AÇIK KAYNAK ARAÇLAR İLE AĞ GÜVENLİĞİ ÖDEVİ

Hazırlayan : Doğukan Yılmaz **410458**

Github : https://github.com/kodkurdu1/AcikKaynakOdevi

AĞ GÜVENLİĞİ POLİTİKALARI

AĞ GÜVENLİĞİ NEDİR ?

Ağ güvenliği politikası, bir organizasyonun veya kurumun bilgi teknolojisi altyapısını güvence altına almak için belirlenen genel prensipler, yönergeler ve uygulamalardan oluşan bir belgedir. Ağ güvenliği politikası, organizasyonun ağ altyapısının güvenliğini temin etmek, bilgi varlıklarını korumak, yetkilendirme ve kimlik doğrulama süreçlerini belirlemek, tehditlere karşı savunma mekanizmalarını kurmak ve çalışanları güvenlik konusunda farkındalık kazandırmak amacıyla oluşturulur.

AĞ GÜVENLİĞİNİN OLUŞTURULMASI İÇİN GEREKEN TEMEL POLİTİKALAR :

Ağ güvenliğinin temel politikaları, bir organizasyonun bilgi teknolojisi altyapısını koruma ve güvence altına alma amacıyla belirlenen genel ilkelerdir. Toplamda 7 adet politika bulunmaktadır onlar da sırayla şu şekildedir ;

1. Kabul Edilebilir Kullanım Politikası (Acceptable Use)

- 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 Politikası

- Ağ güvenliğinin erişim politikası, organizasyonun ağ kaynaklarına güvenli ve yetkilendirilmiş bir şekilde erişimi düzenlemek için belirlenen kuralları içeren bir belgedir. Bu politika, kullanıcı kimlik doğrulama süreçleri, yetkilendirme kuralları ve ağ kaynaklarına erişim kontrol yönergelerini içerir. Ayrıca, erişim politikası, kullanıcıların hangi cihazlardan ve nereden ağa erişebileceği gibi konuları da kapsar.

- Politika, ağ kaynaklarına minimum ayrıcalıklı erişim prensibini benimser ve güvenlik izleme ve değerlendirme süreçlerini içeren bir yaklaşımı destekler. Ayrıca, politika düzenli olarak gözden

geçirilir ve güncellenir, böylece ağ güvenliği olaylarına hazırlıklı olunabilir ve uyumluluk gereksinimlerine uygunluk sağlanabilir.

3. Ağ Güvenlik Duvarı Politikası (Firewall)

Ağ güvenlik duvarı (firewall) politikası, bir organizasyonun ağ güvenliğini sağlamak için belirlediği kurallar ve yönergeleri içeren bir dokümandır. Bu politika, ağ güvenlik duvarının nasıl yapılandırılacağı, hangi trafiğin izin verileceği veya engelleneceği, gelen ve giden verilerin nasıl filtrelenip denetleneceği gibi konuları kapsar. İşte ağ güvenlik duvarı politikasının ana unsurları:

- **Trafik Kontrolü:**
  - İzin verilen ve engellenen ağ trafiğini belirlemek.
  - Belirli protokoller, portlar ve IP adres aralıkları üzerinde kontrol sağlamak.
- **Güvenlik Duvarı Kuralları:**
  - Güvenlik duvarının hangi tür trafiği izleyeceğini ve nasıl tepki vereceğini belirten kuralların tanımlanması.
  - İstisna durumları ve özel durumları içeren kuralların belirlenmesi.
- **İç ve Dış Ağlar Arası Erişim Kontrolü:**
  - İç ağdan dış ağa ve dış ağdan iç ağa erişimi kontrol etme.
  - DMZ (Demilitarized Zone) gibi güvenlik bölgeleri oluşturarak trafiği yönlendirme.
- **Uygulama Katmanı Kontrolleri:**
  - Belirli uygulama katmanı protokollerini ve hizmetlerini kontrol etme.
  - HTTP, FTP, DNS gibi uygulama tabanlı filtreleme.
- **Giriş ve Çıkış Denetimi:**
  - İç ağa giriş ve dış ağa çıkış trafiğini izleme ve kontrol etme.
  - Potansiyel tehditleri engelleyebilmek için giriş ve çıkışlarda filtreleme.
- **Sanal Özel Ağ (VPN) Kontrolleri:**
  - VPN bağlantılarını kontrol etme ve güvenlik standartlarına uygunluğu sağlama.
  - Uzaktan erişim güvenliğini koruma.
- **Günlük Tutma ve İzleme:**
  - Güvenlik duvarı olaylarını izleme ve günlük tutma politikaları.
  - Güvenlik olaylarına hızlı müdahale ve tespit için log kayıtlarını analiz etme.
- **Güncelleme ve Değerlendirme:**
  - Güvenlik duvarı yazılımının ve tanımlarının düzenli olarak güncellenmesi.
  - Politikaların ve kuralların etkinliğinin düzenli değerlendirilmesi.

Bu politika, organizasyonun güvenlik hedeflerine ve ihtiyaçlarına uygun olarak özelleştirilebilir. Ayrıca, hızla değişen tehdit ortamına uyum sağlamak için düzenli olarak gözden geçirilmelidir.

4. İnternet Politikası

İnternet politikası, bir organizasyonun internet kullanımını düzenleyen ve güvenlik risklerini azaltmayı amaçlayan bir belgedir. Bu politika, işle ilgili amaçlara odaklanmayı vurgular, erişim kontrolleri belirler, kötü amaçlı yazılım önlemleri içerir, veri güvenliği standartlarını belirler, sosyal medya kullanımını düzenler, internet trafiğini izler, güvenlik uygulamalarını belirler ve çalışanları eğitmeyi içerir. Politika, organizasyonun güvenlik ihtiyaçlarına uygun olarak düzenli olarak gözden geçirilir ve güncellenir.

- 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 Yönetim Politikası

Şifre yönetimi politikası, bir organizasyonun ağ güvenliğini artırmak ve bilgi varlıklarını korumak amacıyla belirlediği şifre kullanımıyla ilgili kuralları ve yönergeleri içeren bir belgedir.

Bu politika, kullanıcıların güçlü ve benzersiz şifreler oluşturmasını, düzenli şifre değişimini, kimlik doğrulama süreçlerini ve hesap güvenliğini güçlendirmeyi amaçlar. Şifre yönetimi politikası, şifre uzunluğu, karmaşıklığı, değişim sıklığı gibi faktörlere odaklanarak güvenli şifre uygulamalarını belirler. Ayrıca, kullanıcıların şifrelerini güvende tutmaları için güvenlik bilinci oluşturmayı ve şifre unutma/donma durumlarına karşı destek sağlamayı içerir. Politika, organizasyonun güvenlik standartlarına uyumu ve hassas bilgilerin korunmasını sağlamak amacıyla düzenli olarak gözden geçirilir ve güncellenir.

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

Fiziksel güvenlik politikası, bir organizasyonun bilişim sistemlerini, ağ altyapısını ve diğer kritik kaynaklarını fiziksel tehditlere karşı korumayı amaçlayan bir belgedir. Bu politika, organizasyonun fiziksel varlıklarının, bilişim ekipmanlarının ve altyapısının güvenliğini sağlamak için alınması gereken önlemleri belirler. İşte fiziksel güvenlik politikasının ana unsurları:

- **Fiziksel Erişim Kontrolleri:**
  - Bina içine ve özellikle bilgi teknolojisi odalarına erişimi sınırlayan kontrollerin belirlenmesi.
  - Biyometrik tanıma, kart okuma sistemleri gibi güvenli erişim yöntemlerinin kullanılması.
- **Güvenli Alanlar ve Tesisler:**
  - Bilgi teknolojisi altyapısını barındıran alanların güvenlikle korunması.
  - Fiziksel güvenlik ekipmanlarının kullanımı, alarm sistemleri, güvenlik kameraları gibi önlemlerin alınması.
- **Fiziksel İzleme ve Denetim:**
  - Tesislerin güvenlik kameraları ve diğer izleme araçları ile sürekli olarak izlenmesi.
  - Fiziksel güvenlik olaylarını tespit etmek ve önlemek için düzenli denetimlerin yapılması.
- **Hırsızlık ve Zarar Verme Önlemleri:**
  - Ekipmanların fiziksel olarak güvenliğini sağlamak amacıyla kilitleme, zincirleme gibi önlemlerin belirlenmesi.
  - Alarm sistemleri ve güvenlik personeli ile hırsızlık ve zarar verme durumlarına karşı hazırlıklı olunması.
- **Ekipman Taşıma ve İmha:**
  - Bilgi teknolojisi ekipmanlarının güvenli taşıma ve imha politikalarının belirlenmesi.
  - Ekipmanın devre dışı bırakılması veya elden çıkarılması sırasında güvenliği sağlamak için prosedürlerin oluşturulması.
- **Personel Eğitimi:**
  - Çalışanlara fiziksel güvenlik politikaları konusunda düzenli eğitimlerin verilmesi.
  - Personelin güvenlik prosedürlerine uyumunu sağlamak için farkındalık yaratılması.
- **Acil Durum Planları:**
  - Fiziksel güvenlik olaylarına karşı acil durum planlarının belirlenmesi ve çalışanlara bu planların eğitiminin verilmesi.
  - İncelenen olaylardan elde edilen bilgilerle sürekli iyileştirme politikalarının uygulanması.

Fiziksel güvenlik politikası, ağ güvenliği stratejilerinin bir parçası olarak, organizasyonun bütünsel güvenlik çabalarını destekler ve potansiyel fiziksel tehditlere karşı önlemleri içerir.

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. İzleme ve Denetim Politikaları:

- Ağ trafiğini izlemek, güvenlik olaylarını tespit etmek ve denetim yapmak için politikalar oluşturulur.
- Güvenlik olaylarına hızlı tepki vermek amacıyla bir olay yönetimi süreci belirlenir.

SONUÇ :

- Bilgisayar Ağlarında güvenlik politikasının uygulanması kritik önem taşımaktadır. Kurumsal güvenlik için öncelikle yazılı olarak kurallar belirlenmelidir.
- Bir güvenlik politikası yaratmanın en önemli adımı planlamadır.
- Güvenlik politikası oluşturulurken kurumun en alt düzeylerine kadar inerek gereksinimler belirlenmelidir.
- Aynı zamanda oluşturulan politikalar dikkatli bir şekilde uygulanmalıdır. Güvenlik politikasının etkin olması için üst yönetimin desteği sağlanmalı ve kurumun çalışanları kullanılan politika konusunda bilgilendirilmelidir.
- Güvenlik politikaları bir kez hazırlanıp sonra değişmeyen kurallar değildir.
- Güvenlik politikası değişen tehditlere, zayıflıklara ve kurum politikalarına göre yeniden değerlendirilmeli ve gerekli değişiklikler yapılmalıdır.

VERİ GÜVENLİĞİ

VERİ GÜVENLİĞİ NEDİR ?

Veri güvenliği, bir organizasyonun veya bireyin sahip olduğu verilerin, bilgi sistemlerinin ve diğer bilişim kaynaklarının yetkisiz erişim, değişiklik, ifşa veya yok edilme gibi güvenlik tehditlerinden korunmasıdır. Veri güvenliği, hassas bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamayı amaçlar.

Temel olarak, veri güvenliği şu üç ana ilkeye dayanır:

- Gizlilik
- Bütünlük
- Kullanılabilirlik

Veri güvenliği, sadece teknik önlemleri içermeyip aynı zamanda personel eğitimini, güvenlik politikalarını, süreçleri ve fiziksel güvenlik önlemlerini de kapsar. Ayrıca, yasal düzenlemelere uygunluk ve risk yönetimi gibi faktörlere odaklanarak kapsamlı bir yaklaşım benimser. Veri güvenliği, günümüzde artan dijital tehditlere karşı organizasyonlar ve bireyler için kritik bir konudur.

VERİ GÜVENLİĞİNİN BELİRLENMESİ VE SÜRDÜRÜLMESİ

Veri güvenliği standartlarının belirlenmesi ve sürdürülmesi, bir organizasyonun bilgilerini koruma ve güvenliğini sağlama çabalarını içerir. Bu süreç, belirli bir çerçeve içinde standartlar belirleyerek, bu standartları uygulayarak, sürekli olarak gözden geçirerek ve iyileştirme faaliyetleri yürüterek gerçekleştirilir. İşte veri güvenliği standartlarının belirlenmesi ve sürdürülmesi için temel adımlar:

- **Risk Değerlendirilmesi :**
  - Organizasyon, sahip olduğu bilgilerin ve iş süreçlerinin güvenlik risklerini değerlendirir.
  - Hangi bilgilerin kritik olduğu ve hangi risklere maruz kalındığı belirlenir.
- **Standartların Seçilmesi:**
  - Organizasyonun büyüklüğü, sektörü, yasal gereksinimleri göz önüne alarak uygun veri güvenliği standartları seçilir.
  - ISO/IEC 27001, NIST Cybersecurity Framework gibi standartlar yaygın olarak kullanılır.
- **Politika ve Prosedürlerin Oluşturulması:**
  - Seçilen standartlara uygun bir veri güvenliği politikası ve prosedürleri oluşturulur.

    - Bu belgeler, organizasyonun veri güvenliği hedeflerini ve standartlara uyum gereksinimlerini tanımlar.
- **Eğitim ve Farkındalık:**
    - Çalışanlara, veri güvenliği politikalarına uygun davranışlar konusunda eğitimler verilir.
    - Güvenlik farkındalığı artırılarak içeriden kaynaklanan tehditler minimize edilir.
- **Teknolojik Çözümlerin Uygulanması:**
    - Veri güvenliği standartlarına uygun teknik kontroller, güvenlik yazılımları ve diğer önlemler uygulanır.
    - Bu adım, ağ güvenliği, şifreleme, güvenlik duvarları gibi teknolojik çözümleri içerir.
- **Denetim ve İzleme:**
    - Organizasyon, standartlara uyumun düzenli olarak denetlenmesini ve izlenmesini sağlar.
    - Güvenlik olaylarının izlenmesi ve düzenli denetimlerle uyumluluğun sürdürülmesi önemlidir.
- **Sürekli İyileştirme:**
    - Elde edilen geri bildirimler ve denetim sonuçları üzerinden sürekli iyileştirme faaliyetleri belirlenir ve uygulanır.
    - Güvenlik önlemlerinin etkinliği düzenli olarak değerlendirilir.
- **Acil Durum Hazırlığı:**
    - Acil durum durumlarında nasıl hareket edileceğini belirleyen bir acil durum hazırlık planı oluşturulur ve düzenli olarak test edilir.

SONUÇ :

Kişisel verilerin güvenliğinin sağlanması kişisel verilerin korunması hukukunun temel ilkelerinden biri olup bu doğrultuda alınabilecek teknik ve idari tedbirler her bir somut olay özelinde farklılık gösterecektir. Bu nedenle kanun koyucu tarafından söz konusu tedbirlere yönelik sınırlayıcı düzenlemeler yapılmamış olması yerindedir. Ancak GDPR'da yer alan düzenlemelere paralel bir şekilde, sayılanlarla sınırlı olmamak kaydıyla, birtakım tedbirlerin doğrudan mevzuatımızda düzenlenmesi ilgililer için yol gösterici ve faydalı olabilecektir.