T.C.
ESKİŞEHİR OSMANGAZİ ÜNİVERSİTESİ

MTH 151015308 Açık Kaynak Araçlar ile Ağ Güvenliği

2023-2024 Güz Dönemi Ödevi

Ağ Güvenliği Stratejileri ve Uygulamaları

Ağ Güvenlik Politikaları

152120201032

Furkan KOÇ

Öğretim Görevlisi: Cem İbrahim Arı

Aralık 2023

İçindekiler

1. AĞ GÜVENLİĞİ POLİTİKALARI

1.1. AĞ GÜVENLİK POLİTİKASI NEDİR?

Ağ güvenlik politikası, bir kuruluşun bilgisayar ağının ve ağdan erişilebilen kaynakların yetkisiz erişimini, kötüye kullanımını, değiştirilmesini veya reddedilmesini önlemek, tespit etmek ve yanıtlamak için tasarlanmış yazılı bir kurallar dizisidir.

Ağ güvenlik politikaları, gizlilik, bütünlük ve erişilebilirlik olmak üzere üç temel güvenlik ilkesini korumayı amaçlamaktadır.

- Gizlilik, ağdaki verilerin yetkisiz kişiler tarafından erişilememesini veya okunamamasını sağlar.
- Bütünlük, ağdaki verilerin yetkisiz kişiler tarafından değiştirilmesini veya bozulmasını önler.
- Erişilebilirlik, ağdaki verilerin ve kaynakların yetkili kişiler tarafından zamanında ve güvenilir bir şekilde erişilebilir olmasını sağlar.

Ağ güvenlik politikaları, çeşitli konuları kapsayabilir. Ağ güvenliğinin sağlanması için gerekli olan temel politikalar aşağıdaki gibidir.

- Kabul edilebilir kullanım (acceptable use) politikası:
  Ağ kullanıcılarının, bilgisayar sistemlerini ve ağ kaynaklarını nasıl kullanabileceklerini belirleyen bir politikadır. Bu politika, ağın güvenliğini ve performansını korumak için kullanıcıların kabul etmesi gereken kuralları ve sorumlulukları içerir.

- Erişim politikası:
  Bu politika, kullanıcıların ağa ve sistemlere erişimini düzenler. Kimin hangi kaynaklara erişebileceğini ve hangi yetkilere sahip olduğunu belirleyen kuralları içerir. Ayrıca, erişim düzeylerini sınırlamak ve hassas bilgilere sadece yetkili kişilerin ulaşmasını sağlamak amacıyla oluşturulur.

- Ağ güvenlik duvarı (firewall) politikası:
  Ağ güvenlik duvarı kullanımını belirleyen politikadır. Güvenlik duvarı, ağ trafiğini izleyen ve istenmeyen trafiği engelleyen bir önlemdir. Bu politika, güvenlik duvarının nasıl yapılandırılacağını, hangi trafiği engelleyeceğini ve izleyeceğini belirler.

- İnternet politikası:
  Bu politika, çalışanların internet kaynaklarını nasıl kullanacaklarını düzenler. İnternet politikası genellikle zaman kaynaklı sınırlamalar, içerik filtreleme ve güvenlik önlemlerini içerir. Ayrıca, phishing gibi tehditlere karşı korunma önlemlerini de içerebilir.

- Şifre yönetimi politikası:
  Bu politika, kullanıcıların şifreleri nasıl oluşturacakları, değiştirecekleri ve paylaşmamaları gerektiği gibi şifre yönetimi konularını kapsar. Güçlü şifre standartlarını belirler ve şifrelerin düzenli aralıklarla değiştirilmesini sağlar.

- Fiziksel güvenlik politikası:

  Ağa fiziksel erişimi sınırlayan ve koruyan politikadır. Bu politika, sunucu odaları, veri merkezleri ve ağ ekipmanlarının bulunduğu fiziksel alanlara yetkisiz erişimi önlemek için alınan güvenlik önlemlerini içerir.

- Sosyal mühendislik politikası:

  Bu politika, çalışanları sosyal mühendislik saldırılarına karşı eğitmeyi ve bu tür saldırıları önlemek amacıyla izlenecek yöntemleri belirtir. Sosyal mühendislik, genellikle kullanıcıların güvenini kötüye kullanarak bilgi elde etmeye çalışan bir saldırı taktiğidir.

Ağ güvenlik politikaları, bir kuruluşun ağ güvenliğinin temel bir parçasıdır. İyi tasarlanmış ve uygulanan ağ güvenlik politikaları, kuruluşun ağını ve verilerini korumaya yardımcı olabilir.

2. AĞ GÜVENLİĞİNİN TEMEL POLİTİKALARI

2.1. KABUL EDİLEBİLİR KULLANIM POLİTİKASI (Acceptable Use Policy, AUP)

Kabul edilebilir kullanım politikalarının amacı, kuruluşun bilgi sistemleri ve kaynaklarının güvenli bir şekilde kullanılmasını sağlamaktır. Bir kuruluşun bilgisayar sistemleri, ağ kaynakları ve diğer teknolojik varlıklarını kullanımını düzenleyen bir belgelerdir. Bu politika, kuruluşun kaynaklarını etkin ve güvenli bir şekilde kullanmalarını sağlamak, ağ performansını korumak ve güvenlik risklerini azaltmak amacıyla oluşturulur. Politikanın temel unsurları aşağıdaki gibi sıralanmıştır:

- Amaç,
- Kapsam,
- Kullanıcı Sorumlulukları,
- İzin Verilen ve Yasaklanan Kullanımlar,
- Güvenlik İlkeleri
- İhlal Durumunda Alınacak Tedbirler,
- Revizyon ve Güncelleme Süreci.

Yazılan politikalarda temelde aşağıdaki konular bulunmaktadır.

- 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.

2.2. ERİŞİM POLİTİKALARI (Access Policy)

Erişim politikaları kullanıcıların ağa bağlanma yetkilerini belirler. Her kullanıcının ağa bağlanma yetkisi farklı olmalıdır. Erişim politikaları kullanıcılar kategorilere ayrıldıktan sonra her kategori için ayrı ayrı belirlenmelidir. Bir organizasyonun bilgisayar sistemlerine, ağ kaynaklarına veya diğer teknolojik varlıklara erişimi düzenleyen bir belgedir. Erişim politikasının temel unsurları aşağıdaki gibidir:

- Amaç,
- Kapsam,
- Erişim İlkeleri,
- Erişim Kontrolleri,
- Erişim İzleme ve Denetleme,
- Erişim Talepleri ve Onay Süreci,
- Erişim Sonlandırma ve Revizyon.

Yazılan erişim politikalarında genellikle aşağıdaki konuları kapsar:

- Erişim kontrolü: Kimlerin bilgi sistemlerine ve kaynaklarına erişebileceğini belirler.
- Erişim yetkilendirmesi: Kimlerin hangi bilgilere ve kaynaklara erişebileceğini belirler.
- Erişim izlenmesi: Erişimin kim tarafından, ne zaman ve hangi bilgilere veya kaynaklara yapıldığının izlenmesini sağlar.

2.3. AĞ GÜVENLİK DUVARI POLİTİKASI (Firewall Policy)

Ağ güvenlik duvarı politikası, bir organizasyonun bilgisayar ağını korumak ve güvenliğini sağlamak amacıyla uyguladığı kılavuz ve kuralları belirten bir belgedir. Ağ güvenlik duvarları, bir kuruluşun ağını dış tehditlerden korumak için kullanılan bir güvenlik cihazıdır. Ağ güvenlik duvarı politikasının temel unsurları aşağıdaki gibidir:

- Amaç,
- Kapsam,
- Güvenlik Duvarı Konfigürasyonu,
- İzin Verilen ve Yasaklanan Trafiğin Tanımlanması,
- Güvenlik Duvarı Güncelleme Prosedürleri,
- İzin Talepleri ve Denetim Süreçleri,
- Güvenlik Duvarı Loglama ve İzleme,
- Acil Durum Senaryoları ve Yanıt Planları,
- Güvenlik Politikalarının Gözden Geçirilmesi ve Güncellenmesi,
- Güvenlik Duvarı Performans ve Kapasite Yönetimi,
- Uyum ve Yasa Yükümlülükleri.

Bu unsurlar, ağ güvenlik duvarı politikasının temel bileşenlerini oluşturur ve organizasyonun ağ güvenliğini etkili bir şekilde yönetmesine yardımcı olur.

Ağ güvenlik duvarı politikaları, aşağıdakiler de dahil olmak üzere çeşitli konuları kapsayabilir:

- Güvenlik duvarlarının konumu:
    - Güvenlik duvarları, bir kuruluşun ağ giriş noktalarında, genellikle erişim noktaları, yönlendiriciler ve anahtarlar gibi ağ cihazlarının yanında konumlandırılmalıdır.
- Güvenlik duvarlarının ayarları:
    - Güvenlik duvarları, izin verilen ve yasaklanan trafiği belirlemek için bir dizi kuralla yapılandırılmalıdır.
- Güvenlik duvarlarının yönetimi:
    - Güvenlik duvarları, düzenli olarak izlenmeli ve güncellenmelidir.

Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmektedir:

- Proxy:
    - Proxy, bilgisayar ağlarında kullanıcıların erişim sağladığı internet kaynaklarına aracılık eden bir sunucu veya uygulamadır. Proxy sunucuları, kullanıcının gerçek IP adresini gizleyerek anonimlik sağlar, içerik filtreleme ve güvenlik duvarı işlevleri gibi ağ güvenliği amacıyla da kullanılabilir.
- Anti-Virus Çözümleri:
    - Anti-virus çözümleri, bilgisayar sistemlerini zararlı yazılımlardan korumak amacıyla kullanılan yazılımlardır. Virüs, trojan, solucan gibi zararlı yazılımları tespit eder ve temizler veya karantinaya alır. Güncel imza veritabanları ile sürekli olarak yeni tehditlere karşı koruma sağlar.
- İçerik Süzme (content filtering):
    - İçerik süzme, bir ağdaki internet trafiğini denetleyen ve belirli içerik kategorilerine, URL'lere veya anahtar kelimelere dayalı olarak erişimi kontrol eden bir güvenlik önlemidir. Bu, istenmeyen içeriklere karşı koruma sağlamak, verimliliği artırmak ve ağ güvenliğini güçlendirmek amacıyla kullanılır.
- Özel Sanal Ağlar (Virtual Private Network-VPN):
    - VPN, genellikle internet üzerinden güvenli bir bağlantı oluşturarak, uzaktan erişim sağlayan veya iki ağ arasında güvenli iletişimi destekleyen bir teknolojidir. VPN, verilerin şifrelenmesiyle gizliliği sağlar ve kullanıcıya, uzak ofise veya başka bir konuma güvenli bir şekilde bağlanma imkanı tanır.
- Nüfuz Tespit Sistemleri (Intrusion Detection Systems-IDS):
    - Nüfuz tespit sistemleri, bir bilgisayar ağını veya sistemini izleyerek, anormal veya kötü niyetli aktiviteleri tespit etmeye çalışan güvenlik sistemleridir. IDS, saldırı girişimlerini belirleyerek, güvenlik ekibine uyarılar gönderir ve potansiyel tehditlere karşı savunma sağlar. Bu sistemler, imza tabanlı veya davranış tabanlı yöntemlerle çalışabilirler.

2.4. İNTERNET POLİTİKASI (Internet Policy):

İnternet politikası, bir kuruluşun internetinin nasıl kullanılacağını belirleyen bir yazılı kurallar dizisidir. İnternet politikaları, gizlilik, bütünlük ve erişilebilirlik dahil olmak üzere bilgi güvenliğinin temel ilkelerini korumayı amaçlamaktadır. İnternet politikası temel unsurları aşağıdaki gibidir:

- Amaç,
- Kapsam,
- İnternet Kullanım Hakları ve Sorumlulukları,
- İzin Verilen ve Yasaklanan İnternet Kullanımları,
- Güvenlik ve Virüs Koruma Politikası,
- E-Posta Kullanımı ve Güvenliği,
- Veri ve Bilgi Güvenliği,
- İnternet Kullanım İzleme ve Denetleme,
- Ceza ve Disiplin Tedbirleri,
- Güncelleme ve Revizyon Süreci.

İnternet politikası, bir organizasyonun bilgi güvenliği, çalışan verimliliği ve ağ performansını yönetmek amacıyla internet kullanımını düzenlemek ve kontrol etmek için önemli bir araçtır.

İnternet politikalarının amacı, bir kuruluşun internetini aşağıdaki tehditlerden korumaktır:

- Yetkisiz erişim: İnternet politikaları, yetkisiz kişilerin bir kuruluşun internetine erişmesini önlemeye yardımcı olabilir.
- Saldırı: İnternet politikaları, bir kuruluşun internetini saldırılara karşı korumaya yardımcı olabilir.
- Bilgi hırsızlığı: İnternet politikaları, bir kuruluşun bilgilerinin çalınmasını önlemeye yardımcı olabilir.
- Yasa dışı faaliyetler: İnternet politikaları, bir kuruluşun internetini yasa dışı faaliyetler için kullanılmasını önlemeye yardımcı olabilir.

2.5. ŞİFRE YÖNETİMİ POLİTİKASI (Password Management Policy)

Şifre yönetimi politikası, bir organizasyonun güvenliğini artırmak ve yetkisiz erişimlere karşı koruma sağlamak amacıyla şifrelerin nasıl yönetileceğini belirleyen bir belgedir.

Şifre yönetimi politikası temel unsurları aşağıdaki gibidir:

- Şifre Oluşturma ve Karmaşıklık,
- Şifre Güncelleme Döngüsü,
- Şifre Paylaşımı ve Saklama,
- Çoklu Faktörlü Kimlik Doğrulama,
- Şifre Kurtarma Süreçleri,
- Şifre Depolama ve Şifre Yönetim Araçları,
- Şifre İhlallerine Karşı Yanıt Planları,
- Şifre Güvenliği Eğitimleri,
- Şifre Politikası İhlalleri ve Cezalar,
- Politikanın Gözden Geçirilmesi ve Güncellenmesi.

Şifre yönetimi politikaları genellikle aşağıdaki konuları kapsar:

- Şifre gereksinimleri:
    - Şifrelerin ne kadar güçlü olması gerektiğini ve ne tür karakterler içermesi gerektiğini tanımlar.
- Şifre yönetimi uygulamaları:
    - Şifrelerin nasıl oluşturulacağını, değiştirileceğini ve saklanacağını tanımlar.
- Şifre izleme:
    - Şifrelerin ihlal edilip edilmediğini belirlemek için kullanılan yöntemleri tanımlar.

Şifre yönetimi politikaları, kuruluşun bilgi güvenliğinin temel bir parçasıdır. İyi tasarlanmış ve uygulanan şifre yönetimi politikaları, kuruluşun sistemlerine ve verilerine yetkisiz erişimi önlemeye yardımcı olabilir.

2.6. FİZİKSEL GÜVENLİK POLİTİKASI (Physical Security Policy)

Fiziksel güvenlik politikası, bir organizasyonun binaları, ekipmanları ve kaynakları gibi fiziksel varlıklarını korumak için uygulanan kuralları ve yönergeleri belirleyen bir belgedir. Fiziksel güvenlik politikası temel unsurları aşağıdaki gibidir:

- Bina Erişimi ve Kontrolü,
- Personel Kimlik Doğrulama,
- Ziyaretçi Yönetimi,
- Güvenlik Kameraları ve İzleme Sistemleri,
- Personel Eğitimi,
- Hassas Alanlara Erişim Kontrolleri,
- Fiziksel Varlıkların Korunması,
- Acil Durum Yönetimi ve Tahliye Prosedürleri,
- Fiziksel Güvenlik Denetimleri ve Gözden Geçirme.

Fiziksel güvenlik politikaları genellikle aşağıdaki konuları kapsar:

- Erişim kontrolü:
    - Kimlerin fiziksel varlıklara erişebileceğini belirler.
- Güvenlik denetimleri:
    - Fiziksel varlıkların güvenli bir şekilde kullanılmasını sağlamak için kullanılan yöntemleri tanımlar.
- Acil durum planları:
    - Acil durumlarda çalışanların güvenliğini sağlamak için kullanılan yöntemleri tanımlar.

2.7. SOSYAL MÜHENDİSLİK POLİTİKASI (Social Engineering Policy)

Sosyal mühendislik politikası, bir organizasyonun çalışanlarını ve bilgi sistemlerini, kötü niyetli saldırılardan korumak amacıyla sosyal mühendislik taktiklerine karşı alınacak önlemleri belirleyen bir belgedir.

Sosyal mühendislik politikasının temel unsurları aşağıdaki gibidir:

- Amaç,
- Farkındalık ve Eğitim,
- Sosyal Mühendislik Saldırı Senaryoları,
- İletişim Kuralları,
- Sosyal Mühendislik Tuzaklarına Karşı Koruma,
- Şüpheli Durum Bildirimi ve İncelenmesi,
- Bilgi Paylaşımı ve Gizlilik Kuralları,
- Sosyal Medya Kullanımı Politikaları,
- İncelme ve Değerlendirme Prosedürleri,
- Cezalar ve Disiplin Tedbirleri.

Sosyal mühendislik politikaları genellikle aşağıdaki konuları kapsar:

- Sosyal mühendislik saldırılarının tanımı: Sosyal mühendislik saldırılarının ne olduğu ve nasıl çalıştıkları tanımlanmalıdır.
- Sosyal mühendislik saldırılarının yaygın örnekleri: Sosyal mühendislik saldırılarının yaygın örnekleri belirtilmelidir.
- Sosyal mühendislik saldırılarına karşı koruma: Sosyal mühendislik saldırılarına karşı korumak için çalışanlara nasıl yardımcı olunacağı açıklanmalıdır.

3.GÜVENLİK POLİTİKALARININ UYGULANMASI

- Kurumun gereksinimlerinin belirlenmesi ve risk analizi sonucunda güvenlik politikası bir sorumlu veya bir kurul tarafından oluşturulmaktadır. Güvenlik politikası uygulanmadan önce aşağıdaki koşullar sağlanmalıdır:
    - Politika hazırlanırken katılım sağlanmalıdır,
    - Politika standartlara uyumlu olmalıdır: IETF'in "Security Policy Specification Language"(SPSL), Sun Systems'in "Generic Security Services API" (GSSAPI) ve "Pluggable Authentication Modules" (PAM) verilebilir.
    - Yönetimin onayı alınmalı ve politika duyurulmalıdır,
    - Acil durum politikası oluşturulmalıdır.
    - Politikalar oluşturulduktan ve duyurulduktan sonra uygulanmalıdır. Politikada belirtilen kuralların uygulanması için korunacak sistemler üzerinde veya ağ cihazlarında gerekli teknik ayarlar yapılmalıdır. Örneğin güvenlik matrisinde oluşturulan erişim kuralları ve hangi sunuculara hangi protokoller üzerinden erişilebileceği güvenlik duvarı veya erişim listeleri (access-list) yöntemleri kullanılarak oluşturulmalıdır.
    - Fakat daha önemlisi ayarlanan güvenlik sistemleri sık sık sınanmalı, risk haritası çıkarılmalı, sistemin zayıf noktaları saptanıp gerekli önlemler alınmalıdır. Logların incelenmesi ile güvenlik politikasının amacına ulaşıp ulaşmadığı anlaşılabilir.

4.SONUÇ

Ağ güvenliği politikaları, bir kuruluşun bilgisayar ağının ve erişilebilen kaynakların yetkisiz erişimini, kötüye kullanımını, değiştirilmesini veya reddedilmesini önlemek amacıyla oluşturulan kurallar dizisidir. Bu politikalar gizlilik, bütünlük ve erişilebilirlik ilkelerini korumayı hedefler. Kabul edilebilir kullanım, erişim, ağ güvenlik duvarı, internet, şifre yönetimi, fiziksel güvenlik ve sosyal mühendislik gibi temel politikalar, ağ güvenliğini sağlamak için kullanılır. Kabul edilebilir kullanım politikası, ağ kullanıcılarının sorumluluklarını belirlerken, erişim politikası kullanıcıların ağa ve sistemlere erişimini düzenler. Ağ güvenlik duvarı politikası, güvenlik duvarının konfigürasyonunu ve izin verilen/yasaklanan trafiği belirler. İnternet politikası, çalışanların internet kaynaklarını kullanımını düzenler ve şifre yönetimi politikası, güçlü şifre standartlarını ve yönetimini içerir. Fiziksel güvenlik politikası, ağa fiziksel erişimi sınırlar, sosyal mühendislik politikası ise çalışanları bu tür saldırılara karşı eğitir ve önlemler belirler. Bu politikalar, bir kuruluşun bilgi güvenliğini etkin bir şekilde yönetmesine yardımcı olur.

5.KAYNAKÇA

- The SANS Security Policy Project, http://www.sans.org/resources/policies
- KURUMSAL AĞ VE SİSTEM GÜVENLİĞİ POLİTİKALARININ ÖNEMİ VE BİR DURUM ÇALIŞMASI https://dergipark.org.tr/tr/download/article-file/200979
- https://www.forcepoint.com/cyber-edu/network-security
- https://bulutistan.com/blog/ag-guvenligi-network-security/