**AĞ GÜVENLİĞİ**

Ağ güvenliği, temel ağ altyapısının yetkisiz erişime, kötüye kullanıma veya hırsızlığa karşı korunmasıdır. Cihazların, kullanıcıların ve uygulamaların güvenli bir şekilde çalışması için güvenli bir altyapı oluşturulmasını içerir.

Ağ güvenliği nasıl çalışır?

Ağ güvenliği, uçta ve ağda birden fazla savunma katmanını birleştirir. Her ağ güvenlik katmanı politika ve kontrolleri uygular. Yetkili kullanıcılar ağ kaynaklarına erişim sağlar, ancak kötü niyetli etkinliklerin açıklardan yararlanma ve tehdit gerçekleştirmeleri engellenir.

Uygulanan ileri teknoloji nedeniyle yeni teknikler ortaya çıktıkça ağ dünyası hızla büyüyor. İnternet erişim hizmeti için, son kullanıcılar veya kuruluşlar tarafından İnternet hizmetine erişmek için eski yöntem ve teknikler hala kullanılmaktadır. En sık kullanılan hizmetlerden biri Ethernet üzerinden Noktadan Noktaya (PPPoE) hizmettir. Bununla birlikte, Parola Doğrulama Protokolü (PAP), kimlik doğrulamaya duyarlı verilerin, ağda veri dinleme ve dinleme yeteneğine sahip herhangi bir hileli yazılım aracı kullanılarak kolaylıkla istismar edilebileceği veya ele geçirilebileceği bir güvenlik kusuru içerir. Bu hassas veriler görüntülenebilir ve yetkisiz bir erişimin arkasına geçmesine izin vermek için yeniden kullanılabilir. Buna göre, (PAP) hala birçok ISP'de PPPoE hizmeti ile ana kimlik doğrulama protokolü olarak kullanılmaktadır. Ancak, daha yeni alanlarda uygulanan IPsec donanım hızlandırma tekniğinin büyümesiyle; modası geçmiş servislerin değiştirilmesine ihtiyaç vardır. Tüm ağ için daha iyi kararlılık, uçtan uca veri şifreleme ve koruma sunar. Bu belge, İnternet erişim hizmeti sunan ana yönlendirici içindeki IPsec şifreleme ve şifre çözme işlemlerini hızlandırmak ve önceliklendirmek için donanım hızlandırma tekniğini kullanma girişimidir. Donanım hızlandırma tekniği, şifreleme ve şifre çözme işlemlerinde çok büyük bir role sahiptir, daha fazla çip gücü ve enerjisi tüketmeden hızlı işlemleri sunar. Böylece bağlantı oturumlarının gecikmeden ve kesintiye uğramadan aktif kalması sağlanır. Artık kullanılmayan PPPoE çevirmeli bağlantı hizmetinin yerine kullanılmasına ihtiyaç vardır.

Ağ güvenliği, sürdürülebilir bir yapının varlığına atıfta bulunan bir sistemi ifade etmektedir. Temel olarak kurulan bir yapının, uzun süre boyunca devam edebilmesi ve kesin güvenlik sağlaması adına önem arz eden temel husus, sistemin neredeyse her gün güncel olarak takip edilmesidir.

**Ağ Güvenliği Uygulamalarının ve Araçlarının Önemi**

Ağ güvenliği uygulamalarına ihtiyaç duymamızın nedenleri:

* **Veri Koruma:** İşletmeler ve bireyler, hassas bilgilerini (müşteri verileri, finansal bilgiler, ticari sırlar vb.) çeşitli tehditlere karşı korumak isterler. Ağ güvenliği uygulamaları, bu verileri yetkisiz erişimlere ve saldırılara karşı korur.
* **Hizmet Sürekliliği:** Ağ saldırıları, hizmet reddi saldırıları (DoS/DDoS) gibi tehditler, işletmelerin veya kuruluşların online hizmetlerini etkileyebilir. Ağ güvenliği uygulamaları, bu tür saldırılara karşı koruma sağlayarak hizmet sürekliliğini artırır.
* **Kurumsal itibarın Korunması:** Bilgi güvenliği ihlalleri, bir organizasyonun itibarını zedeleme potansiyeline sahiptir. Müşteri güvenini kaybetmek, finansal zararlara yol açabilir. Ağ güvenliği, bu tür olumsuz etkileri önlemeye yardımcı olur.
* **Yasal ve Düzenleyici Uyum:** Birçok sektör, belirli güvenlik standartlarına uymak zorundadır. Ağ güvenliği uygulamaları, bu düzenlemelere uyumu sağlamak ve yasal gereksinimlere uygunluğu güvence altına almak için kullanılır.
* **Finansal Kayıpların Önlenmesi:** Bilgisayar korsanlığı, fidye yazılım saldırıları, veri kaybı gibi güvenlik ihlalleri, organizasyonlara ciddi finansal zararlar verebilir. Ağ güvenliği uygulamaları, bu tür kayıpları en aza indirerek maliyet etkin bir güvenlik sağlar.
* **Çalışan Verimliliği ve Güvenliği:** İşyerlerinde kullanılan ağlar, çalışanların güvenli bir şekilde işlerini yapmalarını sağlamak için korunmalıdır. Ağ güvenliği uygulamaları, çalışanların bilgisayar korsanları, zararlı yazılımlar veya veri sızıntıları gibi tehditlere maruz kalma riskini azaltır.
* **Zaman ve Kaynak Tasarrufu:** Ağ güvenliği uygulamaları, otomatik tehdit algılama ve müdahale sistemleri kullanarak, güvenlik olaylarını daha hızlı ve etkili bir şekilde ele almaya yardımcı olabilir. Bu da organizasyonlara zaman ve kaynak tasarrufu sağlar.

Genel olarak ağ güvenliği uygulamaları modern dünyada artan dijital tehditlere karşı savunma oluşturarak veri güvenliğini sağlamak, hizmetleri sürekli kılmak ve kurumsal riskleri azaltmak için çok önemlidir.

Güvenlik duvarları, IDS/IPS, antivirüs yazılımları gibi temel güvenlik uygulamalarının önemi: Potansşyel güvenlik sistemlerini veya yetkisiz erişimi gerçek zamanlı olarak tespit edebilen sistemlerdir. Bu sayede gelen zararlı yazılımların erişimini engelleyerek bilgisayarımızın güvende kalmasını sağlar.

**Sızma Önleme Sistemleri (IPS) ve Sızma Algılama Sistemleri (IDS):**

* Potansiyel güvenlik tehditlerini veya yetkisiz erişimi gerçek zamanlı olarak tespit edebilen sistemlerdir.

Ağ Güvenliği Politikalarının Uygulanması ve Oluşturulması İçin Temel Adımlar

Kriptografi ve şifrelemenin önemi:

Kriptografi ve şifreleme araçları, bilgi güvenliğini sağlamak, verileri gizlemek ve iletişimi korumak için kullanılan önemli araçlardır. İşte kriptografi ve şifrelemenin kullanımı ve önemine dair temel bilgiler:

* **Veri Güvenliği:**
  + **Kriptografinin Rolü:** Kriptografi, verilerin anlaşılmasını zorlaştırarak, yetkisiz erişimlere karşı koruma sağlar. Şifreleme, verileri şifreleyerek anlaşılmasını engeller.
* **Gizlilik Sağlama:**
  + **Kriptografinin Rolü:** Kriptografi, özellikle hassas bilgilerin iletilmesi sırasında gizliliği sağlar. İletilen veriler şifrelenerek, sadece doğru anahtara sahip olan kişiler tarafından anlaşılabilir.
* **İkimiz Arasında Güvenli İletişim:**
  + **Kriptografinin Rolü:** İki taraf arasındaki iletişimi güvenli hale getirmek için kriptografi kullanılır. Bu, özellikle çevrimiçi bankacılık, e-ticaret ve diğer hassas veri transferlerinde önemlidir.
* **Veri Bütünlüğünü Sağlama:**
  + **Kriptografinin Rolü:** Kriptografi, veri bütünlüğünü korur. Şifrelenmiş verilerin üzerinde yapılan değişiklikler, şifre çözülemediği sürece algılanabilir.
* **Yetkilendirme ve Kimlik Doğrulama:**
  + **Kriptografinin Rolü:** Kriptografi, kullanıcı kimliklerini doğrulamak ve yetkilendirmek için kullanılır. Güvenli kimlik doğrulama süreçleri genellikle şifreleme içerir.
* **Ağ Güvenliği:**
  + **Kriptografinin Rolü:** Ağ trafiğini şifreleyerek, ağ üzerindeki iletişimi korur. Bu, VPN'ler veya güvenli iletişim protokollerinin kullanımını içerir.
* **Güvenli Depolama:**
  + **Kriptografinin Rolü:** Verilerin depolandığı yerlerde şifreleme kullanarak, fiziksel veya sanal saldırılara karşı güvenli depolama sağlanır.
* **Uyumluluk ve Yasal Gerekliliklere Uyum:**
  + **Kriptografinin Rolü:** Bazı sektörlerde, şifreleme uygulamak, veri güvenliği yasalarına ve uyumluluk gereksinimlerine uyum sağlamak anlamına gelir.
* **Çeşitli Şifreleme Algoritmaları:**
  + **Simetrik ve Asimetrik Şifreleme:** Simetrik şifreleme, aynı anahtarın hem şifreleme hem de şifre çözme için kullanıldığı bir yöntemdir. Asimetrik şifreleme ise bir çift anahtar kullanır: biri şifreleme için, diğeri ise şifre çözme için.
  + **Hibrid Şifreleme:** Simetrik ve asimetrik şifreleme yöntemlerini birleştiren bir yaklaşım.
  + **AES (Advanced Encryption Standard):** Genellikle simetrik şifreleme için kullanılan bir standart.
  + **RSA, ECC (Elliptic Curve Cryptography):** Asimetrik şifreleme için kullanılan popüler algoritmalar.
* **Siber Saldırılara Karşı Koruma:**
  + **Kriptografinin Rolü:** Şifreleme, veri sızıntıları, ransomware saldırıları ve diğer siber saldırılara karşı etkili bir savunma sağlar.

Kriptografi ve şifreleme, modern bilgi teknolojilerinde temel bir güvenlik unsurudur. Bu teknolojilerin etkili bir şekilde uygulanması, organizasyonların bilgi varlıklarını korumalarına ve güvenli bir iletişim ortamı sağlamalarına yardımcı olur.

:

Ağ Güvenliği Politikaları

Ağ güvenliği politikaları, bir kuruluşun bilgisayar ağı içindeki bilgi ve kaynakların gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak için belirlenmiş kurallar ve yönergelerdir. Bu politikalar, güvenilmeyen erişimlere, veri ihlallerine ve diğer siber tehditlere karşı koruma sağlamak için güvenlik önlemlerini ve uygulamalarını tanımlar. Genellikle aşağıdaki ana bileşenleri içerir:

* **Erişim Kontrol Politikaları:**
  + Kullanıcı rollerini ve izinleri tanımlar.
  + Belirli ağ kaynaklarına kimlerin erişebileceğini belirtir.
  + Erişim haklarının verilmesi ve geri alınması için prosedürleri belirler.
* **Kimlik Doğrulama ve Yetkilendirme:**
  + Kullanıcı kimlik doğrulama yöntemlerini tanımlar (şifreler, çok faktörlü kimlik doğrulama vb.).
  + Yetkilendirmenin kullanıcı rolleri ve sorumluluklarına dayalı olarak nasıl sağlanacağını belirtir.
* **Güvenlik Duvarı Kuralları ve Yapılandırma:**
  + Gelen ve giden ağ trafiğini yönetmek için kuralları tanımlar.
  + Güvenlik duvarlarının yetkisiz erişimi filtrelemek ve engellemek için nasıl yapılandırılacağını belirtir.
* **Şifreleme Politikaları:**
  + Verinin iletim sırasında ve dinlenirken korunması için şifreleme protokollerini tanımlar.
  + Hangi şifreleme algoritmalarının ve anahtar yönetimi uygulamalarının kullanılacağını belirtir.
* **Olay Yanıtı ve Raporlama:**
  + Güvenlik olaylarını tespit etme ve yanıtlama prosedürlerini belirler.
  + Güvenlik ihlalleri ve yetkisiz erişim için raporlama gereksinimlerini tanımlar.
* **Ağ İzleme ve Günlükleme:**
  + Ağ faaliyetlerini izlemek için politikaları belirler.
  + Hangi bilgilerin kaydedileceğini ve günlük verilerinin ne kadar süreyle saklanacağını belirtir.
* **Mobil Cihaz ve Uzak Erişim Güvenliği:**
  + Ağa erişim sağlayan mobil cihazlar için güvenlik önlemlerini belirler.
  + VPN kullanımı gibi güvenli uzaktan erişim için politikaları tanımlar.
* **Yama Yönetimi:**
  + Yazılım, işletim sistemleri ve ağ cihazlarını en son güvenlik yamalarıyla güncel tutma prosedürlerini belirler.
* **Zayıflık Yönetimi:**
  + Zayıflıkların nasıl tanımlandığını, değerlendirildiğini ve hafifletildiğini belirler.
  + Zayıflık değerlendirmeleri ve taramalarının sıklığını belirtir.
* **Fiziksel Güvenlik:**
  + Ağ altyapısına fiziksel erişimi güvence altına almak için önlemleri içerir.
  + Veri merkezleri, sunucu odaları ve ağ ekipmanları için güvenlik kontrollerini belirtir.
* **Kullanıcı Eğitimi ve Farkındalık:**
  + Çalışanlar arasında güvenlik farkındalığını teşvik eder.
  + Güvenli çevrimiçi davranışlar ve sosyal mühendislik saldırılarını tanıma konusunda yönergeler sağlar.
* **Uyumluluk ve Hukuki Gereklilikler:**
  + Ağ güvenliği politikalarının ilgili yasalara ve düzenlemelere uygunluğunu sağlar.
  + Denetimler ve uyumluluk değerlendirmeleri için prosedürleri belirler.

Etkili ağ güvenliği politikaları, güvenli ve dayanıklı bir IT altyapısını sürdürmek için hayati öneme sahiptir. Bu politikaların düzenli olarak gözden geçirilmesi ve güncellenmesi, değişen siber tehditlere ve teknoloji değişikliklerine uyum sağlamak açısından önemlidir.

Ağ Güvenliği Politikalarının Oluşturulması ve Uygulanması İçin Temel Adımlar:

Ağ güvenliği politikalarının oluşturulması ve uygulanması, bir organizasyonun bilgi varlıklarını koruma ve siber tehditlere karşı etkili bir savunma oluşturma sürecini içerir.

* **Risk Analizi ve Değerlendirme:**
  + Belirli bir organizasyonun güvenlik ihtiyaçlarını anlamak ve yönetmek için bir risk analizi yapılmalıdır. Bu analiz, potansiyel tehditleri, zayıflıkları ve riskleri değerlendirmelidir.
* **Hedef Belirleme:**
  + Ağ güvenliği politikalarının amacını ve hedefleri belirlenir. Bu hedefler, organizasyonun genel stratejilerine ve iş gereksinimlerine dayanmalıdır.
* **Personel Katılımı ve Eğitimi:**
  + Ağ güvenliği politikalarının başarıyla uygulanabilmesi için personelin bu politikaları anlaması ve benimsemesi kritiktir. Personel eğitim programları düzenlenilmeli ve güvenlik bilincini artırmak için uğraşılmalı.
* **Standartlar ve Uyumluluk:**
  + Ağ güvenliği politikaları, ilgili endüstri standartlarına ve yasal düzenlemelere uygun hale getirilmeli. Uyumluluk, organizasyonun yasal gereksinimlere uyumunu sağlar.
* **Güvenlik İlkelerinin Oluşturulması:**
  + Temel güvenlik prensiplerini belirlenir. Bu prensipler; bilgi gizliliği, bütünlüğü, erişilebilirliği, güvenliği ve sorumlulukları içermelidir.
* **Veri Sınıflandırma ve Koruma:**
  + Organizasyon içindeki verileri sınıflandırın ve önem düzeylerine göre koruma seviyeleri belirlenilmelidir. Duyarlı verilerin nasıl ele alınacağına dair politikalar oluşturulur.
* **Yetkilendirme ve Erişim Kontrolleri:**
  + Kullanıcıların ve sistemlerin ağ kaynaklarına erişimini düzenleyen politikalar oluşturun. İhtiyaca göre en az ayrıcalığı uygulayarak prensibi benimseyin.
* **Ağ İzleme ve Güvenlik İncelemeleri:**
  + Ağ trafiğini izleme, güvenlik olaylarını belirleme ve düzenli güvenlik incelemelerini yapma politikalarını uygulayın. Bu, güvenlik açıklarını ve tehditleri tespit etmek için önemlidir.
* **Saldırı Önleme ve Tepki Planları:**
  + Potansiyel saldırılara karşı önleyici tedbirleri ve müdahale planlarını içeren politikalar oluşturun. Olaylara hızlı bir şekilde tepki verebilecek bir plan hazırlayın.
* **Güvenlik Yazılım ve Donanım Politikaları:**
  + Güvenlik duvarları, antivirüs yazılımları, güvenlik yamaları ve diğer güvenlik araçlarının kullanımını düzenleyen politikaları belirleyin.
* **Mobil Cihaz Yönetimi:**
  + Kurumsal ağa bağlı mobil cihazlar için güvenlik politikaları oluşturun. Bu, mobil cihazların güvenliğini sağlamak ve yetkilendirilmemiş erişimi önlemek içindir.
* **İletişim ve Bilgi Akışı:**
  + İletişim kanallarını güvence altına almak için şifreleme ve güvenli iletişim politikalarını oluşturun. Bu, hassas bilgilerin güvenli bir şekilde iletilmesini sağlar.
* **Güvenlik Olaylarının Yönetimi:**
  + Güvenlik olaylarına nasıl tepki verileceğini belirleyen ve olayların nasıl yönetileceğini düzenleyen politikaları oluşturun.
* **Sürekli İyileştirme ve Değerlendirme:**
  + Politikaları düzenli olarak gözden geçirin, güncelleyin ve değerlendirin. Yeniliklere ve değişen tehdit ortamlarına uyum sağlamak için sürekli iyileştirmeyi benimseyin.

Ağ güvenliği politikalarının etkili bir şekilde oluşturulması ve uygulanması, organizasyonun güvenlik seviyesini artırmak ve bilgi varlıklarını korumak için kritik bir adımdır.

Veri Güvenliği Standartlarının Belirlenmesi ve Sürdürülebilmesi

Veri güvenliği standartlarını belirlemek ve sürdürmek, bir organizasyon içinde hassas bilgileri korumanın kritik bir yönüdür.

* **Veri Türlerini Belirle ve Duyarlılık Sınıflandırmasını Yap:**
  + Organizasyonunuzun ele aldığı veri türlerini anlayın (örneğin, müşteri bilgileri, finansal veriler, fikri mülkiyet). Veriyi duyarlılık ve kritiklik temelinde sınıflandırın.
* **Hukuki ve Düzenleyici Uyumluluk:**
  + Veri güvenliği ve gizliliği üzerine etkili olan ilgili yasalar ve düzenlemelere uygunluğu sağlayın (örneğin, GDPR, HIPAA, CCPA). Endüstrinizde veri koruma için yasal gereksinimleri anlayın.
* **Veri Sahipliği ve Sorumlulukları Tanımla:**
  + Veri sahipliği için rolleri ve sorumlulukları net bir şekilde tanımlayın. Belirli türdeki verilerin oluşturulması, erişimi, değiştirilmesi ve silinmesinden kimin sorumlu olduğunu belirtin.
* **Veri Güvenliği Politikaları:**
  + Kabul edilebilir kullanımı, işleme prosedürlerini, şifreleme standartlarını ve veri erişimi için yönergeleri içeren kapsamlı veri güvenliği politikaları oluşturun. Politikaların endüstri en iyi uygulamalarına uygun olduğundan emin olun.
* **Şifreleme Standartları:**
  + Hem veri iletimi sırasında hem de veri dinlenirken şifreleme standartlarını belirleyin. Hassas bilgileri şifrelemek için protokollerinizi belirleyin ve depolanan veri için şifreleme algoritmalarını uygulayın.
* **Erişim Kontrolleri ve Kimlik Doğrulama:**
  + Rol ve sorumluluklara dayalı olarak veri erişimini sınırlamak için erişim kontrolleri uygulayın. Kullanıcı kimliğini doğrulamak için çok faktörlü kimlik doğrulama (MFA) gibi güçlü kimlik doğrulama yöntemlerini kullanın.
* **Veri Retansiyonu ve Bertaraf Politikaları:**
  + Verilerin ne kadar süreyle saklanacağını ve yaşam döngüsünün sonunda nasıl güvenli bir şekilde bertaraf edileceğini belirten politikalar oluşturun. Retansiyon politikalarını düzenli olarak gözden geçirin ve güncelleyin.
* **Ağ Güvenliği Önlemleri:**
  + Veri iletimi sırasında veriyi korumak için ağ güvenliği önlemleri uygulayın. Bu, güvenlik duvarları, sızma tespit/saldırı önleme sistemleri ve sanal özel ağlar (VPN'ler) gibi unsurları içerir.
* **Uç Nokta Güvenliği:**
  + Uç noktaları (bilgisayarlar, mobil cihazlar) güncellenmiş antivirüs yazılımı, uç nokta koruma çözümleri ve güvenlik yamalarıyla güvence altına alın. Organizasyon içinde güvenli mobil cihaz kullanımı için politikaları uygulayın.
* **İzleme ve Denetleme:**
  + Yetkisiz erişimi veya şüpheli aktiviteleri tespit etmek için izleme sistemleri kurun. Düzenli denetimler yaparak veri güvenliği standartlarına uygunluğu sağlayın ve potansiyel zafiyetleri belirleyin.
* **Olay Tepki Planı:**
  + Veri ihlalleri veya güvenlik olaylarıyla başa çıkmak için bir olay tepki planı oluşturun ve sürdürün. Çalışanların olay tepki protokollerine eğitildiğinden emin olun.
* **Güvenlik Farkındalığı Eğitimi:**
  + Çalışanlara sürekli güvenlik farkındalığı eğitimi verin. Onları veri güvenliği en iyi uygulamaları konusunda eğitin, hassas bilgilerin korunmasının önemini vurgulayın ve potansiyel güvenlik tehditlerini tanıma konusunda yardımcı olun.
* **Tedarikçi Yönetimi:**
  + Üçüncü taraf tedarikçileriniz verilerinizi işliyorsa, tedarikçi sözleşmelerinde veri güvenliği gereksinimlerini belirleyin. Tedarikçilerin organizasyonunuzun veri güvenliği standartlarına uyum sağlamasını sağlayın.
* **Düzenli Risk Değerlendirmeleri:**
  + Düzenli risk değerlendirmeleri yaparak yeni tehditleri ve zafiyetleri belirleyin. Veri güvenliği standartlarınızı buna göre ayarlayın.

* **Sürekli İyileştirme:**
* Düzenli olarak veri güvenliği standartlarını gözden geçirerek ve güncelleyerek sürekli bir iyileştirme kültürü oluşturun. Yeni teknolojileri, tehditleri ve veri güvenliği alanındaki en iyi uygulamaları takip edin.
* **Belgeleme ve İletişim:**
* Veri güvenliği standartlarını net bir şekilde belgeleyin ve bunları organizasyon genelinde iletişim kurun. Çalışanları düzenli olarak değişiklikler konusunda bilgilendirin ve başvuru kaynakları sağlayın.

Bu adımları takip ederek, organizasyonların sağlam veri güvenliği standartları oluşturmasını sağlarız, veri ihlali riskini azaltabilir ve hassas bilgileri işleme için güvenli bir ortam yaratabiliriz.