Eren Kaşık

402569

1.Ağ Güvenliği ve Stratejileri

1.1.Giriş

Günümüzde bilişim alanındaki en büyük sorunlardan biri ağ güvenliğidir. Büyük şirketler kurmuş oldukları ağ sistemlerinin saldırılara karşı korunması için yaşamsal bir savaş vermektedirler. Bundan dolayı çok büyük yatırımlar yapmakta ve büyük paralar harcanmaktadır. Ticari anlamda firmalar büyük zarar görmektedirler. Diğer taraftan bu tür sistemleri üreten ve yazılım geliştiren firmalar büyük bir para kazanmaktadırlar. Saldırı çeşitleri arttığı sürece her gün yeni bir ağ güvenliği programı ve sistemi ortaya çıkmaktadır. Tabii olarak bu gelişme yüzünden büyük bir pazar oluşmaktadır.

Burada sadece büyük firmalar değil kişisel bazdaki kullanıcılarda bilgi saklama ve korunması için çeşitli programlar ve sistemler almaktadır. Dünya çapında büyük bir pazar haline gelen bu güvenlik sistemleri dünya ülkelerinde olduğu gibi ülkemiz ekonomisine büyük zararlar vermektedir.

Yapılan araştırmalar dünya genelinde şirkete yapılan atakların % 70 ila % 90 arasında şirket çalışanları tarafından yapıldığını ortaya koymaktadır. Bu bilgi hırsızlığından tutun bilerek ya da bilmeyerek sistemlere verilen zararları kapsamaktadır. Genelde işinden kötü şekilde ayrılan şirket çalışanları sistemlere ait bilgilerini başkalarına verebilmekte ya da özellikle sistemleri sabote edebilmektedirler. Kendi bilgisayarlarına kurdukları “sniffer”(paket dinleyici) lar sayesinde başka kişilerin maillerini ya da gizli bilgilerini elde edebilmektedirler. Ya da her türlü önleminizi dışarıdan gelebilecek saldırılara karşı almışken içeriden birisi kolaylıkla önemli sistemlere erişebilir kritik bilgileri silip değiştirebilir yada rakip bir firmaya verebilir. Yada meraklı bir kullanıcı yeni öğrendiği hacker araçlarını sizin firmanız üzerinden başka firmalara girmek için kullanabilirler.

Güvenlik için yapılan her yatırıma karşı bu saldırılar sürmektedir. Hatta Amerika’da dünyanın en iyi korunan, girilmesi imkansız olan Savunma Bakanlığı bilgisayarlarına girilmiş ve bilgilere ulaşılmıştır. Amerika’da bu tür saldırılara ağır cezalar uygulanırken Türkiye’de bir yasal boşluktan dolayı yakalananlar elini kolunu sallayarak hapisten çıkmaktadır. Bundan dolayı ülkemizde en kısa sürede bu yasal boşluğun kapatılması gerekmektedir.

Soğuk savaş sonrası, siber savaşlar ve siber cepheler açıldı. Ülkelerin, rejimlerin ve toplulukların dijital ortamda sağlanan bilgilerle şekillendiği günümüzde, atılacak adımları ve alınacak aksiyonları bu kapsamda değerlendirmekte fayda var. Bilgi Güvenliği alanındaki en büyük dezavantaj, çalınan bilginin farkına varmak ve sızıntının tespitinin çok zor olmasıdır. Çünkü dijital ortamda sahibi olduğunuz veya yönettiğiniz bilgi çalındığında da hala koyduğunuz yerdedir. Sizden habersiz şirket, kurum veya

kişisel bilgilerinize kim, hangi ip adresinden, ne zaman erişti ve nasıl bu bilgilere ulaştığı sorusunun cevabı çoğu zaman samanlıkta iğne aramaktan farksızdır.

WikiLeaks, Edward Snowden NSA vakası ve Panama belgeleri ile bir kez daha ağ güvenliğinin sağlanması ve bu verilere erişimin takip edilmesinin ne derece önemli olduğunu görmüş olduk. Amacı veya nasıl çalıştıkları konusunda birçok teori olmasına rağmen bilginin ne büyük silah olduğu konusunda hem fikir olmamızı sağlamıştır. Kamu,kurum ve kuruluşlarda sahip olunan ve gizlilik arz eden belgelerin (sağlık bilgileri, finansal bilgiler, müşteri bilgileri, sipariş geçmişi, ARGE-tasarım detayları, pazar araştırmaları, satış planları, finansal planlar, kurum içi yazışmalar, özel yaşamla ilgili bilgiler) korunması ve bu yetkili / yetkisiz erişim bilgilerinin rutin olarak gözden geçirilmesi kendi içimizde yaşanacak WikiLeaks vakalarının önüne geçecektir. Şirket çalışanlarından birisinin ilerleyen zamanlarda Julian Assange (WikiLeaks Kurucusu) rolünü üstlenirse kaybedecekleriniz sadece para değil, tekrar kazanamayacağınız marka değeriniz ve itibarınız da olacaktır.

2. Fiziksel, Yazılımsal ve Ağ Güvenliği Stratejilerinin Önemi

Fiziksel, yazılımsal ve ağ güvenliği stratejileri, bütünsel bir güvenlik yaklaşımının temelini oluşturur ve organizasyonların bilgi varlıklarını korumak, hizmet sürekliliğini sağlamak ve potansiyel tehditlere karşı dirençli olmak için kritik öneme sahiptir.

2.1.Fiziksel Güvenlik Stratejileri:

• Donanım Koruma: Sunucular, veri merkezleri ve ağ ekipmanları gibi fiziksel varlıkları korumak, bu cihazlara fiziksel erişimi sınırlamak önemlidir. Bu, yetkisiz kişilerin donanıma fiziksel olarak zarar vermesini veya çalmasını engeller.

• Erişim Kontrolü: Kapı erişim kartları, biyometrik tanıma sistemleri gibi yöntemlerle bina içindeki bölgelere sınırlı erişim sağlanması, yetkisiz kişilerin bilgi varlıklarına fiziksel erişimini önler.

• Güvenli Teslimat ve İletim: Donanım bileşenlerinin ve cihazların güvenli bir şekilde taşınması, kurulumu ve bakımı, potansiyel tehditlere karşı koruma sağlar.

2.2.Yazılımsal Güvenlik Stratejileri:

• Güvenlik Yazılımları: Antivirüs programları, anti-malware yazılımları ve güvenlik duvarları gibi yazılım tabanlı güvenlik araçları, bilgisayar sistemlerini zararlı yazılımlardan korur.

• Güncelleme ve Yama Yönetimi: Yazılım güncellemeleri ve yamaları, güvenlik açıklarının kapatılmasını sağlar. Güncel yazılım, bilgisayar sistemlerinin güvenliğini artırır.

• Yetkilendirme ve Kimlik Doğrulama: Güçlü kimlik doğrulama ve yetkilendirme protokolleri, yetkisiz erişimi önler ve bilgi varlıklarını korur.

• Veri Şifreleme: Hassas verilerin şifrelenmesi, veri sızıntılarına karşı koruma sağlar.

2.3.Ağ Güvenliği Stratejileri:

• Güvenlik Duvarları: Ağ güvenlik duvarları, ağ trafiğini izleyerek ve kontrol ederek yetkisiz erişimi engeller.

• VPN ve Güvenli İletişim: Sanal Özel Ağlar (VPN), güvenli iletişim kanalları oluşturarak hassas verilerin güvenli bir şekilde iletilmesini sağlar.

• Olay İzleme ve Yanıt: Ağ üzerindeki olayları izleme, tehditleri hızlı bir şekilde tanımlama ve buna uygun yanıtı verme, ağ güvenliğini artırır.

• Sızma Testleri: Ağ güvenliği stratejilerinin etkinliğini değerlendirmek için düzenli sızma testleri yapılması, potansiyel zayıf noktaları belirleme ve giderme açısından önemlidir.

Bu stratejiler, bir organizasyonun bütünsel güvenlik postürünü güçlendirir ve siber tehditlere karşı daha dirençli hale getirir. Ayrıca, düzenli güvenlik eğitimleri ve farkındalık programları da çalışanların bu güvenlik stratejilerini etkili bir şekilde uygulamasına yardımcı olabilir.

3.Veri Güvenliği

Veri güvenliği ve gizliliği, bir organizasyonun en önemli varlıklarını koruma açısından kritik öneme sahiptir.

Veri güvenliği; dijital ortamlarda saklanan, işlenen ve iletilen verilerin gizliliğini, bütünlüğünü ve erişim kontrolünü sağlama sürecidir. Bu tedbirler, bilgileri yalnızca yetkili kişilerin erişimine izin vererek gizli tutulmalarını garanti eder. Verilerin değiştirilmeden korunmasını sağlar ve sadece yetkili kişilerin belirlenmiş işlemleri gerçekleştirebilmesine olanak tanır. Bu kapsamda sürekli izleme ve denetleme ile olası güvenlik ihlalleri hızla tespit edilir. Böylelikle potansiyel aksaklıklara kolaylıkla müdahale edilir. Yani özetle dijital veri güvenliği, bireylerin kişisel bilgilerini koruma ve işletmelerin kritik verilerini güvence altına alma ihtiyacını karşılar. Peki veri güvenliği için neler yapılabilir:

1. Risk Değerlendirmesi ve Yönetimi:
    - Veri güvenliği ve gizliliği açısından potansiyel risklerin belirlenmesi.
    - Risklerin ciddiyeti ve olasılığına göre önceliklendirme.
    - Risklere karşı uygun güvenlik kontrollerinin uygulanması.

2. Güvenlik Politikalarının Oluşturulması ve Uygulanması:
    - Şirket içinde net ve etkili bir güvenlik politikası belirlenmesi.
    - Çalışanların ve paydaşların bu politikalara uyumu sağlamak için eğitilmesi.
    - Politikaların düzenli olarak gözden geçirilmesi ve güncellenmesi.

3. Kimlik Doğrulama ve Yetkilendirme:
    - Güçlü kimlik doğrulama yöntemlerinin kullanılması.
    - Her kullanıcının belirli bir rol ve yetki seviyesi olması ve sadece ihtiyaç duyduğu verilere erişimine izin verilmesi.

4. Veri Şifreleme:
    - Hassas verilerin depolama, iletim ve işleme aşamalarında şifrelenmesi.
    - Şifreleme anahtarlarının güvenli bir şekilde yönetilmesi.

5. Güvenli Yazılım Geliştirme Uygulamaları:
    - Yazılım geliştirme süreçlerinde güvenlik en iyi uygulamalarının benimsenmesi.
    - Yazılım güvenliği için düzenli olarak güvenlik testleri yapılması.

6. Ağ Güvenliği:
    - Güvenlik duvarları, IDS/IPS gibi ağ güvenliği cihazlarının kullanılması.
    - Ağ trafiğinin izlenmesi ve anormal aktivitelerin hızlı bir şekilde tanımlanması.

7. Veri Yedekleme ve Kurtarma:
    - Düzenli ve güvenli veri yedekleme stratejilerinin oluşturulması.
    - Veri kaybı durumunda hızlı bir kurtarma sürecinin sağlanması.

8. Fiziksel Güvenlik:
    - Sunucu odalarının,veri merkezlerinin ve cihazların fiziksel erişimine sıkı kontrol.
    - Biyometrik tanıma ve güvenlik kameraları gibi fiziksel güvenlik önlemlerinin uygulanması.

9. Çalışan Eğitimi ve Farkındalık:
    - Çalışanlara düzenli güvenlik eğitimleri verilmesi.
    - Sosyal mühendislik ve phishing saldırılarına karşı farkındalık oluşturulması.

10. Uyumluluk ve İlgili Mevzuatlara Uyum:
    - Geçerli güvenlik mevzuatlarına ve standartlarına uyumun sağlanması.
    - Veri güvenliği ve gizliliği konusundaki yasal düzenlemelere uyumlu politikaların benimsenmesi.

Bu stratejik yaklaşımlar, veri güvenliği ve gizliliğini sürdürülebilir bir şekilde sağlamak için önemlidir. Ayrıca, bu stratejilere sürekli gözden geçirme ve iyileştirme süreçleri eklemek, değişen tehdit manzaralarına ve teknolojik gelişmelere karşı adapte olmayı sağlar.

4.Sonuç

Ağ güvenliği sağlanırken ister kurumsal ister kişisel bazda olsun ilk önce saldırı tespiti yapılmalıdır. Daha sonra bu tespite göre uygun program ve donanım seçilmelidir. Bilgisayar içindeki bilgiler kişiler için çok önemli olduğundan bunlardan gelebilecek bir saldırı sonucunda bilgilerin yok olması, istenmeyen kişileri eline geçmesi mümkün olacak. Bu da kişi ya da kuruluşların büyük zararlara uğramasına sebep olacaktır. Bu yüzden ağ güvenliği sağlanırken yukarda açıklanmış olan ağ güvenliği sağlama yöntemleri eksiksiz bir biçimde uygulanmalıdır.

5.Ağ Güvenliği Politikaları

5.1.Ağ Güvenliği Politikası Nedir?

Ağ güvenliği politikaları, bir organizasyonun bilgi sistemlerini korumak için belirlenen kurallar ve yönergelerdir. Bu politikalar, veri güvenliği, erişim kontrolü, şifreleme, güvenlik yedeklemeleri gibi konuları kapsar. Ayrıca, kullanıcıların sorumlu davranışlarını ve güvenlik ihlallerine karşı alınacak önlemleri içerir. Politikaların düzenli olarak güncellenmesi ve çalışanlara eğitim verilmesi, etkili bir ağ güvenliği stratejisinin önemli unsurlarıdır.

5.2.Güvenlik Politikalarının Oluşturulması

1. Risk Değerlendirmesi:
    - Organizasyonunuzun özel ihtiyaçlarını ve potansiyel tehditleri belirleyin.
    - Varlık, zafiyet ve tehdit analizi yaparak riskleri önceliklendirin.

2. Hedef Belirleme:
    - Politikaların temel hedeflerini belirleyin, örneğin, veri gizliliği, hizmet sürekliliği, izinsiz erişim önleme.
    - Hedefler, organizasyonun spesifik ihtiyaçlarına yönelik olmalıdır.

3. Uyumluluk ve Standartlar:
    - İlgili yasal düzenlemelere ve endüstri standartlarına uyum sağlayın.

- Özellikle kişisel veri koruma yasalarını göz önünde bulundurun.

4. Politika Yazma:
   - Açık ve anlaşılır bir dil kullanarak politikaları belirleyin.
   - Kullanıcılar, ağ yapılandırması, veri güvenliği gibi alanları kapsayan spesifik politika maddeleri ekleyin.

5. İşbirliği ve Geri Bildirim:
   - İlgili paydaşlar, IT personeli ve çalışanlarla işbirliği yaparak politikaları geliştirin.
   - Politika taslağını paydaşlardan geri bildirim alın ve iyileştirmeler yapın.

6. Eğitim ve Farkındalık:
   - Çalışanlara güvenlik politikalarını anlatan eğitimler düzenleyin.
   - Güvenlik farkındalığını artırmak için düzenli bilgilendirme kampanyaları yapın.

7. Uygulama Planı:
   - Politikaların nasıl uygulanacağını belirleyin.
   - İlgili ekipler arasında sorumlulukları açıkça tanımlayın.

8. Teknolojik Destek:
   - Güvenlik teknolojileri ve araçlarını entegre ederek politikaların etkili bir şekilde uygulanmasını destekleyin.
   - Güvenlik açıkları için düzenli olarak güvenlik taramaları yapın.

9. İzleme ve Değerlendirme:
   - Politikaların etkili bir şekilde uygulandığını izleyin.
   - İzleme sistemleri aracılığıyla anormal aktiviteleri tespit edin ve değerlendirin.

10. Güncelleme ve Revizyon:
    - Politikaları düzenli olarak gözden geçirin ve değişen tehditlere ve teknolojiye uygun şekilde güncelleyin.
    - Revizyonları çalışanlara etkili bir şekilde ileterek uygulamaya koyun.

Bu adımları takip ederek, ağ güvenliği politikalarınızı oluşturabilir ve organizasyonunuzun güvenliğini artırabilirsiniz.

5.3. Güvenlik Politikasının Uygulanması

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.

6.Sonuç

Güvenlik politikasının etkin olması için üst yönetimin desteği sağlanmalı ve kurumun çalışanları kullanılan politika konusunda bilgilendirilmelidir. Güvenlik politikası değişen tehditlere, zayıflıklara ve kurum politikalarına göre yeniden değerlendirilmeli ve gerekli değişiklikler yapılmalıdır. Aynı zamanda oluşturulan politikalar dikkatli bir şekilde uygulanmalıdır. Güvenlik politikasının etkin olması için üst yönetimin desteği sağlanmalı ve kurumun çalışanları kullanılan politika konusunda bilgilendirilmelidir.

7.Veri Güvenliği Standartları - Belirleme ve Sürdürme

7.1. Veri Güvenliği Standartları Nedir?

Veri güvenliği standartları, hukuki düzenlemeler, endüstri normları ve organizasyonun kendi politika ve prosedürleri gibi belirlenen yönergeler ve gerekliliklerdir. Bu standartlar, organizasyonların veri güvenliğini korumak ve yönetmek için temel prensipleri sunar.

7.2. Standart Belirleme Süreci

7.2.1 Hukuki ve Düzenleyici Gereksinimlerin Belirlenmesi

- Veri güvenliği ile ilgili hukuki düzenlemelerin ve yasal gereksinimlerin belirlenmesi.

- Organizasyonun faaliyet gösterdiği sektördeki düzenleyici gereksinimlere uyum sağlama.

7.2.2 Endüstri Standartlarının Gözden Geçirilmesi

- Organizasyonun faaliyet gösterdiği sektördeki en güncel endüstri standartlarının araştırılması.

- Öne çıkan endüstri standartlarının organizasyon ihtiyaçlarıyla uyumluluğunun değerlendirilmesi.

7.2.3 Organizasyonel İhtiyaçların Değerlendirilmesi

- Organizasyonun veri varlıklarının sınıflandırılması ve kategorize edilmesi.

- Risk analizi ve değerlendirme süreçlerinin uygulanması.

7.3. Risk Analizi ve Değerlendirme

7.3.1 Veri Sınıflandırma ve Kategorizasyon

- Organizasyonun sahip olduğu verilerin hassasiyet düzeyine göre sınıflandırılması.

- Veri sınıflandırmasının temel prensipleri ve önemi.

7.3.2 Risk Analizi Yöntemleri

- Olası tehditlerin ve zayıflıkların belirlenmesi.
- Risk analizi yöntemleri ve bu sürecin uygulanması.

7.3.3 Öncelikli Tehditlerin Belirlenmesi

- Risk analizi sonuçlarına dayanarak öncelikli tehditlerin saptanması.
- Öncelikli tehditlere karşı alınabilecek güvenlik önlemleri.

7.4. Teknolojik Çözümler ve Politikalar

7.4.1 Güvenlik Yazılımları ve Donanımları

- Güvenlik yazılımları ve donanımlarının seçimi.
- Ağ güvenliği için kullanılan teknolojik çözümlerin işlevselliği.

7.4.2 Veri Güvenliği Politika ve Prosedürleri

- Güvenlik politika ve prosedürlerinin oluşturulması ve güncellenmesi.
- Personelin bu politika ve prosedürlere uyumunu sağlama.

7.4.3 Eğitim ve Farkındalık Programları

- Personelin veri güvenliği konusunda eğitilmesi.
- Güvenlik politika ve prosedürlerine uyumu artırmak için düzenlenen farkındalık programları.

7.5. Sürdürme Aşaması

7.5.1 Sürekli İzleme ve Değerlendirme

- Güvenlik olaylarının sürekli olarak izlenmesi.
- Güvenlik kontrollerinin etkinliğinin periyodik olarak değerlendirilmesi.

7.5.2 Güvenlik Teknolojilerinin Güncellenmesi

- Güvenlik teknolojilerinin güncel kalması için sürekli takip ve güncelleme.

- Yeni tehditlere karşı güvenlik önlemlerinin hızlı bir şekilde entegrasyonu.

7.5.3 Olay Müdahale Planlarının Gözden Geçirilmesi

- Olay müdahale planlarının periyodik olarak gözden geçirilmesi ve güncellenmesi.

- İncelenen olaylardan elde edilen öğrenmelerin planlara entegrasyonu.

7.6. Yasal ve Düzenleyici Uyum

7.6.1 Yasal Değişikliklere Hızlı Uyum

- Güncel yasal düzenlemelerin düzenli olarak takip edilmesi.

- Organizasyonun hızlı bir şekilde yasal değişikliklere uyum sağlaması.

7.6.2 Düzenleyici Gereksinimlerin Takibi

- Organizasyonun faaliyet gösterdiği sektördeki düzenleyici gereksinimlerin takip edilmesi.

- Uygunluğun düzenleyici değişikliklere göre değerlendirilmesi.

7.7. Denetim ve İncelemeler

7.7.1 İç Denetimler

- İç denetim süreçlerinin oluşturulması ve düzenlenmesi.

- Güvenlik kontrollerinin iç denetimler aracılığıyla değerlendirilmesi.

7.7.2 Dış Denetimler

- Harici denetim süreçlerinin planlanması ve yürütülmesi.

- Harici denetim sonuçlarına dayalı olarak