Sistemi) kurmak isteyen kurumlar için yardımcı kaynak olarak hazırlanmıştır. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

Bu dokümanda anlatılanlar tamamen tavsiye niteliğindedir. UEKAE, yapılan uygulamalardan doğabilecek zararlardan sorumlu değildir. Bu doküman UEKAE'nin izni olmadan değiştirilemez.

BİLGİLENDİRME

Bu dokümanın oluşturulmasında emeđi geen Ađ Güvenliđi personeline ve dokümanı gözden geirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Dođan Eskiyörük'e teşekkürü bor biliriz.

İÇİNDEKİLER

1. GİRİŞ	5
1.1 Amaç ve Kapsam.....	5
1.2 Kısaltmalar.....	5
2. VERİ YEDEKLEMESİ	6
3. YEDEKLEME KAVRAMLARI VE TEKNOLOJİLERİ.....	6
3.1 Veri Yedekleme Türleri.....	6
3.2 Yedekleme Altyapısı	8
3.3 Veri Yedekleme Yöntemleri.....	9
3.3.1 Tek Sunucu Yedekleme	10
3.3.2 Merkezi Yedekleme	10
3.3.2.1 Yerel Alan Ağı Üzerinden Merkezi Yedekleme	10
3.3.2.2 Depolama Alan Ağı Üzerinden Merkezi Yedekleme	11
3.4 Veri Yedekleme Sıklığının Belirlenmesi.....	12
3.5 Veri Koruma Zamanının Belirlenmesi	13
3.6 Yedekleme Medyalarının Yönetimi	13
3.7 Yedekleme Medyalarının Güvenliği.....	14
3.8 Yedekleme Testi	15
4. YEDEKLEME POLİTİKASI	16
5. YEDEKLEME PLANI	17
6. YEDEKLEME SİSTEMİ DENETİMİ.....	20
KAYNAKÇA	23

1. GİRİŞ

Bilgi, bir kurumun önemli varlıkları arasındadır. Herhangi bir nedenle kullanılamaz duruma gelmesi bilginin kritikliği derecesinde kuruma zarar verir. Bu sebeple bilgi sınıflandırılmalı ve kaybı durumunda tekrar elde edilmesi için gereken planlama yapılmalıdır. Bu rehberde yedekleme kavramları ve teknolojileri tanıtılacak, sonrasında yedekleme politikası ve planı üzerine tavsiyeler sunulacaktır.

1.1 Amaç ve Kapsam

Veri yedeklemesinin önemini vurgulamak, hali hazırda yedekleme sistemi olan veya kurmak isteyen kurumlara konu ile ilgili olarak yön göstermek amacıyla hazırlanmıştır. Doküman boyunca sadece veri yedeklemesi dikkate alınmıştır. Ekipman yedeklemesi, personel yedeklemesi gibi konular rehber içerisinde dikkate alınmamıştır.

1.2 Kısaltmalar

AIT	: Advanced Intelligent Tape
BGYS	: Bilgi Güvenliği Yönetim Sistemi
BT	: Bilgi Teknolojileri
DAT	: Digital Audio Tape
DLT	: Digital Linear Tape
LTO	: Linear Tape Open
SAN	: Storage Area Network – Depolama Alan Ağı
SDLT	: Super Digital Linear Tape
UEKAE	: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

2. VERİ YEDEKLEMESİ

Depolanan verinin herhangi bir nedenle zarar görmesi kurum süreçlerinde ciddi zararlara neden olabilmektedir. Felaket durumu sonrasında kurum verisinin geri yüklenememesi kurumun ticari faaliyetine son vermesine neden olabilecek kadar ciddi sonuçlar doğurabilmektedir. Depolanan verinin her geçen gün arttığı ve verinin kurum süreçleri için daha kritik bir rol oynadığı günümüzde verinin yedeklenmemesi büyük risk oluşturmaktadır. Bu sebeple kurumlarda yedekleme sistemleri kurulmakta ve yedekleme işleri günlük olarak takip edilmektedir. Yedekleme sisteminin kurulumu yedeklenecek veri miktarı, yedekleme sıklığı, yedeklenen verinin zaman içerisinde değişme oranı, kabul edilebilir maksimum veri kaybı gibi parametrelere bağlıdır.

Veri yedeklemesinin amacına uygun olarak gerçekleştirilebilmesi için düzenleyici ve yönetimin konuya bakış açısını yansıtan bir yedekleme politikasına ihtiyaç vardır. Yedekleme politikası kurum için yedeklemenin önemini ve en az yerine getirilmesi gerekenleri ifade etmelidir. Yedekleme politikasının yerine getirilmesi için detaylı bir analiz çalışması yapılmalı ve politikayı sağlayacak bir yedekleme planı ortaya koyulmalıdır. Yedekleme planının işletilmesi ve zaman içerisinde günün ihtiyaçlarına göre güncellenmesi veri kaybı durumunda kurumun göreceği zararı en aza indirecektir.

3. YEDEKLEME KAVRAMLARI VE TEKNOLOJİLERİ

Bu bölümde veri yedeklemesi ile ilgili temel kavramlar ve teknolojiler açıklanmaktadır. Bu bölümde yer alan teknik bilgiler yedekleme politikası ve planı için bilinmesi gereken kavramları içermektedir.

3.1 Veri Yedekleme Türleri

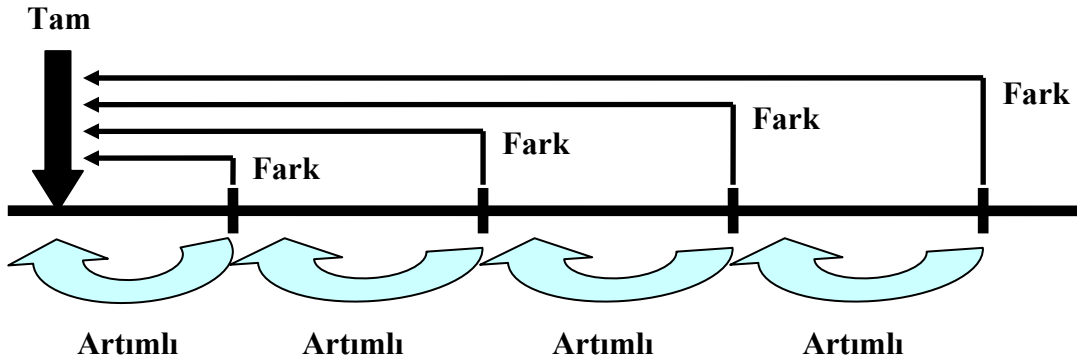
Veri yedekleme temel olarak tam yedekleme (full) , fark yedekleme(Differential) ve artan yedekleme (incremental) olmak üzere üçe ayrılmaktadır.

Tam yedekleme: Tam yedekleme, yedeği alınmak üzere seçilmiş bütün bilgilerin bir kopyasının yedekleme medyasına kaydedildiği bir yedekleme türüdür. Tam yedeklemede orijinal verinin birebir kopyası alındığı için yedekleme medyasında orijinal verinin boyutu kadar yer kaplamaktadır. Bu çalışma biçimi yedek alma süresini uzatmakta ve ihtiyaç duyulan yedekleme sıklığının sağlanmasını zorlaştırmaktadır. Yedekleme donanımının yetersiz olduğu, yedeklenecek veri boyutunun çok yüksek olduğu veya verinin sık yedeklenmesi

gereken ortamlarda yedekleme işlerinin tümünün tam yedek olarak belirlenmesi her zaman mümkün değildir. Diğer yandan, tam yedekleme bilginin geri döndürülme ihtiyacı ortaya çıktığında orijinal verinin tamamını içerdiğinden başka yedekleme işlerine ihtiyaç duymadan kullanılabilir bir yöntemdir. Tam yedekleme diğer bütün yedekleme türleri için bir başlangıç noktası olarak düşünülmelidir.

Fark yedekleme: Başarılı olarak sonlandırılmış en son tam yedeğe göre değişikliklerin yedeklenmesidir. Sadece en son alınan tam yedeğe göre farkın yedeklenmesi nedeni ile tam yedeklemeye göre daha hızlıdır ve yedekleme medyası üzerinde daha düşük alan işgal etmektedir. Fark yedeklemede her zaman en son tam yedeğe göre fark alındığı için yedeklenen veri miktarı sürekli artmaktadır. Belirli aralıklarla tam yedek alınması fark yedeklemesi sırasında yedeklenecek veri miktarını düşürmektedir. Verinin geri döndürülmesi gerektiğinde fark yedeğe ek olarak tam yedeğe de ihtiyaç vardır. Geri döndürme sırasında iki yedeğinde kullanılması nedeni ile tam yedeğe göre daha yavaş bir yedekleme türüdür.

Artan yedekleme: Başarılı olarak sonlandırılmış en son yedeğe göre değişen bilgilerin yedeklenmesidir. En son yedeğin tam, fark veya artan olmasının önemi yoktur. Sadece en son değişikliklerin yedeklenmesi nedeni ile yedekleme işinin tamamlanma süresi kısadır. Yedekten geri döndürme işlemi gerektiğinde tam yedek ve arada alınmış bütün artan yedeklere ihtiyaç vardır. Bu sebeple düşük geri döndürme hızına sahiptir. Ayrıca birçok yedekleme işinde alınan verilerden geri döndürme işi yaptığından geri döndürme başarısı diğer türlere göre düşüktür.



Şekil 1 – Yedekleme Türleri

Her yedekleme türünün avantaj ve dezavantajları vardır. Tam yedekleme türünün geri döndürme hızı çok yüksek iken yedekleme hızı düşüktür ve her yedekleme işi için orijinal veri alanı kadar yer ayırmak gerekmektedir. Bu sebeple yedekleme işlerinin tamamı için tam yedekleme yapmak her zaman tercih edilen bir yöntem değildir. Öbür yandan artan

yedekleme çok hızlı gerçekleştirilebilmesine rağmen verinin geri döndürülmesi sırasında çok sayıda yedekleme işinin çalıştırılmasına ihtiyaç duymaktadır. Bu tür nedenlerle yedekleme işlerinin gerçekleştirilmesi sırasında bu seçenekler genellikle beraber kullanılmaktadır. Hafta sonu tam yedek, hafta içi fark yedek ve mesai saatleri içerisinde artan yedek almak beraber kullanıma örnek olarak verilebilir. Yedekleme türlerinin geri döndürme hızı, yedekleme hızı ve depolama alanı kullanımı bakımından karşılaştırması **Error! Reference source not found.**'de verilmiştir.

Yedekleme Türü	Geri Döndürme Hızı	Yedekleme Hızı	Depolama Alanı Kullanımı
Tam	En yüksek	En düşük	En yüksek
Fark	Orta	Orta	Orta
Artımlı	En düşük	En yüksek	En düşük

Tablo 1 – Yedekleme Türlerinin Karşılaştırılması

3.2 Yedekleme Altyapısı

Günümüzde yedekleme amacıyla manyetik kaset (teyp) kullanımı geçerliliğini korumaktadır. Kullanılan teknolojinin türüne göre yazma/okuma hızı ve her kaset üzerine yazılabilecek veri miktarı değişiklik göstermektedir. Günümüzde en yaygın olarak kullanılan yedekleme teknolojileri LTO, SDLT, DAT, AIT ve DLT'dir. Her bir teknolojinin çeşitli türevleri bulunmaktadır. Yaygın olarak kullanılan LTO teknolojisinin son olarak dördüncü nesli çıkmıştır. İlk neslinde 100GB normal / 200GB sıkıştırılmış olan kartuş kapasitesi yeni nesilde 800GB normal / 1.6TB sıkıştırılmış kapasiteye ulaşmıştır. Yine ilk neslinde 40MB/sn olan sıkıştırılmış veri transfer hızı yeni nesilde 240MB/sn'lere ulaşmıştır.

Manyetik kaset kullanımında kartuş kapasitesi ve transfer hızı yüksek olmasına rağmen geri döndürme işleminde kaset sarma işlemi yapılmaktadır. Geri döndürme işleminin genellikle son veri üzerinden yapıldığı düşünülürse en son alınan yedeğin daha hızlı geri döndürmeye izin verecek disk sistemleri üzerinde bulunması zaman kazandıracaktır. Bu sebeple son yıllarda teyp ve disk tabanlı yedekleme çözümlerinin beraber kullanımı yaygınlaşmaya başlamıştır.

Her geçen gün yedeklenecek veri miktarının artması ve veri kaybı toleransının düşmesi nedenleri ile daha sık yedek alma gerekliliği ortaya çıkmıştır. Bu sebeple yedekleme altyapısı kurumlarda genellikle otomasyona geçirilmiştir. Yedekleme otomasyonu için yedeklemeyi merkezi olarak kontrol edecek bir yazılıma ve yedeklerin merkezi olarak alınması için bir teyp kütüphanesine ihtiyaç vardır. Teyp kütüphanesi daha küçük ortamlarda tek bir yedekleme sürücüsü veya az sayıda kartuş yuvası içeren daha ilkel otomatik teyp değiştiricileri olabilmektedir.

Yedekleme yazılımı yedekleme işlerinin yönetimi amacı ile kullanılmaktadır. Yedekleme yazılımı temel olarak aşağıda belirtilen fonksiyonları yerine getirir.

- ✓ Yedekleme işlerinin tanımlanması
- ✓ Yedekleme işlerinin zaman planına uygun olarak çalıştırılması
- ✓ Yedekleme donanımlarının (kütüphane ve kartuşlar) yönetimi
- ✓ Yedekleme donanımı ile ortak çalışarak yedeklerin alınması
- ✓ Gerçekleşmiş yedekleme işlerinin kaydının tutulması (Ne zaman, hangi verinin, hangi kartuşa yedeği alındığı bilgisi dahil olmak üzere)
- ✓ Yedekleme hataları ile uyarı bildirimini
- ✓ Yedekleme işleri ile ilgili rapor üretme
- ✓ İstenildiğinde yedeği alınmış verinin geri döndürme işleminin gerçekleştirilmesi

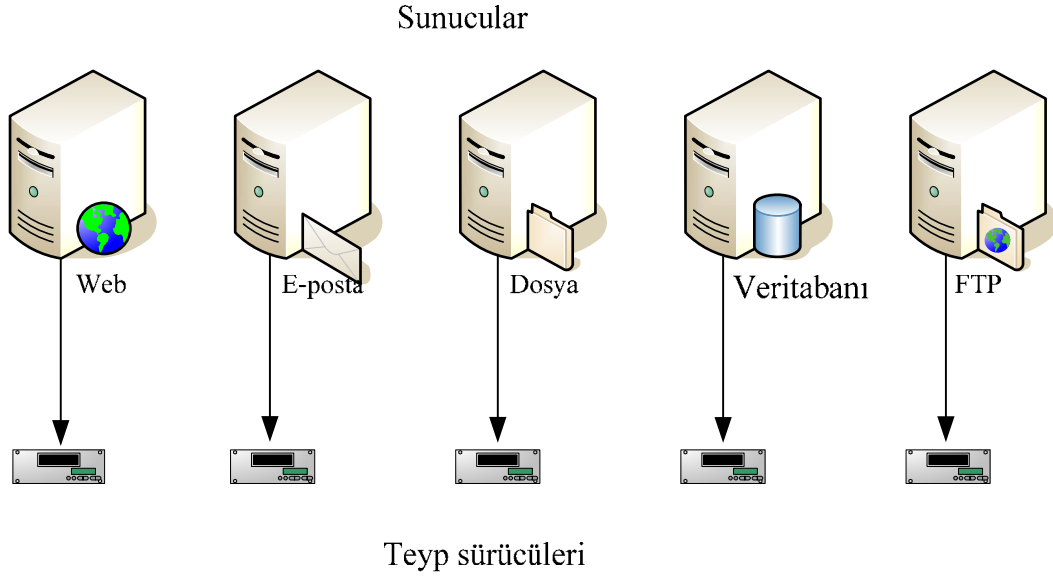
Teyp kütüphanesi teyp sürücülerini, kartuş yuvaları ve robot kol olmak üzere üç parçaya ayrılmaktadır. Teyp sürücülerini yedekleme kartuşlarına veri yazma veya kartuş üzerinde bulunan verinin okunması amacıyla kullanılmaktadır. Kartuş yuvasına göre sayıca daha azdır. Bir teyp kütüphanesinin içerisinde kütüphanenin büyüklüğüne göre bir ila kırk adet teyp sürücüsü bulunabilmektedir. Kartuş yuvaları ise sekiz yuvadan başlayarak binlerce yuvaya kadar çıkabilmektedir. Robot kol, kartuş yuvaları ile teyp sürücülerini arasında kartuş taşımak amacı ile kullanılmaktadır. Bu sayede operatöre ihtiyaç duyulmadan yedekleme işlemleri gerçekleştirilebilmektedir.

3.3 Veri Yedekleme Yöntemleri

Veri yedekleme yöntemleri tek sunucu ve merkezi yedekleme olarak temel iki kategoriye ayrılmaktadır.

3.3.1 Tek Sunucu Yedekleme

Bu yedekleme yönteminde her sunucunun ayrı ayrı yedeği alınmaktadır. Sunucular üzerinde bulunan veri yine sunucular üzerinde bulunan yedekleme sürücülerini vasıtasıyla yedeklenmektedir. Sunucular üzerinde genellikle DAT, AIT veya DVD yazıcı bulunmaktadır. Yedekleme işlerinin takibi ve yedekleme işlerinde kullanılan yedekleme medyalarının yönetimi zordur. Sunucuların ayrı ayrı yedeklenmesi sunucu sayısı fazla olan ortamlarda uygulanması zor bir yöntemdir. Bu sebeplerle veri merkezlerinde sık karşılaşılmayan bir yedekleme yöntemidir. Bazı sunuculara tek düğmeye basarak işletim sistemi kurtarma özelliğinden faydalanabilmek için kullanılmaktadır.



Şekil 2 – Tek Sunucu Yedekleme

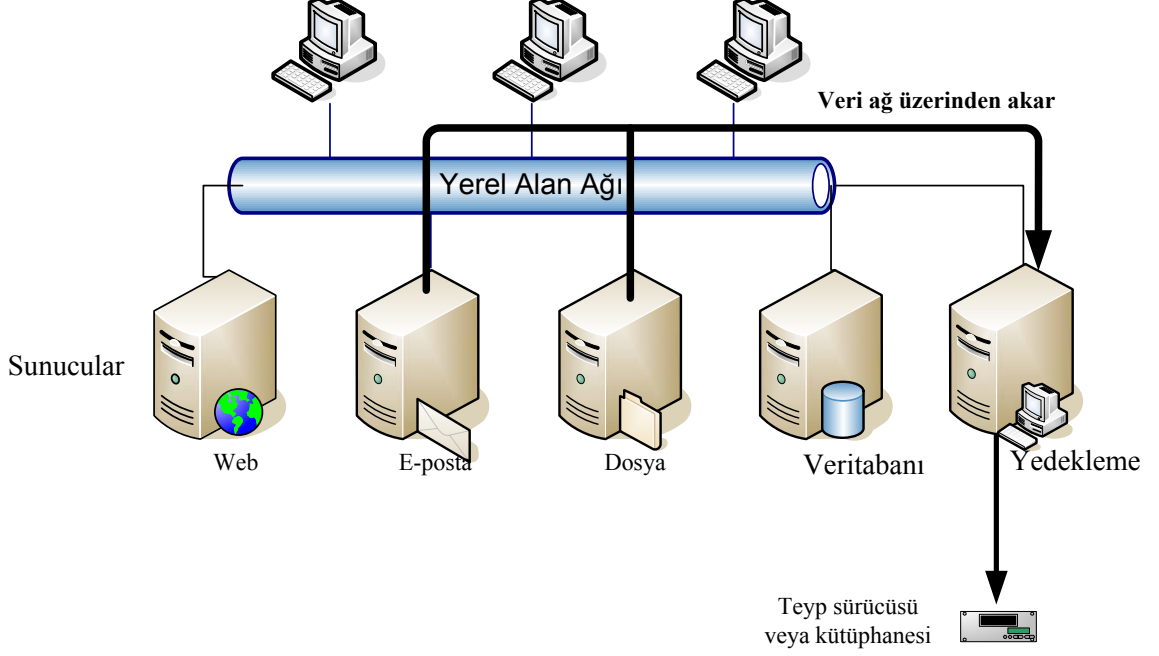
3.3.2 Merkezi Yedekleme

Merkezi yedekleme yerel alan ağı ve depolama alan ağı üzerinden yedekleme olarak iki başlık altında incelenecektir.

3.3.2.1 Yerel Alan Ağı Üzerinden Merkezi Yedekleme

Yerel alan ağı (LAN) üzerinden merkezi yedekleme altyapısı Şekil 3’de görünmektedir. Bu yapıda teyp kütüphanesi bir yedekleme sunucusuna bağlıdır. Yedekleme sunucusu üzerinde yedekleme yazılımı kuruludur ve yedekleme işlerinin merkezi olarak yönetimini gerçekleştirir. Yedekleme yazılımları genellikle ajan tabanlı çalışır. Yedeği alınacak sunucular üzerine kurulan küçük uygulama parçaları ile veri ağı üzerinden yedekleme

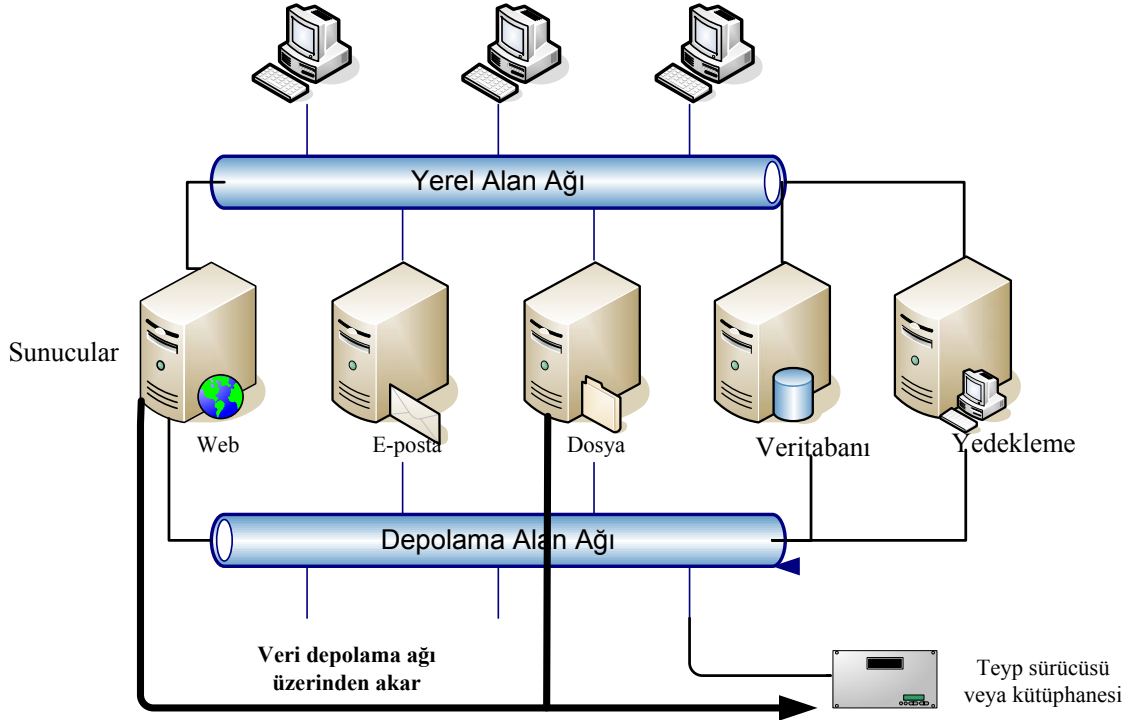
sunucusuna ve oradan da teyp kütüphanesinde bulunan yedekleme kartuşlarına yazılır. Bu tür bir yapıda verinin tamamı bilgisayar haberleşmesi için de kullanılan yerel alan ağından (LAN) akmaktadır. Yüksek miktarlarda veri yedeklemesi yapılmak istendiğinde yerel alan ağını yoran bir yedekleme türüdür.



Şekil 3 – Yerel Alan Ağı Üzerinden Merkezi Yedekleme

3.3.2.2 Depolama Alan Ağı Üzerinden Merkezi Yedekleme

Kurumsal yedekleme alt yapısı depolama alan ağı (SAN) ismi verilen bir ağ üzerinden gerçekleştirilmektedir. Depolama alan ağı yüksek miktarlarda veri depolama kapasitesine ihtiyaç duyan ve ölçeklenebilirlik gereken ortamlarda kullanılmaktadır. Bu yapıda teyp kütüphanesi de depolama alan ağına bağlanmaktadır. Yedekleme sunucusu dâhil olmak üzere ağda bulunan bütün sunucular teyp kütüphanesi ile haberleşebilmektedir. Yedekleme sunucusunun görevi klasik yedekleme altyapısında olduğu gibi yedekleme işlerinin yönetimidir. Bir yedekleme işinin başlaması için ajanlar ile gereken haberleşmeyi yapar. Veri yedeği alınan sunucu üzerinden teyp kütüphanesinde bulunan bir sürücüye akar ve sürücü içerisinde bulunan kartuşa yazma işlemi gerçekleştirilir. Yazma işinin başlamadan önce ilgili kartuşun sürücü içerisine yerleştirilmesi, yedekleme sonrasında ilgili yuvaya geri çıkartılması, yedekleme sırasında ortaya çıkabilecek hataların yönetimi işlerini yedekleme yazılımı gerçekleştirir.



Şekil 4 – Depolama Alan Ağı Üzerinden Yedekleme

3.4 Veri Yedekleme Sıklığının Belirlenmesi

Veri yedekleme sıklığı, kurum verisi için belirlenmesi gereken kabul edilebilir veri kaybı süresi ile ilgilidir. Söz konusu süre uygulamadan uygulamaya değişebilmektedir. Bir dosya sunucu için kabul edilebilir veri kaybı süresi bir gün ve hatta bir hafta olabilirken, veritabanı için bir saat ve belki daha kısa olabilmektedir. Yedeği alınacak veriler için kabul edilebilir veri kaybı süresi göz önüne alınarak kategoriler oluşturulmalıdır.

Kategori için örnek: Çok yüksek (<1 saat), yüksek (< 4 saat), orta (< 1 gün), düşük (< 1 hafta), çok düşük (< 1 ay)

Yedeği alınacak verilerin belirlenmesinin ardından veri kategorilere ayrılmalıdır. Verinin kategorilere ayrılması sunucu bazında yapılmak zorunda değildir. Dosya sunucu üzerinde bulunan kurumsal ve şahsi veriler için farklı zamanlar belirlenebilir. Aynı şekilde bir veritabanı sunucusunda bulunan farklı veritabanları için kabul edilebilir veri kaybı süreleri farklı belirlenebilir. Yedekleme işleri en az kabul edilebilir veri kaybı süresini karşılayacak biçimde oluşturulmalıdır. Kabul edilebilir veri kaybı süresinin aşılması esastır. Kabul edilebilir veri kaybı süresinin bir gün olması söz konusu verinin yedeğinin günde bir defa alınması gerektiği anlamına gelmemektedir. Sürenin bir gün olarak belirlenmesinden her gün en az bir defa yedekleme yapılması gerektiği anlamı çıkartılmalıdır.

Yedeklenecek veri miktarının zaman içerisinde artması nedeni ile mevcut yedekleme sistemi yetersiz kalabilmektedir. Bu sorun günümüz yedekleme sistemlerinde sık karşılaşılan bir sorundur. Bu tür durumların önüne geçebilmek için yedeklenen veri miktarı izlenmeli ve yedekleme donanımı yatırımı planlanmalıdır. Aksi takdirde veri için ön görülen kabul edilebilir veri kaybı süresinin aşılması söz konusudur.

3.5 Veri Koruma Zamanının Belirlenmesi

Verinin zarar görmesi durumunda son alınan yedeğin geri döndürülmesi en çok karşılaşılan geri döndürme türüdür. Fakat bazı durumlarda verinin eski halinin geri döndürülme ihtiyacı oluşmaktadır. Bir dosyanın açıldıktan sonra farklı kaydet yerine kaydet butonuna basılarak asıl dosyanın üzerine yazılması bu duruma örnek olarak verilebilir. Ayrıca verinin herhangi bir zamandaki hali çeşitli (hukuki vb) nedenlerle gerekebilir. Ülkemizde bankalar, internet servis sağlayıcılar ve daha bir çok sektör için belirli sürelerde kayıt saklama zorunluluğu getirilmiştir. Veri koruma zamanının belirlenmesinde iş ihtiyaçları göz önüne alındığı gibi hukuki yaptırımlarda dikkate alınmalıdır.

Alınan yedeğin kalıcı olarak saklanması yedek alınan medyanın tamamı kullanıldıktan sonra tekrar kullanılamaması anlamına gelmektedir. Bu durum sürekli olarak yedekleme medyası yatırımı gerektiren bir durum olduğu için her zaman uygulanabilir değildir. Yedekleme medyalarının tekrar kullanılabilmesi için veri koruma zamanının belirlenmesi gereklidir. Yedeği alınan verinin, yedekleme medyası üzerinde ne kadar süre üzerine yazmaya karşı korumalı olarak saklanacağı veri koruma zamanı parametresi ile belirlenmektedir. Bu değer alınan yedeklerin geri döndürme ihtiyaçlarına göre değişmektedir. Örneğin günlük olarak alınan yedeklerin son bir ay içerisinde gün bazında geri döndürülmesi, daha eskilerinin haftalık bazda geri döndürülmesi, 3 aydan eski verinin aylık bazda geri döndürülmesi gibi bir tanımlama yapılması söz konusudur.

3.6 Yedekleme Medyalarının Yönetimi

Yedekleme işlemleri sırasında çok sayıda yedekleme medyası kullanılmaktadır. Yedekleme medyalarının yönetiminin yedekleme yazılımı tarafından yapılması günümüzde en yaygın kullanılan tekniktir. Yedekleme yazılımı veri yedeklemesi sırasında kullanılan medyalara ait kayıtları tutmaktadır. Herhangi bir zamanda, verinin geri döndürülme ihtiyacı olduğunda yedekleme yazılımı ihtiyaç duyulan medyayı tuttuğu kayıtlardan öğrenmekte ve yedekleme işletmenine bildirmektedir. Teyp kütüphanesi kullanılması durumunda otomatik olarak sürücüyü yüklemekte ve geri döndürme işini başlatmaktadır. Söz konusu kayıtların el ile

tutulması da mümkündür. Öbür yandan sürekli olarak yedek alınmasından dolayı yedekleme kayıtları her gün artmaktadır. Ayrıca veri koruma zamanı dolan medyaların tekrar kullanıma alınması gibi işlemlerin gerçekleştirilmesi takip gerektirir. Oluşturulan kayıtların yönetiminin zor olmasından dolayı bu işlemler için genellikle yönetim yazılımı kullanılmaktadır.

Yedekleme yazılımları kullandıkları yedekleme medyalarına tanımlayıcı bir numara atamaktadır ve medya içerisine tanımlayıcı numarayı kaydetmektedir. Bu numaralar kullanarak medya takibi yapmak oldukça zordur. Bu sebeple yedekleme medyalarında barkot numarası kullanımı yaygınlaşmıştır. Bugün yedekleme altyapılarının otomasyonu için kullandığımız teyp kütüphanelerinin çoğu barkot okuma desteği sunmaktadır. Kütüphane içerisinde bulunan barkot okuyucu, yedekleme medyalarının bir yüzüne yapıştırılmış barkot numarasını okumakta ve medyanın takibi bu numara ile yapılmaktadır. Bu sayede yedekleme yazılımı teyp kütüphanesinde bulunmayan bir yedekleme medyasını barkot numarasını bildirerek isteyebilmektedir.

Yedekleme medyalarının sürekli olarak teyp kütüphanesi veya yedekleme sürücüsü içerisinde bulunması boş yuva sayısının kullanılan medya sayısına göre az olmasından dolayı zordur. Ayrıca yedekleme yapılan ortamda çıkabilecek yangın, sel gibi fiziksel bir etki durumunda verinin tamamının kullanılmaz duruma gelmesi durumu söz konusudur. Bu tür sebeplerle yedekleme medyasının belirli aralıklarla teyp kütüphanesinden alınarak fiziksel olarak güvenli bir ortamda saklanması gereklidir.

Bir diğer önemli konu yedekleme medyalarının ömrüdür. Alınan yedeklerden ihtiyaç durumunda geri döndürme işlemi yapabilmek için mutlaka takip edilmesi gereken bir konudur. Yedekleme medyalarının ömrü medyanın kullanım sayısı, depolanma ortamı ve üretim tarihi gibi parametrelere bağlıdır. Yedekleme sisteminde kullanılan yedekleme medyaları için bir kullanım ömrü belirlenmelidir. Yedekleme medyasının ömrü, 250 defa üzerine yazma işlemi yapılmış veya üretim tarihi 5 yıldan eski yedekleme medyaları ömrünü tamamlamıştır şeklinde tanımlanabilir. Verilen sayılar örnek olarak verilmiştir. Sayının belirlenmesi için medya üreticisine danışılmalıdır.

3.7 Yedekleme Medyalarının Güvenliği

Bilginin gizliliği göz önüne alındığında yedekleme medyaları üzerinde bulunan veri, canlı verinin bulunduğu sistemler kadar öneme sahiptir. Bu sebeple yedekleme medyalarının güvenliği üzerine kontroller oluşturulmalı ve uygulanmalıdır. Genellikle canlı verinin bulunduğu ortamın güvenliği sağlanırken yedekleme medyaların güvenliği ihmal

edilmektedir. Yedekleme medyalarının kolay elde edilebilecek yerlerde bulunması, medyanın bir ortamdan başka bir ortama aktarılması sırasında güvenliğin ihmal edilmesi kurum verisinin gizliliğine zarar verebilecek açıklıklardandır.

Yedekleme medyaları canlı veri zarar gördüğünde kullanılmaktadır. Yedekleme medyalarının tamamının canlı veri ile aynı fiziksel ortamda bulunması hem canlı verinin hem yedeğinin aynı zamanda zarar görmesine neden olabilmektedir. Bu sebeple yedekleme medyalarının sistem odası ile aynı etkiye maruz kalmayacak kadar uzak bir mesafede saklanması gereklidir. Sistem odası dışarısında saklanacak yedekleme medyalarının neler olduğu ve hangi aralıklarla aktarımının gerçekleştirileceği planlanmalıdır. Yedekleme medyalarının gerek sistem odası içerisinde yerel olarak gerek uzakta depolanması sırasında güvenli olarak saklanması sağlanmalıdır.

Yedekleme medyalarının uzak mesafe depolanması sırasında medya aktarımının güvenliği dikkate alınmalıdır. Uzak ortama gönderilen yedekleme medyalarına yazılan verinin şifreli olması, aktarımın kilitli ve dayanıklı kasa içerisinde gerçekleştirilmesi, kasanın teslim alınması ve karşı tarafa teslim edilmesinin tutanak ile sağlaması ve aktarımı gerçekleştiren personel veya firma ile gizlilik anlaşması yapılması uygulanabilecek kontroller arasındadır.

Yedekleme medyalarının güvenliği konusundaki bir hususta ömrünü tamamlayan medyaların imha edilmesidir. Kurum içerisinde veri taşıma ortamı imhası konusunda hazırlanmış bir prosedür veya talimat varsa yedekleme medyaları bu dokümanlara uygun biçimde imha edilmelidir. Eğer bu tür bir doküman yoksa ömrünü tamamlayan veya artık kullanılmayacak biçimde zarar gören medyaların imhası için bir yöntem geliştirilmeli ve bu yöntem yedekleme planında belirtilmelidir.

3.8 Yedekleme Testi

Yedekleme altyapısında çıkabilecek sorunların tamamı fark edilebilir değildir. Medya üzerine yazamama, ajanlara ulaşamama veya yedekleme sürücüsündeki fiziksel problemler yedekleme işlerinin tamamlanamamasına neden olabilir. Fakat başarılı olarak gerçekleşmiş yedekleme işi sonucunda oluşturulan yedekleme medyasının ihtiyaç durumunda kullanılabilmesinin veya alınmış olan yedeğin gerçekten istenilen yedek olduğunun garantisi yoktur. Yedekleme sürücüsündeki bir problem nedeni ile verinin okunamayacak biçimde yazılması veya yedekleme medyalarının depolandığı ortamdaki problemler nedeni ile medyaların bozulması karşılaşılabilecek durumlardır. Yedekleme alt yapısı ne kadar yeni ve güncel olursa olsun yedekleme testi yapılmadığı sürece geri döndürme işlemi risk altındadır.

Alınan yedeklerin niçin test edilmesi gerektiğine dair birkaç örnek aşağıda verilmiştir;

- ✓ Yedekleme işlemi sırasında verinin güvenilir biçimde medyaya yazıldığına garantisizdir. Geri döndürme işlemi sırasında yedekleme yazılımı verinin güvenilir olarak yedeklenmemesi nedeniyle hata verebilir. Bugün birçok yedekleme yazılımı yazma işlemini doğrulamak için seçenek sunmaktadır.
- ✓ Yedekleme işleri yedekleme yazılımında bir defa tanımlanır ve tanımlanmış zaman planına göre çalışmaya bırakılır. İş tanımlayan personelin yedeği alınacak verileri doğru seçtiğinin garantisizdir. Yedekleme işin tanımlanması aceleyle gelmiş olabilir veya herhangi bir zamanda daha önce tanımlanmış yedekleme işi değiştirilmiş olabilir. Bu tür durumların geri döndürme ihtiyacından önce fark edilebilmesi için gerekli önlemler alınmalıdır. Yedekten test amacıyla geri dönülmesi eksik yedek alındığının fark edilmesi için kullanılacak yöntemlerden birisidir.
- ✓ Alınan yedekler güvenli kasalarda saklanıyor olabilir. Fakat kasada bulunan medyaların etrafına medyalara zarar verebilecek cisimlerin yerleştirilmeyeceğinin veya medyaların kasanın bulunduğu ortamdan etkilenmeyeceğinin garantisizdir. Medyaların test edilmesi ile depolama ortamı problemleri tespit edilebilir.
- ✓ Veri, yedekleme medyalarına şifreli olarak yazılabilir. Eğer geri döndürme testi yapılmazsa şifreyi açabilmek için gerekli olan bilgilerin bilinmediğinin farkına varılmayabilir. Yedekleme yazılımının kurulduğu zaman bir parola verilmesi ve aradan zaman geçmesi nedeni ile parolanın unutulmuş olması söz konusudur.
- ✓ Yedekleme yazılımının güncellenmesi sonrasında eski medyaların okunamaması durumu oluşabilir. Yazılım üreticisi tarafından eski sürüm ile uyumlu olduğu iddia edilse bile bu tür durumlar oluşabilir. Yazılımın eski sürümü ile alınmış yedeklerin yeni sürüm ile geri döndürülmesi gerçekleştirilmediği sürece oluşabilecek problemler gözlenemez.

4. YEDEKLEME POLİTİKASI

Veri yedeklemesi kurumun kritik BT işlemlerinden birisidir. Kurum politikasında yedekleme konusu mutlaka yer almalı ve veri yedeklemesi için yönetim prensiplerini ortaya koyan bir politika bulunmalıdır. Kurum verisinin yedekleme işlemleri yedekleme politikasına göre yerine getirilmelidir.

Yedekleme politikasında kullanılabilir örnek ifadeler aşağıda sıralanmıştır;

- ✓ Kurumun bütün verisinin, kurum çapında kullanılan işletim sistemlerinin ve uygulamaların tamamının yedeği uygun ve düzenli olarak alınır.
- ✓ Yedekleme sistemi iş sürekliliği planında yer alan veri yedekleme ihtiyacını karşılayacaktır.
- ✓ Yedeği alınacak veri ve uygulamalar için sınıflandırma yapılır ve her bir sınıf için kabul edilir veri kaybı süresi belirlenir.
- ✓ Kabul edilir veri kaybı süresi yönetim tarafından onaylanır.
- ✓ Yedekleme işlemlerinin sağlanması için yedekleme politikasına uygun olarak bir yedekleme planı oluşturulur.
- ✓ Yedekleme işlerine ait kayıtlar tutulur.
- ✓ Başarısız olan yedekleme işleri takip edilir ve yedeği alınamamış verinin yedeği alınır.
- ✓ Yedekleme medyaları etiketlenir ve hangi medyada hangi yedeğin bulunduğu dair kayıtlar tutulur.
- ✓ Yedekleme medyalarının kopyaları alınarak ana sistem odasına zarar verebilecek felaketlerden etkilenmeyecek kadar uzakta ve güvenli olarak depolanır.
- ✓ Yedeklenmiş verinin düzenli aralıklarla geri döndürme testi yapılır.
- ✓ Yedekleme altyapısı, yedekleme ve geri döndürme işlemleri için talimatlar hazırlanır.
- ✓ Yedekleme politikasının uygulanması ve yenilenmesinden ... sorumludur.

5. YEDEKLEME PLANI

Yedekleme planı detaylı bir analiz çalışması sonrasında ve kurum yedekleme politikasına uygun olarak geliştirilmelidir. Yedeği alınacak kurum verisi belirlenmeli, sınıflandırılmalı ve verinin sahibinden alınan bilgiler ışığında kabul edilebilir veri kaybı süreleri hesaplanmalıdır. Yedekleme altyapısının en az bu süreleri karşılayacak biçimde kurulması gerekmektedir. Eğer var olan bir yedekleme altyapısı kullanılıyorsa kabul edilebilir veri kaybı sürelerinin karşılanıp karşılanamayacağı belirlenmeli ve gerekiyorsa yeni yatırım talebinde bulunulmalıdır. Yedekleme planı içerisinde en az, yedeklenen verilere ait bilgiler, yedekleme işleri, yedekleme sıklığı ve türü, yedekleme medyalarının yönetimi bulunmalıdır. Aşağıda yedekleme planı içerisinde bulunması tavsiye edilen bilgiler sunulmaktadır;

- ✓ **Yedekleme Sorumlulukları:** Yedekleme planının sahibi ve planı uygulamaktan sorumlu personel belirtilmelidir. Yedekleme planı, planın sahibi tarafından onaylanmalıdır. Planın sahibi yedekleme işlemlerinin politikaya uygun olarak gerçekleştirilmesinden, planın uygulama sorumlusu planda yazılı işlemlerin yerine getirilmesinden sorumludur.
- ✓ **Yedekleme işleri:** Yedekleme işlerinin detaylı bilgileri bulunmalıdır. Yedeği alınan veri, yedekleme türü ve yedekleme sıklığı detaylı olarak bulunmalıdır. Yedekleme işleri genellikle bir tabloda özetlenmektedir.
- ✓ **Veri koruma süreleri:** Yedekleme medyasında tutulan verinin, üzerine yazmaya karşı ne kadar süre korumalı olduğu belirtilmelidir. Bu süreler aynı zamanda yedekleme sisteminde uygulanmış olmalıdır.
- ✓ **Hataların izlenmesi ve yönetimi:** Hataları izleme yöntemi belirlenmelidir. Hata durumunda uyarı gönderilmesi, günlük olarak çalışan yedekleme işlerinde meydana gelen hatalarının e-posta ile bildirilmesi gibi yöntemlerin kullanımı açıklanmalıdır. Hata sonrasında atılacak adımlar ve hatanın giderilene kadar takibinin nasıl yapılacağı belirlenmeli ve planda yer almalıdır.
- ✓ **Medya yönetimi:** Yedekleme medyalarının sayısı, nerede bulunduğu, medyaların içerisinde hangi yedekleme işlerinin bulunduğu gibi kayıtlar tutulmalıdır. Bu işlemlerin nasıl gerçekleştirileceği planda belirtilmelidir. Medyaların takibi için genellikle barkot numaraları kullanılmaktadır. Barkot kullanılsın veya kullanılsın medyaların etiketlenmesi için bir standart geliştirilmeli ve uygulanmalıdır.
- ✓ **Yedekleme Altyapısı:** Yedekleme altyapısı detaylı olarak açıklanmalıdır. Donanım altyapısı ve yedekleme yazılımının yönetim ve ajanlarının kurulu olduğu bilgisayarlar belirtilmelidir.
- ✓ **Yedeklerin uzak ortamda saklanması:** Alınmış olan yedeklerin uzakta saklanmasına yönelik olarak işlemin hangi sıklıkla gerçekleştirileceği, kimin gerçekleştireceği, medyanın aktarımın ne şekilde gerçekleştirileceği ve bu işlemler için kullanılacak prosedürler ayrıntılı olarak belirtilmelidir. Uzak ortam saklama koşulları ve medya güvenliğinin nasıl sağlanacağı planda belirtilmelidir.
- ✓ **Alınmış yedeklerin test edilmesi:** Yedeklerin test edilmesine dair test planı hazırlanmalıdır. Düzenli olarak test edilmesi ve bu testlerin kontrolünün nasıl gerçekleştirileceği planda belirtilmelidir.

-
- ✓ **Yedekleme ve geri dndrme talimatı:** Yedekleme sisteminin gnlk iřlerinin yerine getirilmesi ve yeni yedekleme iřinin tanımlanması iin yedekleme talimatı hazırlanmalıdır. Ayrıca alınmıř olan yedeklerden geri dndrme iřlemlerinin anlatıldıđı bir geri dndrme talimatı hazırlanmalıdır. Sz konusu talimatlar yedekleme planı ierisinde bulunmak zorunda deđildir. Plan ierisinde talimatların isimleri ve nasıl ulařılacađının belirtilmesi yeterlidir. Zaman ierisinde talimatlarda deđiřiklikler gerekmektedir. Bu deđiřiklikler zaman kaybetmeden yapılmalıdır. Yedekleme ve geri dndrme talimatlarının dzenli aralıklarla gncelliđi kontrol edilmelidir.

6. YEDEKLEME SİSTEMİ DENETİMİ

Yedekleme sisteminin denetimi yedekleme politikası ve yedekleme planına göre yapılmalıdır.

Aşağıda yedekleme sistemi denetimi için örnek kontrol listesi verilmiştir.

SIRA NO	DENETLEME MADDESİ	BEKLENEN SONUÇ	BULGU
1	Yedekleme planı	<p>Yedekleme işleri konusunda kuralların belirtildiği bir yedekleme planı bulunmalıdır. Plan içerisinde en az aşağıdaki maddeler bulunmalıdır.</p> <ol style="list-style-type: none"> 1) Yedeklemeden sorumlu olan personelin bilgileri. 2) Yedekleme donanımları, yedeklenen sunucu ve uygulamaların bilgileri 3) Sunucu veya uygulama bazında hangi sıklıkla ve hangi türlerde (tam, fark, artan) yedek alındığı 4) Alınan yedeklerin (data retention time)ne kadar saklanacağı. 5) Yedekleme sisteminde oluşan hataların nasıl izleneceği 6) Geri dönüş işleminin nasıl yapılacağı (ayrı bir talimat olabilir) 7) Yedekleme yazılımının dahili veritabanının veya işletim sisteminin zarara uğraması durumunda nasıl kurtarılacağı (ayrı bir talimat olabilir) 8) Kartuş yönetiminin nasıl yapılacağı 9) Sürekli olarak saklanacak arşiv kopyaları için gerekenler (uzak ofise gönderme, kartuş sayısı vb) 10) Kartuşların nasıl saklanacağı 11) Yedekleme testinin hangi sıklıkta ne nasıl yapılacağı (ayrı bir talimat olabilir) 	
2		Yedekleme işlerinin zamanında çalışmasını, yedekleme ve geri döndürme işlerinin yapılmasını sağlamak üzere gerekli talimatlar bulunmalıdır.	

SIRA NO	DENETLEME MADDESİ	BEKLENEN SONUÇ	BULGU
3		Düzenli olarak geri döndürme testi yapılıyor olmalıdır.	
4		24 saat boyunca çalışan yedekleme işlerinin başarılı olarak tamamlanıp tamamlanmadığı takip edilmelidir.	
5		Ömrünü tamamlayan yedekleme medyalarının takibi yapılmalıdır.	
6	Yedekleme Altyapısı	Yedekleme işleri için ayrı bir sunucu bulunmalıdır.	
7		Yedekleme için gereken yazılım lisansları ile birlikte temin edilmiş olmalıdır.	
8		Yedeklemeden sorumlu personel yazılımın eğitimini almış olmalıdır.	
9		Planda belirtilen sürelerde yedek almayı destekleyecek otomasyon sistemi (teyp kütüphanesi vb) olmalıdır.	
10		Kullanılan yedekleme medyaları güvenli ortamda saklanmalıdır.	
11		Yedekleme medyalarının takibi için barkot okuyucu desteği bulunmalı, bulunmuyorsa alternatif bir yöntem izlenmelidir.	
12		Alınan yedeklerin bir kopyası ana sitede meydana gelebilecek bir felaketten etkilenmeyecek kadar uzak bir mesafede güvenli olarak saklanmalıdır. Planda ön görülen sürelerde medya gönderilmelidir.	
13	Yedekleme yazılımı yapılandırması	Yedekleme yazılımı yapılandırması planda belirtilen yedekleme işlerini yapacak şekilde ayarlanmış olmalıdır.	
14		Yedekleme yazılımı yapılandırmasında gereksiz kullanıcılar bulunmamalıdır.	

SIRA NO	DENETLEME MADDESİ	BEKLENEN SONUÇ	BULGU
15		Veri koruma zamanları (data retention time) planda belirtildiği biçimde ayarlanmış olmalıdır.	
16		Günlük işlerin durumu ve yedekleme hataları ile ilgili uyarım yapılandırması yapılmış olmalıdır.	
17		Yedekleme yazılımının koştugu sunucunun güvenlik sıkılaştırması yapılmış olmalıdır.	
18		Yedekleme yazılımı ve yazılımın koştugu işletim sisteminin son yamaları yapılmış olmalıdır.	
19		Yedekleme yazılımının dahili veritabanı (eğer veritabanı kullanıyorsa) her gün ve belirli bir yedekleme medyasına (barkot numarası veya etiketi belirli olan) alınmalıdır.	
20		Dahili veritabanı yedeklemesi için kullanılan medyanın bilgileri (barkot numarası, etiket adı vb) yedekleme sistemi çalışmasa bile ulaşılabilir olmalıdır.	
21		Yedeklenecek sunucuların farklı ağda bulunması durumunda port sıkılaştırmaları ve güvenlik duvarı ayarları yapılmış olmalıdır.	

KAYNAKÇA

- [1]. Curtis Preston, Backup & Recovery
- [2]. Dorian Cougias, E. L. Heiberger , Karsten Koop, The Backup Book: Disaster Recovery from Desktop to Data Center
- [3]. David B Little , David A. Chapa , Implementing Backup and Recovery: The Readiness Guide for the Enterprise
- [4]. Jon William Toigo, Disaster Recovery Planning: Preparing for the Unthinkable (3rd Edition)