Desteğin bir kısmı DBMS tedarikçileri ile etkileşim yoluyla sağlanır. Yazılım tedarikçileriyle iyi ilişkiler kurmak, şirketin iyi bir dış destek kaynağına sahip olmasını sağlamanın bir yoludur. Satıcılar yeni ürünler ve personelin yeniden eğitimi ile ilgili güncel bilgilerin kaynağıdır. İyi satıcı-şirket ilişkilerinin, veritabanı gelişiminin gelecekteki yönünü belirlemede kuruluşlara avantaj sağlaması da muhtemeldir.

VTYS, Yardımcı Programlar ve Uygulamaların Bakımı

DBA'nın bakım faaliyetleri operasyonel faaliyetlerin bir uzantısıdır. Bakım faaliyetleri VTYS ortamının korunmasına adanmıştır.

Periyodik DBMS bakımı, fiziksel veya ikincil depolama cihazlarının yönetimini içerir. En yaygın bakım faaliyetlerinden biri, veritabanındaki verilerin fiziksel konumunu yeniden düzenlemektir. (Bu genellikle DBMS ince ayar faaliyetlerinin bir parçası olarak yapılır.) Bir veritabanının yeniden düzenlenmesi, performansı artırmak için DBMS'ye bitişik disk sayfası konumları tahsis etmek üzere tasarlanabilir. Yeniden düzenleme işlemi ayrıca silinen verilere ayrılan alanı boşaltarak yeni veriler için daha fazla disk alanı sağlayabilir.

Bakım faaliyetleri DBMS ve yardımcı program yazılımının yükseltilmesini de içerir. Yükseltme, DBMS yazılımının yeni bir sürümünün veya bir İnternet ön uç aracının yüklenmesini gerektirebilir. Ya da, farklı bir ana bilgisayarda çalışan bir ana DBMS'ye erişime izin vermek için ek bir DBMS ağ geçidi oluşturabilir. DBMS ağ geçidi hizmetleri, istemci/sunucu ortamında çalışan dağıtılmış DBMS uygulamalarında yaygındır. Ayrıca, yeni nesil veritabanları uzamsal veri desteği, veri ambarı ve yıldız sorgu desteği ve İnternet erişimi için Java programlama arayüzleri desteği gibi özellikler içerir (bkz. Bölüm 15, Veritabanı Bağlantısı ve Web Teknolojileri). Şirketler sıklıkla farklı formatlarda ya da veritabanları arasında veri alışverişi yapma ihtiyacı ile karşı karşıya kalmaktadır. DBA'nın bakım çalışmaları, uyumsuz formatlardaki ya da farklı DBMS yazılımlarındaki veriler için geçiş ve dönüştürme hizmetlerini içerir. Bu tür durumlar, sistem bir sürümden diğerine yükseltildiğinde veya tamamen yeni bir DBMS mevcut DBMS'nin yerini aldığında yaygın olarak görülür. Veritabanı dönüştürme hizmetleri, kullanıcının çeşitli aktiviteleri (elektronik tablo analizi, grafik oluşturma, istatistiksel modelleme vb.) gerçekleştirmesine olanak sağlamak için ana DBMS'den (ana bilgisayar tabanlı) son kullanıcının kişisel bilgisayarına veri indirmeyi de içerir. Taşıma ve dönüştürme hizmetleri mantıksal düzeyde (VTYS'ye özgü veya yazılıma özgü) veya fiziksel düzeyde (depolama ortamı veya işletim sistemine özgü) yapılabilir. Yeni nesil DBMS'ler, veritabanları arasında veri alışverişi için standart bir format olarak XML'i desteklemektedir. sistemler ve uygulamalar (bkz. Bölüm 15).

16-6 Güvenlik

Bilgi sistemi güvenliği, bir bilgi sisteminin ve ana varlığı olan verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlayan faaliyetleri ve önlemleri ifade eder.[4] Verilerin güvenliğini sağlamak, şirket çapında kapsamlı bir yaklaşım gerektirir. Yani, donanım sistemleri, yazılım uygulamaları, ağ ve cihazları, dahili ve harici kullanıcılar, prosedürler ve verilerin kendisi dahil olmak üzere etrafındaki tüm süreçleri ve sistemleri güvence altına almazsanız verileri güvence altına alamazsınız. Veri güvenliğinin kapsamını anlamak için üç güvenlik hedefinin her birini daha ayrıntılı olarak ele alın:

- **Gizlilik**, verilerin yetkisiz erişime karşı korunmasını ve yetkili bir kullanıcı verilere erişirse, yalnızca yetkili bir amaç için kullanılmasını sağlamakla ilgilenir. Başka bir deyişle gizlilik, bir kişi veya kuruluşun gizlilik haklarını ihlal edecek herhangi bir bilginin ifşa edilmesine karşı verilerin korunmasını gerektirir. Veriler gizlilik seviyesine göre değerlendirilmeli ve sınıflandırılmalıdır: son derece kısıtlı (çok az kişinin erişimi vardır), gizli (yalnızca belirli grupların erişimi vardır) ve kısıtlanmamış (erişilebilir).

GİZLİLİK
Veri güvenliği bağlamında, verilerin yetkisiz erişime karşı korunmasının sağlanması ve verilere bir kişi tarafından erişilmesi durumunda
Yetkili kullanıcı, verilerin yalnızca yetkili bir amaç için kullanıldığını.

[4]Krause, M. ve Tipton, H., *Handbook of Information Security Management*, CRC Press LLC, 1999.

tüm kullanıcılar tarafından erişilebilir). Veri güvenliği sorumlusu, kuruluşun istenen gizlilik seviyelerine uygun olmasını sağlamak büyük miktarda zaman harcar.

Uyumluluk
Veri gizliliği ve güvenliği raporlama yönergelerini veya gereksinimlerini karşılayan faaliyetler.

- **Uyumluluk**, veri gizliliği ve güvenliği raporlama yönergelerini karşılayan faaliyetleri ifade eder. Bu yönergeler ya dahili prosedürlerin bir parçasıdır ya da federal hükümet gibi harici düzenleyici kurumlar tarafından dayatılır. Veri gizliliği ve mahremiyetini sağlamak için çıkarılan ABD mevzuatına örnek olarak Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA), Gramm-Leach-Bliley Yasası (GLBA) ve Sarbanes-Oxley Yasası (SOX) verilebilir.

bütünlük
Veri güvenliği çerçevesinde, verilerin tutarlı ve hata veya anormalliklerden uzak tutulması anlamına gelir. Ayrıca bkz. *veri bütünlüğü*.

- Veri güvenliği çerçevesinde **bütünlük**, verilerin tutarlı ve hata ya da anormalliklerden uzak tutulmasıyla ilgilidir. (Veri tutarsızlıkları ve veri anomalileri kavramlarını gözden geçirmek için Bölüm 1'e bakınız). VTYS, veritabanındaki verilerin bütünlüğünün sağlanmasında çok önemli bir rol oynar. Ancak, güvenlik açısından bakıldığında, kurumsal süreçler, kullanıcılar ve kullanım şekilleri de bütünlüğü korumalıdır. Örneğin, evde çalışan bir personelin ürün maliyetlerine erişmek için interneti kullanması kabul edilebilir bir kullanım olarak değerlendirilebilir; ancak güvenlik standartları, çalışanın güvenli bir bağlantı kullanmasını ve basılı raporları parçalamak ve verileri yerel sabit sürücüye kopyalamak için şifreleme kullanmak gibi evde verileri yönetmek için katı prosedürleri izlemesini gerektirebilir. Veri bütünlüğünün korunması, veri toplama ile başlayan ve veri depolama, işleme, kullanım ve arşivleme ile devam eden bir süreçtir (bkz. Bölüm 13, İş Zekası ve Veri Ambarları). Bütünlüğün arkasındaki mantık, verileri kuruluştaki en değerli varlık olarak ele almak ve kuruluş içindeki tüm seviyelerde titiz veri doğrulaması yapılmasını sağlamaktır.

kullanılabilirlik
Veri güvenliği bağlamında, verilerin yetkili kullanıcılar tarafından ihtiyaç duyulduğunda ve yetkili amaçlar için erişilebilir olmasını ifade eder.

- **Kullanılabilirlik**, verilerin yetkili kullanıcılar tarafından istendiği zaman ve yetkili amaçlar için erişilebilirliğini ifade eder. Veri kullanılabilirliğini sağlamak için, tüm sistem herhangi bir iç veya dış kaynaktan kaynaklanan hizmet bozulmasına veya kesintisine karşı korunmalıdır. Hizmet kesintileri hem şirketler hem de kullanıcılar için çok maliyetli olabilir. Sistem kullanılabilirliği güvenliğin önemli bir hedefidir.

16-6a Güvenlik Politikaları

Normalde, sistemin ve ana varlığı olan verilerin güvenliğini sağlama görevi, uyumlu bir veri güvenliği stratejisi oluşturmak için birlikte çalışan veritabanı güvenlik görevlisi ve veritabanı yöneticisi/yöneticileri tarafından yerine getirilir. Böyle bir strateji, sağlam ve kapsamlı bir güvenlik politikasının tanımlanmasıyla başlar. **Güvenlik politikası**, bir sistemin güvenliğini garanti altına almak ve denetim ve uyumluluğu sağlamak için oluşturulan standartlar, politikalar ve prosedürler bütünüdür. Güvenlik denetimi süreci, kuruluşun bilgi sistemi altyapısındaki güvenlik açıklarını tespit ederek ve sistemi ve verileri bu açıklara karşı koruyacak önlemleri belirleyerek başlar.

güvenlik politikası
Aşağıdakileri garanti altına almak için oluşturulan standartlar, politikalar ve prosedürler bütünü
Bir sistemin güvenliğini, denetimini ve uyumluluğunu sağlar.

16-6 b Güvenlik Açıkları

Güvenlik açığı, bir sistem bileşeninde yetkisiz erişime izin vermek veya hizmet kesintilerine neden olmak için kullanılabilecek bir zayıflıktır. Bu tür güvenlik açıkları aşağıdaki kategorilerden birine girebilir:

güvenlik açığı Bir sistem bileşeninde bulunabilecek bir zayıflık
yetkisiz erişime izin vermek veya hizmet kesintilerine neden olmak için istismar edilebilir.

- *Teknik*. İşletim sistemindeki veya web tarayıcısındaki bir kusur buna örnek olarak verilebilir.
- *Yönetimsel*. Örneğin, bir kuruluş kullanıcıları kritik güvenlik sorunları hakkında eğitmeyebilir.
- *Kültürel*. Kullanıcılar şifrelerini klavyelerinin altına saklayabilir veya gizli raporları parçalamayı unutabilir.
- *Prosedürel*. Şirket prosedürleri karmaşık parolalar veya kullanıcı kimliklerinin kontrol edilmesini gerektirmeyebilir.

Bir güvenlik açığı kontrol edilmeden bırakıldığında, bir güvenlik tehdidine dönüşebilir. **Güvenlik tehdidi**, yakın bir güvenlik ihlalidir.

güvenlik tehdidi
Kontrol edilmemiş güvenlik açıkları nedeniyle meydana gelebilecek yakın bir güvenlik ihlali.

Bir **güvenlik ihlali**, sistemin bütünlüğünü, gizliliğini veya kullanılabilirliğini tehlikeye atmak için bir güvenlik tehdidinden yararlanıldığında meydana gelir. Güvenlik ihlalleri, bütünlüğü korunmuş ya da bozulmuş bir veritabanına yol açabilir.

güvenlik ihlali
Bir güvenlik tehdidinin bütünlüğü tehlikeye atacak şekilde istismar edildiği bir olay,
sistemin gizliliği veya kullanılabilirliği.

- *Korunmuş*. Bu durumlarda, benzer güvenlik sorunlarının tekrarlanmasını önlemek için harekete geçilmesi gerekir, ancak veri kurtarma gerekli olmayabilir. Aslında, çoğu güvenlik ihlali bilgi amaçlı yetkisiz ve fark edilmeyen erişimden kaynaklanır, ancak bu tür gözetlemeler veri tabanını bozmaz.
- *Bozulmuş*. Benzer güvenlik sorunlarının tekrarlanmasını önlemek için harekete geçilmeli ve veritabanı tutarlı bir duruma getirilmelidir. Bozucu güvenlik ihlalleri arasında bilgisayar virüsleri ve verileri yok etmek ya da değiştirmek isteyen bilgisayar korsanları tarafından veri tabanına erişim yer alır.

Tablo 16.4'te sistem bileşenlerinin bazı güvenlik açıkları ve bunlara karşı tipik koruyucu önlemler gösterilmektedir.

Tablo 16.4 Örnek Güvenlik Açıkları ve İlgili Koruyucu Önlemler

Sistem Bileşeni	Güvenlik Zafiyeti	Güvenlik Önlemleri
İnsanlar	• Kullanıcı boş bir parola belirler. • Parola kısadır veya doğum tarihi içerir. • Kullanıcı ofis kapısını her zaman açık bırakır. • Kullanıcı bordro bilgilerini uzun süre ekranda bırakır.	• Karmaşık parola politikaları uygulayın. • Çok düzeyli kimlik doğrulama kullanın. • Güvenlik ekranları ve ekran koruyucuları kullanın. • Kullanıcıları hassas veriler konusunda eğitin. • Güvenlik kameraları kurun. • Otomatik kapı kilitleri kullanın.
İş istasyonu ve sunucular	• Kullanıcı verileri bir flash sürücüye kopyalar. • İş istasyonunu birçok kişi kullanıyor. • Bir elektrik kesintisi bilgisayarı çökertir. • Yetkisiz personel bilgisayarı kullanabilir. • Hassas veriler bir dizüstü bilgisayarda saklanmaktadır. • Çalınan bir sabit disk veya dizüstü bilgisayar nedeniyle veri kaybı • Bir doğal afet meydana gelir.	• Flash sürücülerin kullanımını kısıtlamak için grup ilkelerini kullanın. • İş istasyonlarına kullanıcı erişim hakları atayın. • Kesintisiz güç kaynakları (UPS'ler) kurun. • Bilgisayarlara güvenlik kilitleri ekleyin. • Çalınan dizüstü bilgisayarlar için bir kill switch uygulayın. • Veri yedekleme ve kurtarma planları oluşturun ve test edin. • Sistemi doğal afetlere karşı koruyun - ortak yerleşim stratejilerini kullanın.
İşletim sistemi	• Arabellek taşması saldırıları • Virüs saldırıları • Kök kitleri ve solucan saldırıları • Hizmet reddi saldırıları • Truva atları • Casus yazılım uygulamaları • Şifre kırıcılar	• İşletim sistemi güvenlik yamalarını ve güncellemelerini uygulayın. • Uygulama sunucusu yamalarını uygulayın. • Antivirüs ve antispyware yazılımı yükleyin. • Bilgisayarlarda denetim izleri uygulayın. • Periyodik sistem yedeklemeleri gerçekleştirin. • Yalnızca yetkili uygulamaları yükleyin. • Yetkisiz yüklemeleri önlemek için grup ilkelerini kullanın.
Uygulamalar	• Uygulama hataları-tampon taşması • SQL enjeksiyonu, oturum kaçırma vb. • Uygulama güvenlik açıkları-çapraz site komut dosyası oluşturma, doğrulanmamış girdiler • E-posta saldırıları -pamming, phishing, vb. • Sosyal mühendislik e-postaları	• Uygulama programlarını kapsamlı bir şekilde test edin. • Kodun içine koruma önlemleri ekleyin. • Uygulamalarda kapsamlı güvenlik açığı testi yapın. • E-posta sistemleri için spam filtreleri ve antivirüs yazılımı yükleyin. • Güvenli kodlama tekniklerini kullanın (bkz. www.owasp.org). • Kullanıcıları sosyal mühendislik saldırıları konusunda eğitin.
Şebeke	• IP sahtekarlığı • Paket koklayıcılar • Hacker saldırıları • Ağdaki parolaları temizleyin	• Güvenlik duvarlarını kurun. • Sanal özel ağları (VPN'ler) kullanın. • İzinsiz giriş tespit sistemleri (IDS'ler) kullanın. • Ağ erişim kontrolünü (NAC) kullanın. • Ağ etkinliği izlemeyi kullanın.
Veri	• Veri paylaşımları tüm kullanıcılara açıktır. • Verilere uzaktan erişilebilir. • Paylaşılan bir kaynaktan veri silinebilir.	• Dosya sistemi güvenliğini uygulayın. • Paylaşım erişim güvenliğini uygulayın. • Erişim iznini kullanın. • Verileri dosya sistemi veya veritabanı düzeyinde şifreleyin.

16-6c Veritabanı Güvenliği

veritabanı güvenliği
Bir kuruluşun güvenlik gereksinimlerine uymak için DBMS özelliklerinin ve diğer ilgili önlemlerin kullanılması.

Veritabanı güvenliği, kuruluşun güvenlik gereksinimlerine uyan VTYS özelliklerini ve diğer ilgili önlemleri ifade eder. DBA'nın bakış açısından, VTYS'yi hizmet bozulmasına karşı korumak ve veritabanını kayıp, bozulma veya yanlış kullanıma karşı korumak için güvenlik önlemleri uygulanmalıdır. Kısacası, DBA VTYS'yi kurulum noktasından işletme ve bakım aşamasına kadar güvence altına almalıdır.

Not

James Martin'in bir veritabanı güvenlik stratejisinin arzu edilen özelliklerine ilişkin mükemmel tanımı bugün de geçerliliğini korumaktadır (*Managing the Database Environment*, Prentice-Hall, 1977). Martin'in güvenlik stratejisi, veritabanı güvenliğinin yedi temel unsuruna dayanmaktadır ve verilerin korunduğu, yeniden yapılandırılabildiği, denetlenebildiği ve kurcalanmaya karşı dayanıklı olduğu ve kullanıcıların tanımlanabilir, yetkilendirilebilir ve izlenebilir olduğu bir strateji olarak özetlenebilir.

VTYS'yi hizmet bozulmasına karşı korumak için bazı güvenlik önlemleri tavsiye edilmektedir. Örneğin:

- Varsayılan sistem parolalarını değiştirme
- Varsayılan kurulum yollarını değiştirme
- En son yamaları uygulayın
- Uygun erişim haklarına sahip güvenli kurulum klasörleri
- Yalnızca gerekli hizmetlerin çalıştığından emin olun
- Denetim günlüklerini ayarlama
- Oturum günlüğünü ayarlama
- Oturum şifrelemesi gerektir

Ayrıca DBA, VTYS'yi ve ağ üzerinde çalışan tüm hizmetleri koruyan ağ güvenliğini uygulamak için ağ yöneticisiyle yakın işbirliği içinde çalışmalıdır. Modern kurumlarda bilgi mimarisinin en kritik bileşenlerinden biri ağdır.

yetkilendirme yönetimi
Veritabanı güvenliğini ve bütünlüğünü koruyan ve garanti eden prosedürler. Bu prosedürler arasında kullanıcı erişim yönetimi, görünüm tanımı, DBMS erişim kontrolü ve DBMS kullanım izleme yer alır.

Veritabanındaki verilerin korunması, yetkilendirme yönetiminin bir işlevidir. **Yetkilendirme yönetimi**, veritabanı güvenliğini ve bütünlüğünü korumak ve garanti altına almak için prosedürleri tanımlar. Bu prosedürler aşağıdakileri içerir:

- *Kullanıcı erişim yönetimi*. Bu işlev veritabanına erişimi sınırlandırmak için tasarlanmıştır; en azından aşağıdaki prosedürleri içerir:
  - *Her bir kullanıcıyı veritabanına tanımlar*. DBA bu işlevi işletim sistemi düzeyinde ve DBMS düzeyinde gerçekleştirir. İşletim sistemi düzeyinde, DBA bilgisayar sisteminde oturum açan her son kullanıcı için benzersiz bir kullanıcı kimliği oluşturulmasını talep edebilir. VTYS düzeyinde, DBA farklı bir kullanıcı kimliği oluşturabilir ya da son kullanıcının VTYS'ye erişimini yetkilendirmek için aynı kullanıcı kimliğini kullanabilir.
  - *Her kullanıcıya parola atayın*. DBA bu işlevi hem işletim sistemi hem de DBMS düzeyinde gerçekleştirir. Veritabanı parolalarına önceden belirlenmiş son kullanma tarihleri atanabilir, bu da DBA'nın son kullanıcıları periyodik olarak taramasını ve parolalarını değiştirmelerini hatırlatmasını sağlar, böylece yetkisiz erişim olasılığı azalır.
  - *Kullanıcı gruplarını tanımlayın*. Kullanıcıları ortak erişim ihtiyaçlarına göre gruplar halinde sınıflandırmak, DBA'nın bireysel kullanıcıların erişim ayrıcalıklarını kontrol etmesine ve yönetmesine yardımcı olabilir. Ayrıca

DBA, sistemdeki haydut kullanıcıların etkisini en aza indirmek için veritabanı rollerini ve kaynak sınırlarını kullanabilir. (Bu konular hakkında daha fazla bilgi için Bölüm 16-10d'ye bakın).

- *Erişim ayrıcalıkları atayın*. DBA, belirli veritabanlarına erişmeleri için belirli kullanıcılara erişim ayrıcalıkları atar. Erişim hakları yalnızca okuma ile sınırlı olabilir veya yetkili erişim okuma, yazma ve silme ayrıcalıklarını içerebilir. İlişkisel veritabanlarında erişim ayrıcalıkları SQL GRANT ve REVOKE komutları aracılığıyla atanır.

Not

GRANT ve REVOKE komutları SQL'de ayrıcalık ve kullanıcı belirtilerek uygulanır. Örneğin, MJORDAN kullanıcısına PRODUCT tablosunda güncelleme ayrıcalıkları vermek aşağıdaki komutla yapılır:

MJORDAN'A ÜRÜN GÜNCELLEMESİ VERİN;

PRODUCT tablosunda MJORDAN'dan güncelleme ayrıcalığını kaldırmak için aşağıdaki komutu kullanın:

MJORDAN'DAN GELEN ÜRÜN GÜNCELLEMESINI IPTAL EDIN;

- *Fiziksel erişimi kontrol edin*. Fiziksel güvenlik yetkisiz kullanıcıların DBMS kurulumuna ve tesislerine doğrudan erişimini engelleyebilir. Büyük veri tabanı kurulumları için yaygın fiziksel güvenlik, güvenli girişler, parola korumalı iş istasyonları, elektronik personel rozetleri, kapalı devre video, ses tanıma ve biyometrik teknolojiyi içerir.

- *Görünüm tanımı*. DBA, yetkili bir kullanıcı tarafından erişilebilen verilerin kapsamını korumak ve kontrol etmek için veri görünümlerini tanımlamalıdır. DBMS, bir veya daha fazla tablodan oluşan görünümlerin tanımlanmasına izin veren araçlar sağlamalı ve kullanıcılara erişim hakları atamalıdır. İlişkisel veritabanlarında görünümleri tanımlamak için SQL CREATE VIEW komutu kullanılır. Oracle DBMS, DBA'nın farklı kullanıcılar için verilerin özelleştirilmiş görünümlerini oluşturmasına olanak tanıyan Sanal Özel Veritabanı (VPD) sunar. Bu özellik sayesinde DBA, bir bordro veritabanını sorgulayan normal kullanıcıların yalnızca gerekli satır ve sütunları görmesini kısıtlayabilirken, departman yöneticileri yalnızca kendi departmanlarıyla ilgili satır ve sütunları görebilir.
- *DBMS erişim kontrolü*. Veritabanı erişimi, DBMS sorgu ve raporlama araçlarının kullanımına sınırlar getirilerek kontrol edilebilir. DBA, araçların doğru şekilde ve yalnızca yetkili personel tarafından kullanıldığından emin olmalıdır.
- *VTYS kullanım izleme*. DBA ayrıca veritabanındaki verilerin kullanımını da denetlemelidir. Birçok DBMS paketi, tüm kullanıcılar tarafından gerçekleştirilen veritabanı işlemlerinin kısa bir açıklamasını otomatik olarak kaydeden bir **denetim günlüğünün** oluşturulmasına izin veren özellikler içerir. Bu tür denetim izleri DBA'nın erişim ihlallerini saptamasını sağlar. Denetim kayıtları tüm veritabanı erişimlerini ya da sadece başarısız olanları kaydedecek şekilde uyarlanabilir.

denetim günlüğü
Tüm kullanıcılar tarafından gerçekleştirilen veritabanı işlemlerinin kısa bir açıklamasını otomatik olarak kaydeden bir veritabanı yönetim sisteminin güvenlik özelliği.

Bir veritabanının bütünlüğü, DBA'nın kontrolü dışındaki dış etkenler nedeniyle kaybolabilir. Örneğin, veritabanı bir patlama, yangın ya da deprem nedeniyle hasar görebilir ya da yok olabilir. Sebep ne olursa olsun, veritabanının bozulması ya da yok olması ihtimali, yedekleme ve kurtarma prosedürlerini her DBA için çok önemli hale getirir.

16-7 Veritabanı Yönetim Araçları

Kurumlardaki veri yönetimi faaliyetlerinin olağanüstü büyümesi, daha iyi yönetim standartlarına, süreçlerine ve araçlarına ihtiyaç duyulmasına neden oldu. Yıllar içinde, yalnızca veri yönetim araçlarına adanmış yeni bir endüstri ortaya çıktı. Bu araçlar, veri yönetiminin tüm spektrumunu kapsamaktadır.