AĞ GÜVENLİĞİ

*Emin DOĞAN AYDIN

Önsöz

Bu makale, organizasyonlarındaki ağ güvenliğini iyileştirmek için program geliştirmede kılavuza ihtiyaç duyan yöneticilere (genel, fonksiyonel ve bilişim sistemleri yönetimindeki) yardım amacıyla yazılmıştır.

Bu manual veri güvenliği ve bütünlüğü ile ilgili yönetim denetimindeki temel etkenlerle birlikte bilişim sistemleri ağı ortamındaki güvenlik risklerini tanımlama ve sınırlama için ilgili kavramları gösterir.

Burada tartışılan tekniklerin bazı çeşitleri çoğu ağ çevrelerine uygulanabilir. Buna rağmen seçilen tekniğin organizasyonun amaçlarıyla ve politikalarıyla uyumlu olması ve düşük maliyetli olması için iyi seçilmesi ve uygulanması gerekir.

Genel Bakış

Ağ güvenliği şöyle tanımlanabilir :

Bilişim sistemi ağı ortamındaki bilginin bütünlüğünü ve korunmasını sağlamak için yerine getirlen, yönetim denetim ve

*Öğretim Üyesi, Marmara Üniversitesi İletişim Fakültesi Bilişim Ana Bilim Dalı.

işlemlerinin alt kümesidir.

Ağ Güvenliği Amaçları

Çoğu ağ güvenlik programlarının amaçları aşağıdaki maddelerden bir veya daha fazlasından oluşmuştur :

Aşağıdaki herhangi bir noktadan iletilen bilginin tasarlanan varış noktasından alınmasını ve başka bir yere daha ulaşmamasını sağlamak

Alınan bilginin içeriğinin gönderilen ile tamamen aynı olmasını sağlamak (hiç bir şey eklenmemeli, hiç bir şey silinmemeli, hiç bir şey değiştirilmemeli)

Organizasyonun yerindeki tüm ağ bileşenlerine (terminaller, terminal denetleyicileri, modemler, node'lar, veri link'leri ve iletişim hatları) sadece yetkili kılınan elemanların erişebilmesini sağlamak

Bilgiyi gönderenin, bilginin yetkili alıcı (ve sadece o) tarafından alındığının kontrolünün yapabilmesini sağlamak

Bilgiyi alanın, iletişim başladığında gönderici durumunda gözüken kişinin gerçekten onu gönderen kişi olduğunu kontrol edebilmesini sağlamak

İletişim halindeki bilginin yetkisiz kişi veya araç tarafından gözlemlenmesinin, karıştırılmasının veya ağdan alınmasının önlenmesini sağlamak

Ağdaki bilginin alınmasına, karıştırılmasına yetkisiz bir kişi veya araç tarafından herhangi bir teşebbüsün tesbit edilmesini ve daha sonraki oluşumları önlemek için uygun hareketin yapılmasını sağlamak

Gerektiğinde ağdaki bir noktadaki bilgiyi başka bir noktaya iletmek için alternatif uygun yolların bulunmasını sağlamak

Ana ve alternatif yolların başarısızlığında iletişim tenkit bilgileri vasatalarının tanımlanmasını, yerine getirilmesini ve test edilmesini sağlamak

AĞ Güvenliği Sorunları

Doğal olarak ağlar şunları kapsar :

Yönetilecek geniş sayı ve çeşitlilikde araçlar
"Akıllı" ve "Aptal" terminallerin karışımı
Değişik ağ oluşturma şemalarını
Değişik ortam türlerini
Değişik topolojileri
Değişik iletim tekniklerini
Değişik ağ protokollerini ve protokol katmanlarını
Organizasyon alanının dışındaki veri akışını

Bundan dolayı organizasyonun, ağ ortamı üzerine dikkatle odaklanması ve o ortama özel riskleri dikkatlice ortaya koyması gereklidir.

Riskler tanımlandığında koruyucu önlemler belirleneblir ve maliyet/yarar temeline göre seçilerek yerine getirilebilir. Tercihen bunların belirlenmesi ağın kurulumunda sonra yerine önceden yapılır. Var olan bir ağa güvenliği yerleştirmek pahalı olabilir.

Güvenlik önlemlerinin yerine getirilmesinden sonra bile periyodik olarak risk analizleri yapılmalıdır.

AĞ Güvenlik Riskleri ve Denetimi

Bilişim sistemi ağında güvenlik denetiminin bazı

maliyetleri vardır. Bu denetimler uygulanmadan tedbirli yönetici :

Birincisi, genel olarak veri güvenliğinin değerini bilmeli

İkincisi, güvenliğe maruz bırakan temel kaynakların, suçlu hareketlerden çok kazara ve istek dışı olaylar olduğunu anlamalı

Üçüncü, organizasyonun ağını ve temel zarar alabilecek noktalarını anlamalı

Dördüncü, ortamlarındaki riski azaltmak için uygun yönetim denetimlerini ayırt edebilmeli

Beşinci, risk azaltımını gözönüne alarak düşük maliyetli güvenlik denetimlerini yerine getirebilmeli

Mali Kayıba Maruz Kalma Sebebleri

Not: Aşağıda tartışılan maruz kalınan olayların hiyerarjisi geniş müşteri spectrumu ile uğraşmış güvenlik danışmanlarının tarihsel perspektifini gösterir. Maruz kalınan bu olaylar kurulumun yapısına ve uygulanan yönetim denetiminin derecesine bağlı olarak büyük değişiklik gösterebilir.

En büyük mali kayıp, veri girişi, veri günlemesi, uygulama değiştirmesi sırasında hata yapan dürüst kullanıcı yanlış ve ihmallerinden oluşmaktadır.

İkinci büyük mali kayıp ise ellerinde tuttukları yetkiyi suistimal eden dürüst olmayan kullanıcılardan doğar. Dürüst kullanıcı yönetim tarafından farkedilmeyen hatalar ve ihmalleri yaparak organizasyondan nasıl yararlanabileceğini öğrenir. Kişisel ihtiyaç taahütü yendiğinde dürüst kullanıcı çabucak dürüst olmayan olur.

Üçüncü yangın ve doğal afetlerdir. Yönetim tarafından küçümsenmesine rağmen yangın halen önemli tehlikedir. Otomatik yangın önleme sistemleri kurmakta kısmi çözümdür. Ayrıca otomatik sistemin periyodik testi ve yangın söndürme cihazlarının doğru kullanılmasının periyodik eğitimi yapılmalıdır. Coğrafik yere bağlı olarak tarihsel olayların ışığında doğal afetler daha tahmin edilebilir durumdadır. Doğal afetlerin etkisini azaltmada uygun hazırlıklar ve simulaston testleri yararlı olmaktadır.

Dördüncü organizasyon için çalışan veya çalışmış olan ve organizasyona zarar vermek isteyen kullanıcılardır. Darast olmayan kullanıcılar ile temel farklılıkları, şahsi kazanç kaynaklarının kesilmesine yolaçacağından onların yaptıklarının bulunmasını istememeleri iken bunların farkedilecek zarar verme istekleridir.

Beşinci su hasarıdır. Bu çok dikkat edilmesine rağmen patlak borular, sızan tavanlar ve diğer özürler gibi öngörülmemiş olaylar nedeni ile halen tehlikedir.

Altıncı dış tehlikelerdir. Bunlar savaş ve isyan gibi insanlarca yapılan tehlikelerdir. En az tehlike bu alanda olmsına rağmen ihmal edilmemeli.

Son deneyimler yeni bir tehlike kategorisi doğuracak yeni bir etmeni işaret etmektedir. Bu toxic PCB'lerin ve kimyasal dökümlerin organizasyon üzerindeki etkisidir. Bu tipte bir çok olay tespit edilmiştir ve ya PCB bulaşması nedeni ile zamanın uzatılması için organizasyonun imkanlara ulaşamaması veya kimyasal dökümler nedeni ile evlerini boşaltmak durumunda kalan çalışanların çalışamaması sonucunu doğurur.

Bu tarihsel maruz kalınan kayıplar hiyerarşisinin farkında olmak, büyük kayıplı alanlarda etkili denetim ve işlemlerin yapılması ile birlikte, diğer tehlikelere karşı uygun koruyucu önlemlerin alınmasını sağlamadaki uzun yolda ilerleme yaratır.

Ağdaki Kolayca Zarar Verilebilir Noktalar

Ağ ortamları bilişim sistemi ortamındaki ve belirli bir alanda yoğunlaşma yerine coğrafik olarak yayılmış diğer birçok bileşen ile bağlıdır ve bulunan bilgiye erişmek isteyen çalışan sayısı artmaktadır. Bundan dolayı, daha etkili yönetim incelemelerinde bulunulmalı ve basit sıralı işlemler yerine yüksek dereceli denetimler uygulanmalıdır. Her yeni terminalin, ağdaki linkin ve Ağlarda organizastonu bozmak için dürüst olmayan kullanıcıların fırsatları artmaktadır.

Organizasyonlardaki ağlar siteler arası genişlediğinden yangın, su ve doğal afet gibi zararların oluşma şansı artmaktadır. Ayrıca ağ bileşenlerinin hırsızlıktan fiziksel korunumuda önemlidir. Organizasyonu desteklemek için ağ genişlediğinde küçükde olsa dışarıdan saldırılarda olabilir.

Güvenlik teknolojik değil yönetimsel harekettir. Tedbirli yönetim ağ ortamındaki kaybın diğerlerinden daha büyük olduğunu bilmesinin avantajını kullanarak ağı kurarken etkili güvenlik önlem ve denetimlerini öngörür ve ağ genişliğinde bu denetimlerin ince ayarını yapar.

Temel Ağ Güvenlik Denetim ve İşlemleri

Hiçbir iki ağ tamamen aynı olmamasına rağmen, ağların basitlik ve karmaşıklığından bağımsız olarak

uygulanabilecek bazı temel güvenlik denetimleri vardır. Bu denetimler şöyle kategorize edilebilir :

Fiziksel erişim denetimleri
Mantıksal erişim denetimleri
Organizasyonel denetimler
Personel denetimleri
İşlemsel denetimler
Uygulama geliştirme denetimleri
İşistasyonu denetimleri
Veri iletim koruması

Bu sekiz denetim kategorisi ağ olsun veya olmasın herhangi bir bilişim sistemine uygulanabilir.

Fiziksel Erişim Denetimi

Çoğu bilişim sistemi kurulumunda fiziksel erişim denetimi iyi bir şekilde uygulanır. Gerekli dikkat normalde yetkisiz kullanıcıların özel ve sınırlanmış imkanlara erişimini önlemek için engel kurulmasına verilir. B disiplin yetkili kullanıcıların kendi yardımlarını gerektiren imkanlara erişimlerini sınırlayan işlemleri kapsar. Bir çok durumda fiziksel erişim denetimi merkezi işlem imkanı üzerinde odaklanmıştır.

Ağ ortamı fiziksel güvenliğe tekrar odaklanma ihtiyacını işaret eder ve birincil olarak ağ menşeili olan aşağıdaki alanlardaki erişim kontrolüne dikkat çeker :

Merkezi işlem imkanı ile aynı binada olan veya başka sitede olan uzakdan tesisatlar

Bakır tel, eşeksenli kablo, mikrodalga kulesi, uydu çanağı olabilen iletişim bağlantı elemanları

Araç-gereçlere, bağlantılara ve organizasyondaki

bilginin iletimindeki tesisatlara ortak taşıyıcı ile sağlanmış erişim denetimi

Ağ elemanlarını test eden, izleyen özel ağ araç-gereçlerini barındıran ağ denetim merkezi

Uzmanlaşmış bölümsel uygulamalırın tasarım ve işletilmesinde son kullanıcılara yardım için kurulan bilişim merkezleri

Kullanıcılar tarafından gereksinim duyulan işlem manualleri, disketler, lisanslı yazılım kopyaları

Paylaşımlı uzakyazıcı çıktı alanları

Ek olarak ağ elemanları arasındaki fiziksel bağlantı için ağ bağlaşıklığı planlamalı ve periyodik olarak geliştirilmeli. Tüm ağ elemanlarını birbirine bağlamakda (güvenlik riski artar) her zaman gerekli değildir. Ufak alt ağlar kurarak belirli işleyicilere erişmek daha tedbirli bir hareket olabilir. Dışarıdaki ağlara veya işleyicilere erişmek ayrı bir önemli noktadır.

Mantıksal Erişim Denetimi

Bu denetim bilişim sistemi ortamında önemli rol oynar. Yetkili kullanıcıların tanımlanması ve doğrulanması için yöntem sağlaması yanında mantıksal erişim denetimi atanmış iş fonksiyonlarını gerçekleştirmek için gerekli kaynaklara erişmede yetkili kullanıcıları limitler. Etkili olması için mantıksal erişim denetim yeteneği, kaynakların tümden veya seçimsel korunmasını sağlamalı, tüm erişimlerde ve erişim seviyelerinde tahsisat/geri alm yetkisini sağlamalı, uygun yönetimi sağlamalı, tanımlaması ve kullanılması kolay olmalı ve kullanılan kaynakları ve atanan koruma seviyelerini listelyebilmelidir.

Aşağıdaki ağ ortamındaki bilgiyi korumak için en önemli güvenlik işlemlerinden bir tanesidir. Mantıksal erişim denetiminin uygulanması, iyi yönetimsel işlemleri gerektirir :

Korunacak kaynakları tanımlama

Organizasyondaki her şahsiyeti biricik kullanıcı tanımlayıcısı ile tanımlama

Kullanıcının kabul edilebilir seviyede riskistediğini doğrulayacak güvenilir kapasiteyi sağlamak. Bu her kullanıcı sisteme şu şekilde tanıtılarak yapılabilir :

1.Sadece kullanıcının bildiği ile - örneğin şifre

2.Sadece kullanıcının sahip olduğu ile - örneğin manyetik kart

3.Sadece kullanıcıda olan - örneğin imza, parmak izi

Yetki şemasını sağlamk için kaynak sahibinin sorumluluğunda şunlar vardır :

1.Korunmuş kaynaklara erişebilecek kullanıcılar veya kullanıcı gruplarını tanımlamak

2. Her bir kullanıcı veya kullanıcı grubuna atanan erişim yetkisini (sadece okuma veya değiştirme gibi) tanımlama

. Kaynak kullanımını kaydetme, değişiklikleri not emte, kullanım ve değişiklikleri kullanıcıların yöneticilerine, kaynak sahiplerine ve yetki verilmişse güvenlik memurlarına iletmek

Normal hareketlerden sapmaları düzeltmek ve gelecekteki ihlalleri önlemek için uygun yönetimsel işlemleri yapmak

Mantıksal erişim denetimleri IBM'in Kaynak Erişim Denetim Kolaylığı gibi yazılımlar ilede yapılabilir.

Dial-up portları kullanan ağlar için ek bir mantıksal erişimdenetim seviyesi gerekir. Bu ortamlarda sadece

kaynakların kendilerine erişimi sınırlamak değil sisteme pencere gibi olan portlarıda düşünmek gerekir. "Dial-up sistemleri için uygun güvenlik uygulamaları" dökümanı bu tür ortamlardaki koruma yollarını tartışır.

Organizasyonel Denetimler

DP'yi kullanıcılardan ayırmak, DP içindeki görevleri ayırmak, fonksiyonel ayırımları yapmak, şahsi güvenlik sorumluluğu atamak, yönetim denetiminin uygun açıklıklarını kullanmak, uygun olduğunda güvenlik personelini kullanmak geleneksel organizasyonel denetimlerindendir.

Ağ ortamında, bu geleneksel denetimlere odaklanma ihtiyacı var olur, özellikle uzak terminal tesisatlarında, ağ nodlarında, uygulama geliştirme kapasiteleriyle birlikte dağıtılmış veri işleme sitelerinde bu önemlidir. Bir çok durumda geleneksel veri işleyen şahsı ve geleneksel kullanıcıyı (aynı veya farklı kişiler olabilir) ayırmak imkansız olmaktadır. Buna rağmen organizasyonda olduğu gibi çalışanları sisteme uzlaştırma için potansiyeli kaldırma veya en azından minimize etme sorumluluğu yönetimindir.

Bazı ortamlardaki büyüklük izin olanak sağlar ise, organizasyonel denetimlerin her biri bireysel olarak uygulanabilir. Çoğu ortamda denetimler dengelenebilir. Örneğin görevleri ayırmanın uygun olmadığı yerde, yönetim denetiminin süresini azaltma gerekli olabilir. Ek olarak, beklenen olaylar topluluğuna karşı gerçekleştirilen daha sık dinleme aktiviteleri uygun olabilir.

Personel Eğitimi

Geleneksel personel denetimi Uygun kiralama işlemlerini, seyahat ve işe dönme denetimini, çalışan hesaplarını sınırlamayı ve aşağıdaki komple bitirme işlemlerini kapsar.

Ağ ortamlarının doğası nedeni ile yönetim iş dönüşümü ve çalışanların hesap kısıtlamaları üzerinde daha çok kuvvet uygulamak isteyebilir. Çalışan organizasyondan ayrıldığında veya çalışma atamasını değiştirdiğinde mantıksal erişim denetim mekanizmasına girişi sağlayan işlemin varolduğunu sağlamak için özel ilgi gösterilmelidir. Bu işlem çalışanın kimlik bilgisini ve şifresini derhal sistemden çıkartmalıdır.

İşlemsel Denetimler

Geleneksel işlemsel denetimler hataları kont rol etme, hata düzeltmeyi denetleme, formları kontrol etme ve giriş/çıkış ortamını kontrol etmeyi kapsar.

Bu kontroller eğer karmaşıklık artar ise ağ ortamında kritik olabilir. Hataların ve ihmallerin bilgilerin kazara değiştrilmesinde veya tahrip edilmesinde en yüksek risk faktörü oldukları kanıtlandığından yönetim bu alanda sıkı kortrol isteyebilir. Hataları kontrol etmede anahtar eleman, donanım araçlarını, yazılımı, iletişim araç/gereçlerini, iletişim ortamını ve iletişim protokollerini içeren network elemanlarının doğru seçimidir. Ağdaki en zayıf noktalardan biride hata oluştuğunda bunun tesbiti ve hataya göre düzeltici işlem yapmak becerisidir. Bundan dolayı, performans karakteristiklerinin geliştirimi yanında, ağın donanım ve yazılım oluşturumu

güvenirlik, denetlenebilirlik ve hata ele alma yetenekleri ile yapılmalıdır.

Güvenilir ağ elemanları seçimine ek olarak, yönetim yararlı problem yönetim teknik ve işlemlerini düşünmelidir. Her oluşan hata tanımlanmalı ve her düzeltici işlem problem nedeninin pozitif yönde çözümü olmalı ve birkezdaha olmayacağı garanti edilmeli. Detaylı problem yönetm raporları problemin oluş tarih ve saati, problem rapor noktası, problemin etkisi, problemin kaynakları, problemin çözümünden sorumlu şahıslar, alınan düzeltici önelem ve düzeltici işlem tarih ve zamanı gibi bilgileri göstermeli.

Periyodik toplantılar (örneğin minimum aylık, haftalık tercih edilir, yüksek etkili ve yüksek hacimli problemler var ise daha sık) problem tarihçelerinin gözden geçirimi, açık olarak tartışmak, işlem planlarını tanımlamak ve çözüm için amaçların belirlenmesi gibi işlemler için yapılmalı. Bu toplantılar, hizmet fonksiyonlarından tüm departmânların, etkilenen tm kullanıcı gruplarından, ağdaki sorunları çözmek ve ayrıştırmak için organizasyon ile çalışan tüm satıcı veya satıcı acentalarından bir temsilci ile olur.

Uygulama Geliştirme Denetimleri

Geleneksel uygulama geliştirme denetimleri proje denetim sistemleri altında proje evre özetleri, standartları koyma, değişimleri denetleme, kalite kontrolü, kütüphane içerik denetimi yapısal programlama ve bekleyenlere uygulamaların anlatılması gibi teknolojik tekniklerinin programlanmasının gelişimini içerir.

Organizasyonlar bilişim ağlarını kullanarak büyüdüklerinden, eğilim biricik veya uzmanlaşmış uygulamalar geliştirecek daha fazla son kullanıcı yeteneği sağlamak yönünde. Normalde, kullanıcıya yardım ve kılavuzluk sağlamadaki bilgi ve uzmanlık ile beraber merkezi bilişim sistemi kolaylığı tarafından desteklenir fakat işin gereksinimlerine veya belirli departmanın ihtiyaçlarına göre uygulama geliştirme özgürlüğüne sahiptir. Bu ğilim bir çok nedenden oluşmaktadır. Örneğin, birçok uzmanlaşmış uygulamaya ihtiyaç duyan organizasyonlar bu yaklaşımı tüm uygulamaları merkezi uygulama geliştirme bölümünden alamdan daha üretken buldular. Son kullanıcıya uygulama geliştirmeye izin vermekle işyükü organizasyon bütününde dağıtılır, kullanıcılar uygulamayı sadece ne istiyorlar ise ona göre oluştururlar ve uygulamalar daha zamanında oluşur.

Uygulama geliştirme yetksini son kullanıcılara dağıtma yaklaşımı ile merkezi ortamda iyi kurulmuş geleneksel denetimler parçalar. Bu da sıkça son kullancı departmanlarının standart olmayan yazılım elde etmeleri durumunu, uyulamaların geliştiriminin tm organizasyonun bilişim sistemine uygun adapte edilmemesini, uygun şekilde yedeklenmediği için organizasyonun blgi kaybetmesini doğurur.

Uygulama geliştirmedeki bu dağıtılmış yaklaşımı seçen organizasyonlar yeni çevreyi desteklemeye hazır olmalılar. Bu destek, politikaların kurulumunu, işlemleri ve bölümsel uygulamaları geliştirmeden önce son kullanıcıların pratik yapma yöntemleri için kılavuzları içermelidir. Bu kılavuzdaki olması gereken bazı elemanlar şöyle olmalı :

Organizasyonun standartlarına uyan yetkili yazılımı elde etmek.

Yerel geliştirilen kodlar için dökümantasyon gereksinimi

Sert değişim şlemleri

Amaç kodların sadece ana makinadan çekilmesi

Yeni uygulamalar için test ve tümleştirme işlemleri

Veri yedekleme denemeleri

Uyulamaların işletimi için dökümantasyon gereksinimi

Uygulama kütükleri için gereksinimler

Veri bütünlüğü için gereksinimler

Uygulama sonuçlarını dinletmek için gereksinimler

Giriş/çıkış hataları kütükleri için gereksinimler

Hata izolasyonu ve çözümü için gereksinimler

İş İstasyonları Denetimi

Geleneksel stasyonları denetimi, işistasyonlarının fiziksel olarak karıştırma ve elde etme isteklerinden korumayı ve yetkisiz kullanımları önlemek için mantıksal erişim denetimlerini içerir.

Eğer istasyonları paylaşılıyor ise kullanıcı sayısı işistasyonları sayısından daha hızlı bir artış gösterir. Sonuç olarak yönetim çevreyi çok titizlikle dikkate almalı ve işistasyonlarının kurulduğu her yerdeve her durumda geleneksel işistasyonu denetimlerinin uygun yerine getirildiğinin sağlanması için koruyucu önlemleri almalı.

IBM tarafından basılan iki döküman bu alandaki denetimler için yaralı olabilir :

"Kişisel Bilgisayarlar İçin Yararlı Güvenlik Uygulamaları "

"Mahal Dışındaki Terminal Ve Yazılım Kullanımının Denetimi İçin Yararlı Güvenlik Uygulamaları"

Veri İletim Denetimi

Veri iletim denetimi iletişim ortamı üzerinde, veri iletim halinde iken korumak için gereksinimleri belirler.

Mahal içindeki iletişim hatları, kablo bağlantıları, terminal erişim kabloları, denetim birimleri ve onların kabloları, duvardaki kablo bağlantıları ve modemler gibi araçlara erişimi engelleyerek iyi bir fiziksel erişim denetimi sağlamaya çalışır.

Veri mahal dışına iletildiğinde veya mahal içinde başka binaya iletildiğinde fiziksel erişim denetimi yetersiz kalır ve bu durumda bazı organizasyonlar şifrelemeyi kullanmak isteyebilir. Şifreleme çeşitli yollardan yapılabilir :

Bir linkin iki ucunada şifreleme aletleri koyarak linki fiziksel olarak şifreleme

İletilecek bilginin ana işleyici mahalde denetlenmesi ve seçilen uygulamalar için veya seçilen iletişim oturumları için veri iletiminin her yapılışında çağrılması yeteneği, tümleşik şifrelemedir

Şifreleme kişisel bilgisayarda veya ana işleyicide çalışan belirli yazılımsal ürünler vasıtası ile ortaya çıkar

Daha çok şifreleme bilgisi için IBM'in "Şifreleme İle Veri Güenliği" yayını mevcuttur.

Özet

Bilişim sistemleri güvenliği ve iyi güvenlik programlarının anahtar elemanları, organizasyonun veriyi işlemek için nasıl aldığından bağımsızdır. Ağlar işlem kapasitesinin sınırlarını organizasyonun tüm alanlarına kadar hatta birçok durumda organizasyonun sınırları dışına genişletti. Sonuç olarak, yönetim uğraşacağı tamamen yeni bir çevresel şartlar ile karşılaştı ve daha karmaşık ağ, daha karmaşık oturum yarattı.

Bu oturumlarla uğraşmada yardımcı olmak için bu dökümanın kalanı yönetimi eğitmek için tasarlanmış ve varolan çeşitli uygulama seçeneklerine ayrılmıştır. Ağların türleri olan gelecek bölümde daha geniş yazım SNA, SNA bağlantısı, yerel ağlar üzerinde olacaktır. Bu yöneticilere bu uygulamaların biricik olduğunu anlatmak için bilerek yapılmıştır. Ek olarak, Ağ Ortamı, Ağ Teknolojisi, İletim Teknikleri ve Protokolleri adlı ekler bu ağ niteliklerinin ağ güvenliğini niçin ve nasıl etkilediğini yöneticilere daha iyi anlatma fırsatı verir.

Bu meteryalin incelenmesinden elde edilen bilginin organizasyonun çevresine uygulanması mit edilmektedir. Bu başarıldığında, yönetim ne kadar risk alınabilir, ne kadarından kaçınmak mantıklıdır ve riskden kaçınmak için hangi güvenlik önlemleri kullanılabilir diye düşünme durumunda olacak. Her organizasyon ağının farklı olması nedeni ile karar işleminde kullanılacak en uygun önlemler değişir. Bazı durumlarda etkinlik ve verim açısından sıkı yönetim kararları gerekebilir. Tedbirli yöneticler bu iki yayın arasında dengeyi kuracak ve organizasyonun büyük riskden kaçınması için gerekli önlemleri uygulayacak.

Sonuç olarak, ağ ortamının karmaşıklığına bağlı olmaksızın, güvenlik bir yönetim konusudur. Geçmişte organizasyonları zarardan koruyan yararlı güvenlik uygulamaları halen kullanılabilir. Mesele yönetimin organizasyonlarına uyguladıkları yöntemlerinin seçimi, bu yöntemlerin gerekliliğini tüm çalışanlara vurgulama ve yöntemlerin bildirildiği gibi uygulandığını sağlamak için izlenmesidir.