1. AMAÇ

Üniversitemiz Bilgi Sistemlerinin, Güvenli Sistem Mühendisliği prensipleri temelinde, tasarlanması, geliştirilmesi ve işletilmesi amacıyla hazırlanmıştır.

2. KAPSAM ve SORUMLULUKLAR

Bu dokümandaki ilkeler üniversitemizin tüm birimlerini kapsamaktadır.

Bu kılavuz uygulanabilir genel güvenlik mühendisliği ilkelerini ortaya koymaktadır. Tüm prensipler her bir sistemin yaşam döngüsü boyunca dikkatlice göz önüne alınmalıdır. Burada sunulan ilkeleri dikkate alacak çalışanlar:

1. Kullanıcılar: Fonksiyonel gereksinimleri geliştiren ve değerlendiren ya da kendi kurumlarında bilgi sistemi işleten,

2. Sistem Mühendisleri ve Mimarlar: Bir bilgiyi tasarlayan, uygulayan ya da düzenleyen,

3. Program Yöneticileri ve Bilgi Güvenliği Görevlileri: Yeterli güvenlik önlemlerinin sistem yaşam döngüsünün tüm aşamalarında dikkate alındığından emin olmak için.

3. UYGULAMA

Bu ilkeler; inşa edilebilecek BT güvenliği yapısının, tasarım, geliştirme ve uygulamasına daha tutarlı ve yapılandırılmış bir yaklaşım sağlanmasına zemin oluşturmaktadır.

Bu ilkelerin odak noktası teknik kontrollerin uygulanmasıdır. Bununla birlikte, etkili olabilmek için, “Bir sistem güvenlik tasarımı aynı zamanda politika, operasyonel prosedürler, kullanıcı farkındalığı ve eğitim gibi teknik olmayan konuları dikkate almalıdır” gerçeğine vurgu yapar.

İdeal olarak, burada sunulan ilkeler, bir programın başlangıcında uygulanır ve programın sonraki sistem yaşam döngüsü boyunca kullanılır. İlkeler hazırda konuşlanmış bilgi sistemlerinin, güvenlik yapısının teyit edilmesine yardımcı olur. İlkeler kısa ve özdür. Sistem yaşam döngüsü politikaları geliştirmek için tüm kuruluşlar tarafından kullanılabilir.

Güvenlik mühendisliği prensiplerini uygulaması öncelikle, geliştirilmekte olan yeni bilgi sistemlerini, veya kapsamlı yükseltmelerin uygulandığı sistemleri hedeflemiştir ve sistem geliştirme yaşam döngüsü içine entegre edilmelidir. Eski bilgi sistemleri için kuruluşlar,

güvenlik mühendisliği ilkelerini sistem yükseltmelerine ve modifikasyonlara mümkün ölçüde uygulamalıdır.

İLKELER

1. Tasarım için "temel" bir güvenlik politikası oluşturmak

Üniversitemiz Bilgi Güvenliği Politikası, sistem tasarımı ve güvenlik çözümlerine her yönden uygulanır. BGYS Politikası sistemin desteklemesi gereken hedefleri (gizlilik, bütünlük, kullanılabilirlik, hesap verebilirlik ve güvence) tanımlar ve bu hedefler, IT güvenlik mimarisi tasarımında kullanılan prosedür, standart ve kontrollere rehberlik eder. BGYS Politikası, kritik varlıkları, algılanan tehditleri, güvenlikle ilgili rolleri ve sorumlulukların da tanımlanmasını gerektirmektedir.

2. Güvenliği, genel sistem tasarımının ayrılmaz bir parçası olarak değerlendirmek

Güvenlik bilgi sistemi tasarımında dikkate alınır ve sistem yaşam döngüsü içine tam entegre edilir.

Güvenlik tüm yeni bilgi sistemlerinin tasarım aşamasında ve mümkün olduğunca tüm eski sistemlerin modifikasyonunda ve devam eden operasyonunda uygulanır. Bu, güvenlik politikalarının oluşturulmasını, ortaya çıkan güvenlik gereksinimlerini anlamayı, güvenlik ürünleri değerlendirilmesinde yer almayı ve mühendislikte, sistem tasarım, uygulama ve bertarafını içerir.

3. İlgili güvenlik politikaları ile yönetilen fiziksel ve mantıksal güvenlik sınırlarını açıkça tanımlamak

Bilgi sistemi geliştirirken, güvenlik sınırları dikkate alınır ve ilgili sistem dokümantasyonunda ve güvenlik politiklarında tebliğ edilir.

Bilgi teknolojileri fiziksel ve mantıksal alanlardadır ve bu alanlar arasında sınırlar vardır. Dış faktörlerden neyin korunacağını anlamak, uygun koruyucu önlemlerin en etkili olacağı yerlerde uygulanmasının sağlanmasına yardımcı olabilir. Bazen bir sınır, tek bir fiziksel lokasyon ile bağlantılı olan insan, bilgi ve bilgi teknolojileri tarafından tanımlanır. Fakat bu; tek bir konumda içinde birçok farklı güvenlik politikasının kullanımda olabileceği, bazılarının

kamuya açık bilgileri kapsayabileceği, bazı hassas veya gizli bilgileri kapsayabileceği gerçeğini göz ardı eder.

Bazı durumlarda ise, sınır fiziksel sınırları geçebilen belirli bir bilgi ve bilgi teknolojileri setini yöneten bir güvenlik politikası tarafından tanımlanır. Durumu daha karmaşık hale getiren ise, çoğu kez, tek bir makine ya da sunucu hem kamu erişimini hem de hassas bilgiyi barındırabilmesidir. Sonuç olarak çoklu güvenlik politikaları tek bir makineye ya da tek bir sistem içine uygulanabilir. Bu nedenle bilgi sistemi geliştirirken, güvenlik sınırları dikkate alınır ve ilgili sistem dokümantasyonunda ve güvenlik politiklarında tebliğ edilir.

4. **Geliştiricilerin güvenli yazılım geliştirme alanında yetkin olmalarına dikkat etmek**

Geliştiricilerin sisteminin geliştirilmesi öncesinde tasarım, geliştirme, konfigürasyon kontrolü, entegrasyon ve yazılım güvenlik testi alanlarında yeterince eğitilmiş olduğu teyid edilir.

5. **Riski kabul edilebilir bir seviyeye çekmek**
6. **Dış sistemlerin güvensiz olduğunu varsaymak**
7. **Azalan risk ve artan maliyet arasındaki potansiyel takası tanımlamak**
8. **Örgütsel güvenlik hedeflerine ulaşmak için uyarlanmış sistem güvenlik önlemlerini uygulamak**

Genel olarak, BT güvenlik önlemleri bir kuruluşun kendine özgü ihtiyaçlarına göre tasarlanır. Baskın misyon gereksinimleri ve rehberlik gibi çok sayıda faktöre dikkat edilirken; temel mesele BT güvenliği ile ilgili, olumsuz etkilerden misyon ya da işin korunmasıdır çünkü; IT güvenlik ihtiyaçları homojen değildir. Diğer dış ağlar ve iç alt domain-lere bağlanırken, sistem tasarımcıları ve güvenlik uygulayıcıları güven seviyesini dikkate almalıdır.

Katmanlı bir güvenlik stratejisi kullanılmasına izin veren her sistemin benzersizliğini kabul etmek – kritikliği düşük sistemleri korumak için düşük maliyetle daha düşük güvence uygulamak ve en kritik alanlarda yüksek güvence çözümleri uygulamak.

9. **Bilgiyi; işleme, transit ve depolama esnasında korumak**

Verinin yetkisiz değiştirilmesi veya imhası, bilginin ifşa edilmesi, transit esnasında veriye erişimin reddi; muhafaza edilen ya da işlenen verilerle ilişkili riskleri ile birlikte ele alınmalıdır.

Bu nedenle, sistem mühendisleri, mimarlar ve BT uzmanları verilerin işlenirken, transfer edilirken ve depolanırken bütünlük, gizlilik ve erişilebilirliğini, gerektiği gibi, korumak için güvenlik önlemleri uygulamalıdır.

10. Yeterli güvenliği sağlamak için özel ürünler düşünmek

11. Olası tüm "saldırı" sınıflarına karşı korunmak

Tasarımda, güvenlik kontrolleri, çeşitli saldırı sınıfları göz önünde bulundurulur.

12. Taşınabilirlik ve birlikte çalışabilirlik için mümkün olan yerlerde, güvenliği açık standartlara dayandırmak

Çoğu kuruluş görevini veya işlerini gerçekleştirmek için "dağıtık bilgi sistemleri"ne önemli ölçüde bağlıdır. Bu kuruluşlar hem kendi organizasyonlarına hem de diğer organizasyonlara bilgi dağıtır.

Güvenlik yeterliliklerinin bu tip ortamda etkin olabilmesi için, güvenlik program tasarımcılarının birlikte çalışılabilirliği ve taşınabilirliği üniversitede kurmak tüm güvenlik tedbirlerine, donanım ve yazılımı kapsayan ve pratik amaçlı uygulamaları.

13. Güvenlik gereksinimlerini gelişmekte kullanın ortak dil

14. Güvenli ve makul teknoloji yükseltme süreci de dahil olmak üzere, yeni teknolojilere düzenli uyumu sağlamak için güvenlik tasarlamak

15. Operasyonel kullanım kolaylığı için çabalamak

16. Katmanlı güvenlik uygulanması benimsemek

17. Hasarı sınırlamak ve buna karşı esnek olması için bir BT sistemi tasarlamak ve işletmek

18. Beklenen tehditler karşısında sistemin esnek olduğuna ve olmaya devam edebileceğini garanti etmek

Güvence, bir sistemin güvenlik beklentilerine ulaştığı güvenlik zeminidir. Bu beklentiler hem direkt penetrasyona hem de güvenlik kontrollerini aşma girişimlerine yeterli direç temini olarak özetlenebilir.

Tehdit ortamını iyi anlama, gereksinim setlerini değerlendirme, donanım ve yazılım mühendisliği disiplinleri, ürün ve sistem değerlendirmeleri, güvence elde etmek için kullanılan birincil önlemlerdir.

Buna ek olarak özel ve gelişen tehditlerin belgelenmesi, uygulanan güvenlik sisteminde zamanında ayarlama yapılmasında ve değişen güvenlik arttışının stratejik olarak desteklenmesinde önemlidir.

19. Zayıflıkları sınırlamak veya frenlemek

Güvenlik açıklıklarını sınırlamak veya kontrol altına almak için sistemler tasarlamak. Eğer bir güvenlik açığı mevcut ise; hasar diğer bilgi sistemleri elemanlarının düzgün çalışmasına izin verecek şekilde sınırlanır veya kontrol altına alınır. Güvensizlikleri sınırlamak veya kontrol altına almak; bilgi sisteminin en çok ihtiyaç duyulan alanlarına müdahale ve yapılandırma eforunun odaklanmasına da katkı sağlar. (Bkz: İlke 10)

20. Kamu erişim sistemlerini kritik kaynaklardan izole etmek (örneğin; veri, süreçler)

21. Bilgisayar sistemleri ve ağ altyapılarını ayırmak için sınır mekanizmaları kullanmak

22. İzinsiz kullanımı tespit etmek ve olay soruşturmaları desteklemek için denetim mekanizmaları tasarlamak ve uygulamak

23. Uygun kullanılabilirliğini sağlamak için acil durum ve felaket kurtarma prosedürleri geliştirmek ve tatbik etmek

24. Basitlik için çabalamak

Mekanizma karmaşıklaştıkça, sömürülebilir kusurları da artar. Basit mekanizmalar, sömürülebilen daha az kusurları barındırma ve az bakım gerektirme eğilimindedir. Dahası konfigürasyon yönetimi konuları basitleştirildiği için; basit bir mekanizma güncelleme veya yer değiştirme, daha az yoğun bir süreç haline gelir.

25. Güvenilir olmak için sistem elemanlarını azaltmak

Güvenlik ölçütleri insanları, operasyonları ve teknolojiyi içerir. Teknolojinin kullanıldığı yerde, donanım, aygıt yazılımı ve program tasarlanmalı ve uygulanmalıdır böylece; koruma sağlamak için güvenilecek sistem elemanlarının sayısı en az sayıda olacaktır. Ayrıca, sistem güvenlik özelliklerinin maliyet-etkin ve zamanında sertifikasyonunu temin etmek için; sistem için en güvenli işlevleri sağlaması beklenen yazılım ve donanım miktarını en aza indirmek önemlidir.

26. En az ayrıcalık uygulamak

27. Gereksiz güvenlik mekanizmalarını uygulamamak

28. Bir sistemin kapatırken ya da yok ederken uygun güvenliği sağlamak

29. Yaygın hata ve güvenlik açıklıklarını tanımlamak ve önlemek

30. Fiziksel ve mantıksal şekilde dağıtılan tedbirlerin kombine ederek güvenlik uygulamak

Genellikle tek bir güvenlik hizmeti, ayrı makinelerde bulunan ve iş birliği yapan elemanlar tarafından elde edilir. Örneğin, sistem kimlik doğrulaması tipik olarak, kimlik doğrulama sunucusu üzerindeki bir uygulamaya, ag elemanları kanalıyla, bir iş istasyonu üzerinde kullanıcı arayüzünden değişen elemanlar kullanılarak gerçekleştirilir. Sağladıkları güvenlik hizmeti ile tüm öğeleri ilişkilendirmek önemlidir.

Bu bileşenler daha üst bütçe ve operasyonel kontrolün altında geçen altyapı kaynakları gibi, güvenliği sağlamak için sistemler arasında paylaşılmış olmaları muhtemeldir.

31. Birden fazla örtüşen bilgi alanlarını (domainleri) ele almak için güvenlik önlemleri hazırlamak

32. Domainler arasında ve içinde uygun erişim kontrol kararı sağlamak için kullanıcı ve işlemlerinde kimlik doğrulaması yapmak

33. Hesap verebilirliği sağlamak için benzersiz kimlikler kullanmak