**ZEHRA USLU**

**417304**

**AĞ GÜVENLİĞİ POLİTİKALARI  
  
Ağ Güvenlik Politikası Nedir?** Kurumlar, bilgi paylaşımı amacıyla bilgisayar ağları oluşturup bunları İnternet'e uyarlamıştır. Güvenlik kavramı, eski zamanlardaki kilitli odalardan bilgisayar ağları ve İnternet'e geçişle değişmiştir. İnternet, denetlenemeyen bir sanal dünyadır; saldırganlar, bilgiye ulaşmak için ağların zayıf noktalarını kullanarak yasadışı yollar denemektedir. Kurumlar, kendi ağlarını belirli kurallarla yöneterek ağ güvenlik politikalarını oluşturmalıdır. Bu politikalar, mümkünse sistem kurulmadan önce ve güvenlik sorunu yaşanmadan önce hazırlanmalıdır.  
  
**Ağ Güvenliğinin Sağlanması İçin Gerekli Olan Temel Politikalar**

**1.** **Kabul Edilebilir Kullanım (Acceptable Use) Politikası:**

* Ağ ve bilgisayar kaynaklarının kullanımıyla ilgili olarak kullanıcıların hakları ve sorumluluklarını belirleyen bir politika hazırlamak önemlidir.
* Yazılacak politikada temelde aşağıdaki konular belirlenmelidir:
* Kaynakların kullanımına kimlerin izinli olduğu,
* Kaynakların uygun kullanımının nasıl olabileceği,
* Kimin erişim hakkını vermek ve kullanımı onaylamak için yetkili olduğu,
* Kimin yönetim önceliklerine sahip olabileceği,
* Kullanıcıların hakları ve sorumluluklarının neler olduğu,
* Sistem yöneticilerin kullanıcılar üzerindeki hakları ve sorumlulukların neler olduğu,
* Hassas bilgi ile neler yapılabileceği.

**2. Erişim Politikaları**

* Erişim stratejileri, kullanıcıların ağa bağlanma haklarını düzenler. Her bir kullanıcının özelleştirilmiş ağ erişim yetkileri olmalıdır. Kullanıcıları gruplara ayırdıktan sonra, erişim politikaları her kategori için ayrı ayrı belirlenmelidir.
* Bu kategoriler arasında sistem yöneticileri de bulunmaktadır. Sistem yöneticileri için erişim kuralları belirlenmemesi durumunda, bazı kuralların sistem yöneticisinin inisiyatifine bırakılması, güvenlik açıklarıyla sonuçlanabilir. Bu, istenmeyen güvenlik zafiyetlerine yol açabilir.

**3.Ağ Güvenlik Duvarı (Firewall) Politikası**

* Ağ güvenlik bariyeri (network firewall), şirketin ağı ile dış ağlar arasında bir köprü vazifesi gören ve İnternet bağlantısındaki potansiyel sorunları çözmek üzere geliştirilmiş çözümlerdir.
* Güvenlik bariyerleri yalnızca dışarıdan gelen saldırılara karşı koruma sağlamakla kalmaz, aynı zamanda performans arttırıcı ve izin politikası uygulayıcı hedefler için de kullanılırlar.
* Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmektedir:
* Proxy,
* Anti-Virus Çözümleri,
* İçerik Süzme (content filtering,
* Özel Sanal Ağlar (Virtual Private Network-VPN),
* Nüfuz Tespit Sistemleri (Intrusion Detection Systems-IDS).

**4.İnternet Politikası**

* Şirket ölçeğinde her çalışanın dış kaynaklara, yani İnternet'e erişmesi zorunlu değildir. İnternet erişiminin sebep olabileceği sorunlar aşağıdaki gibidir:
* Zararlı kodlar,
* Etkin Kodlar,
* Amaç dışı kullanım,
* Zaman Kaybı

**5.Şifre Yönetimi Politikası**

* Parolalar, kullanıcıların hedefledikleri bilgilere erişim izinlerinin var olup olmadığını anlamamıza yardımcı olan bir kontrol aracıdır. Parolaların yanlış ve kötü niyetli kullanımları, güvenlik sorunlarına yol açabileceği için güvenlik politikalarında önemli bir yer tutar.
* Sistem yöneticileri, kullanıcıların parola seçimlerine gerektiğinde müdahale etmelidir. Kullanıcılar, basit ve kolay tahmin edilebilir parolalar seçmemeleri konusunda bilinçlendirilmeli ve programlar aracılığıyla zayıf parolalar tespit edilip kullanıcılar uyarılmalıdır.
* Ayrıca kurumlar güvenlik politikalarında şifre seçimi ile ilgili aşağıdaki kısıtlamaları belirleyebilmektedirler:
* Şifrenin boyutu ve içeriği,
* Süre dolması (eskime) politikası,
* Tek kayıt ile her şeye erişim (Single Sign On-SSO) politikası.

**6.Fiziksel Güvenlik Politikası**

* Bilgisayar veya etkin cihazlara fiziksel olarak ulaşabilen saldırganın, cihazın kontrolünü kolayca ele geçirebileceği göz ardı edilmemelidir. Ağ bağlantısına ulaşabilen saldırgan, kabloya özel ekipman kullanarak (tapping) hat üzerinde dinleme yapabilir veya hatta trafik gönderebilir.
* Açıkça ifade edilmelidir ki fiziksel güvenlik ihmal edildiğinde, alınacak yazılımsal güvenlik önlemlerinin hiçbir değeri olmayacaktır.

**7. Sosyal Mühendislik Politikası**

* Sosyal manipülasyon, bireyleri kandırma yöntemleriyle istediğini yaptırma ve kullanıcıya ait bilgileri elde etme eylemidir. Sistem sorumlusu olduğunu iddia ederek kullanıcının şifresini öğrenmeye çalışmak veya teknisyen kılığında kurumun içine fiziksel olarak sızmak veya çöp konteynerlerini karıştırarak bilgi toplamak gibi çeşitli yöntemlerle gerçekleştirilebilir.
* Kurum çalışanları, kimliğini doğrulamayan kişilere kesinlikle bilgi vermemeli ve iş hayatını özel hayatından ayırmalıdır. Kurum politikasında bu tür durumlarla ilgili gerekli uyarılar yapılmalı ve önlemler alınmalıdır.

**8.Sürekli İyileştirme**

* İzleme sistemleri kullanarak ağ ve sistem aktivitelerini sürekli olarak takip edilmelidir.
* Periyodik denetimler yaparak veri güvenliği standartlarının uygunluğunu değerlendirilmelidir.

**SONUÇ:**

Bilgisayar ağlarında güvenlik politikalarının hayati bir rol oynaması kaçınılmazdır. Kurumsal güvenliğin temeli, öncelikle yazılı kuralların belirlenmesidir. Bir güvenlik politikası oluşturmanın anahtarı, başarılı bir planlamadır. Güvenlik politikası oluşturulurken, kurumsal ihtiyaçları belirlemek için kurumun en temel düzeylerine kadar inilmelidir. Oluşturulan politikaların titizlikle uygulanması elzemdir. Güvenlik politikasının etkili olabilmesi için üst yönetimden gerekli destek sağlanmalı ve çalışanlar, benimsenen politikalar hakkında bilinçlendirilmelidir. Güvenlik politikaları, sabit kurallar olmayıp değişen bir dinamiktir. Politika, sürekli değişen tehditlere, zayıflıklara ve kurumsal politikalara göre düzenli olarak gözden geçirilmeli ve gerekli adapte edilmelidir.

**VERİ GÜVENLİĞİ**

**Veri Güvenliği Nedir?**

Veri güvenliği standartları, organizasyonların sahip oldukları bilgilerin gizliliği, bütünlüğü ve erişilebilirliğini korumak için benimsedikleri politikalar, prosedürler ve teknik yaklaşımlardır. Bu standartlar, bilgi ihlallerini önleme, itibarı koruma ve mevzuata uyum sağlama konularında yardımcı olur. Veri güvenliği standartlarının belirlenmesi ve sürdürülmesi, organizasyonun büyüklüğüne, faaliyet alanına ve sahip olduğu verilerin hassasiyetine göre değişebilir. Ancak, genel olarak şu adımları içerir:

**1.Veri Varlıklarının Belirlenmesi**

* Veri güvenliği standartları, organizasyonun sahip olduğu tüm veri varlıklarını kapsamalıdır. Bu nedenle, ilk adım, veri varlıklarının bir listesini oluşturmaktır. Bu liste, kişisel bilgiler, finansal veriler, müşteri bilgileri ve ticari sırlar gibi hassas verileri içermelidir.

**2.Veri Risklerinin Belirlenmesi**

* Veri varlıkları belirlendikten sonra, bu varlıklara yönelik riskler tanımlanmalıdır. Doğal afetler, insan hataları, siber saldırılar ve teknolojik hatalar gibi çeşitli faktörlerden kaynaklanan riskler değerlendirilmelidir.

**3.Risk Azaltma Stratejilerinin Geliştirilmesi**

* Tanımlanan risklere yönelik olarak, riskleri azaltmak için stratejiler geliştirilmelidir. Bu stratejiler, teknik önlemler, yönetim önlemleri ve eğitim gibi çeşitli unsurları içerebilir.

**4.Veri Güvenliği Standartlarının Oluşturulması**

* Risk azaltma stratejileri doğrultusunda, veri güvenliği standartları oluşturulmalıdır. Bu standartlar, verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak için gereken politikaları, prosedürleri ve teknikleri içermelidir.

**5.Standart Uygulanması ve Sürdürülmesi**

* Veri güvenliği standartları oluşturulduktan sonra, bu standartların uygulanması ve sürdürülmesi gerekir. Bu, standartlara uygunluğun düzenli olarak değerlendirilmesini ve güncellemelerin yapılmasını içerir.

**6.İzleme ve Müdahale**

* Veri güvenliği politikalarının etkinliğini gözlemleyin.
* Bilgi erişim kayıtlarını periyodik olarak gözden geçirin ve anormal faaliyetleri tespit ederek müdahalede bulunun.

**SONUÇ:**

Veri güvenliği standartlarının belirlenmesi ve sürdürülmesi, karmaşık ve sürekli bir süreçtir. Ancak, bu süreci doğru bir şekilde yürütmek, organizasyonların veri ihlallerini önlemesine ve veri güvenliğini sağlamasına yardımcı olabilir.

Veri güvenliği standartları belirlenirken ve sürdürülürken dikkat edilmesi gereken bazı noktalar şunlardır:

* Standartlar, organizasyonun ihtiyaçlarına ve hedeflerine uygun olmalıdır.
* Standartlar, uygulanabilir ve sürdürülebilir olmalıdır.
* Standartlar, organizasyonun tüm çalışanları tarafından bilinmelidir.

Veri güvenliği standartlarının belirlenmesi ve sürdürülmesi, organizasyonun veri güvenliğini sağlamada önemli bir adımdır. Bu süreci doğru bir şekilde yürüterek, organizasyonların veri ihlallerini önlemesine ve itibarını korumasına yardımcı olunabilir.

Formun Üstü

**GÜVENLİK DENETİMLERİ VE TESTLERİ**

**Ağ Güvenliği Denetimleri**

Ağ güvenliği denetimleri, bir ağdaki güvenlik açıklarını ve zayıflıkları tespit etmek ve bunlara karşı önlemler almak için yapılan çalışmalardır. Bu denetimler, ağ güvenliğini sağlamak ve ağdaki hassas verilerin korunmasını sağlamak için çok önemlidir.

Ağ güvenliği denetimlerinin önemi şu şekilde sıralanabilir:

* Ağdaki güvenlik açıklarını ve zayıflıkları tespit ederek, olası saldırıları önlemeye yardımcı olur.
* Ağ güvenliği politikalarının ve prosedürlerinin etkinliğini değerlendirir.
* Ağdaki güvenlik farkındalığını artırır.
* Ağ güvenliğinin iyileştirilmesi için gerekli önerileri sunar.

Ağ güvenliği denetimleri, aşağıdaki aşamalardan oluşur:

* **Planlama ve hazırlık aşaması:** Bu aşamada, denetimin kapsamı, hedefleri ve yöntemleri belirlenir.
* **Uygulama aşaması:** Bu aşamada, belirlenen yöntemler kullanılarak denetim gerçekleştirilir.
* **Raporlama aşaması:** Bu aşamada, denetim bulguları ve önerileri raporlanır.

Ağ güvenliği denetimleri, bir ağdaki güvenlik açıklarını ve zayıflıkları tespit etmek için çeşitli yöntemler kullanılarak gerçekleştirilebilir. Bu yöntemler arasında, şunlar sayılabilir:

* **Dosya ve sistem denetimleri:** Bu denetimler, ağdaki sistemlerin ve dosyaların güvenliğini değerlendirir.
* **Ağ trafiği analizi:** Bu denetimler, ağ trafiğini analiz ederek olası saldırıları tespit eder.
* **Zafiyet taraması:** Bu denetimler, ağdaki sistemlerde ve uygulamalarda bulunan güvenlik açıklarını tespit eder.
* **Güvenlik farkındalığı eğitimi:** Bu eğitimler, ağ kullanıcılarının güvenlik farkındalığını artırır.

Ağ güvenliği denetimleri, düzenli olarak gerçekleştirilmelidir. Bu sayede, ağdaki güvenlik açıkları ve zayıflıkları zamanında tespit edilerek, olası saldırılar önlenebilir.

Ağ güvenliği denetimlerinin nasıl gerçekleştirileceği konusunda, aşağıdaki hususlara dikkat edilmesi gerekir:

* Denetimler, deneyimli ve yetkin kişiler tarafından gerçekleştirilmelidir.
* Denetimler, kapsamlı ve detaylı olmalıdır.
* Denetimler, düzenli olarak gerçekleştirilmelidir.

**SONUÇ:**

Ağ güvenliği denetimleri, bir ağdaki güvenliği sağlamak için önemli bir araçtır. Bu denetimlerin düzenli olarak gerçekleştirilmesi, ağdaki hassas verilerin korunmasını ve olası saldırıların önlenmesini sağlar.

**AĞ GÜVENLİĞİ TESTLERİ**

Ağ güvenliği testleri, bir organizasyonun bilgi sistemlerini ve ağ altyapısını değerlendirmek, potansiyel güvenlik açıklarını belirlemek ve genel ağ güvenliği seviyesini artırmak amacıyla kullanılan çeşitli teknik yöntemleri içerir. Ağ güvenliği testlerinin türleri ve sağladığı avantajlar aşağıda sıralanmıştır:

**1.İçerik Denetim ve Filtreleme Testi**

* İnternet trafiğini izleyerek, içerik filtreleme çözümlerini test eder.
* Zararlı içerikleri ve kötü amaçlı trafiği engelleyip engellemediğini kontrol eder.
* Filtreleme politikalarını ve ayarlarını değerlendirir.

**Faydaları:**

* Zararlı içeriği engelleyerek siber saldırıları önler.
* Veri sızıntılarını önler ve hassas bilgilerin korunmasına katkıda bulunur.
* İnternet kullanım politikalarına uyumu değerlendirir.
* Filtreleme performansını test eder, phishing ve spam içeriklerini tespit eder.

**2.Zafiyet Tarama(Vulnerability Scanning)**

* Bilgisayar ağlarındaki IP adreslerini ve bağlı cihazları tarar.
* Ağda çalışan yazılımların ve işletim sistemlerinin güvenlik açıklarını tespit eder.
* Otomatik araçlar, geniş ağları hızlı bir şekilde tarayarak zafiyetleri sıralar.

**Faydaları:**

* Hızlı ve otomatik tarama imkanı sağlar.
* Bilinen zafiyetleri hızlı bir şekilde tespit eder.
* Sürekli izleme ve tarama imkanı sunar.

**3.Penetrasyon Testi (Penetration Testing)**

* Saldırıcıların bakış açısından ağı test eder; manuel ve otomatik metodlar kullanılabilir.
* Gerçek saldırı senaryolarını simüle eder, böylece organizasyonun savunma mekanizmalarını test eder.
* Sistemlere ve uygulamalara yönelik zayıflıkları tespit eder ve bunları sömürerek test eder.

**Faydaları:**

* Gerçek dünya saldırılarını simüle ederek, organizasyonun güvenlik açıklarını tespit eder.
* İnsan faktörünü değerlendirir.
* Özel güvenlik önlemlerini test eder.

**4.Denial-of-Service (DoS) Saldırı Testi**

* Ağ altyapısının dayanıklılığını ve performansını ölçmek amacıyla DoS saldırıları simüle eder.
* Ağa aşırı trafik göndererek servis kesintilerini test eder.
* Yük testi yaparak ağın maksimum kapasitesini belirler.

**Faydaları:**

* Ağın dayanıklılığını ve sürdürülebilirliğini test eder.
* Servis kesintilerine karşı organizasyonun tepkisini değerlendirir.
* DoS saldırılarına karşı savunma önlemlerini test eder.

**5.Web Uygulama Güvenliği Testi**

* Web uygulamalarındaki güvenlik açıklarını tespit etmek amacıyla, uygulama katmanında testler yapar.
* SQL enjeksiyonu, cross-site scripting (XSS), güvensiz oturum yönetimi gibi zafiyetleri değerlendirir.
* Web uygulamalarını güvenlik standartlarına uygunluğunu kontrol eder.

**Faydaları:**

* Web uygulamalarındaki yaygın güvenlik açıklarını tespit eder.
* Müşteri verilerini koruma açısından kritik öneme sahiptir.
* Web uygulama geliştiricilerine eğitim ve bilgi sağlar.

**6.İç Denetim ve İzleme**

* Ağ içindeki trafiği ve aktiviteleri izler.
* Yetkisiz erişimleri ve anormal aktiviteleri tespit eder.
* İç ağda yer alan sistemlerin ve kullanıcıların güvenlik politikalarına uygunluğunu kontrol eder.

**Faydaları:**

* İç tehditlere karşı daha etkin bir koruma sağlar.
* Güvenlik politikalarına uyulup uyulmadığını değerlendirir.

**7.Kara Kutu ve Beyaz Kutu Testleri**

* Kara kutu testi, test eden ekibin sistem hakkında önceden hiçbir bilgiye sahip olmadığı durumu simgeler.
* Beyaz kutu testi, test eden ekibin sistem hakkında detaylı bilgi sahibi olduğu bir durumu simgeler.
* Her ikisi de farklı bakış açıları sunar.

**Faydaları:**

* Kara kutu testleri, gerçek dünya saldırı senaryolarını simüle eder.
* Beyaz kutu testleri, iç ağ yapılarını daha ayrıntılı bir şekilde inceleyerek özel güvenlik önlemlerini test eder.

**8.Kablo Ağ Güvenliği Testi**

* Kablosuz ağlardaki güvenlik açıklarını değerlendirir.
* Sızma testleri ve şifre kırma gibi teknikleri kullanarak kablosuz ağlardaki riskleri belirler.

**Faydaları:**

* Kablosuz ağlardaki zafiyetleri tespit eder.
* Kötü niyetli kullanıcıların veya cihazların ağa sızma olasılığını değerlendirir.

**9.Fiziksel Güvenlik Testi**

* Fiziksel güvenlik önlemlerini değerlendirir.
* Güvenlik kameraları, erişim kontrol sistemleri, server odaları gibi fiziksel güvenlik unsurlarını test eder.

**Faydaları:**

* Fiziksel erişim kontrolünü test ederek yetkisiz girişlere karşı önlem almayı sağlar.
* Fiziksel güvenlik önlemlerinin etkinliğini değerlendirir.

**SONUÇ:**

**Ağ Güvenliği Testlerinin Genel Faydaları:**

* Güvenlik açıklarını ve zayıflıkları tespit ederek, olası saldırıları önlemeye yardımcı olur.
* Ağ güvenliği politikalarının ve prosedürlerinin etkinliğini değerlendirir.
* Ağdaki güvenlik farkındalığını arttırır.
* Ağ güvenliğinin iyileştirilmesi için gerekli önerileri sunar.

Ağ güvenliği denetimleri, düzenli olarak gerçekleştirilmelidir. Bu sayede, ağdaki güvenlik açıkları ve zayıflıkları zamanında tespit edilerek, olası saldırılar önlenebilir.

Ağ güvenliği denetimlerinin nasıl gerçekleştirileceği konusunda, aşağıdaki hususlara dikkat edilmesi gerekir:

* Denetimler, deneyimli ve yetkin kişiler tarafından gerçekleştirilmelidir.
* Denetimler, kapsamlı ve detaylı olmalıdır.
* Denetimler, düzenli olarak gerçekleştirilmelidir.

Ağ güvenliği denetimleri, bir ağdaki güvenliği sağlamak için önemli bir araçtır. Bu denetimlerin düzenli olarak gerçekleştirilmesi, ağdaki hassas verilerin korunmasını ve olası saldırıların önlenmesini sağlar.