ZBEÜ BİLGİ İŞLEM DAİRE BAŞKANLIĞI
GÜVENLİ YAZILIM GELİŞTİRME PROSEDÜRÜ

Revizyon Takibi:

Sıra No	Rev. No	Tarih	Hazırlayan	Revizyon Nedeni	Onaylayan	İmza
1						
2						
3						
4						

AMAÇ

Bu prosedürün amacı bilgi güvenliği saldırılarına (gizlilik, bütünlük, erişilebilirlik) karşı daha dirençli ve hatasız çalışan yazılım üretmektir.

1. KAPSAM

Bu prosedür ZBEÜ Bilgi İşlem Daire Başkanlığı bünyesindeki yazılım geliştiren çalışanları kapsar.

2. SORUMLULUK

Bu prosedürün uygulanmasından tüm yöneticiler sorumludur.

3. TANIMLAR

Güvenli Yazılım: Yazılımın, saldırı veya tehdit altındayken işlevlerini doğru bir şekilde yerine getirmeye devam edecek şekilde korunmasıdır.

4. UYGULAMA

4.1 Kurum Üst Yönetimi tarafından sadece uygun görülen yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olunur.

4.2 Uygulama yazılımlarının kurum içerisinde mi hazırlanacağı yoksa satın mı alınacağının belirlenmesi Kurum Üst Yönetimi tarafından tanımlanır.

4.3 Yeni alınmış veya revize edilmiş bütün yazılımlar ile hazırlanan sistemler mevcut politikalar dâhilinde, işin gerekliliklerini yerine getirdiklerinden ve iç kontrol yapıldığından emin olunması açısından test edilir.

4.4 Eski sistemlerdeki veriler tamamen veya ihtiyaca yönelik şekilde, doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılır ve/veya uygun şekilde saklanır.

4.5 Her bir yazılım prosedürü kendi işini bitirmesi için gerekli en az hak kümesiyle çalıştırılır. En az yetki ilkesiyle aşağıdaki durumlar amaçlanır:

5.5.1 Uygulamanın sistem üzerinde yapabileceği değişiklikler sınırlanır

5.5.2 Bir uygulamadaki zayıflıkların sistemin geri kalanına sızmak için kullanılamaz.

5.5.3 Karmaşık ortamlara konuşlandırma kolaylaşır.

5.5.4 Sistem kaynaklarına erişmesi gereken uygulamalara yalnızca erişmesi gereken kısıtlı bölgeler için yetki verilir ve bu uygulamalar yönetici haklarıyla çalıştırılmaz.

5.5.5 Yükseltilmiş hakları gerektiren yazılım süreçleri bu haklara sadece gereken en az süre boyunca sahip olmalıdır.

5.6 Tüm erişimler denetlenir. Her bir nesneye yapılan erişimde yetki kontrolü yapılmalıdır.

5.6.1 Normal durumların dışında, başlatma, geri kazanım, kapatma, bakım safhalarında da erişim denetlenmelidir.

5.6.2 Bir istek alındığında yapılan yetki kontrolü aynı isteğin yanıtı verilirken de yapılmalıdır

5.7 Yetkiler ayrılmalıdır. Bir sistem yüksek güvenlikli bir işleme yalnızca tek bir koşula bağlı olarak izin vermemelidir. Yüksek güvenlikli bir işleme izin verilmesi için birden fazla koşulun sağlandığı doğrulanmalıdır.

5.8 Varsayılan değerler güvenliği artıracak şekilde seçilmelidir. Bu amaçla;

5.8.1 Çalıştırılabilir dosyalar varsayılan olarak herkesin yazabileceği şekilde kurulmamalıdır.

5.8.2 Uygulama ana dizini herkesin okuyabileceği şekilde kurulmamalıdır.

5.8.3 Herkesin yazabileceği iz kaydı dosyaları, herkes tarafından okunabilen dizinler bulunmamalıdır.

5.8.4 Herkesin okuyabileceği dosyalarda varsayılan (geliştirme, test) parolaları bulunmamalıdır.

5.8.5 Cihazlarda IP sahtekârlığına izin veren varsayılan ayarlar kullanılmamalıdır.

5.8.6 Paylaşılan anahtar dosya / veri tabanlarında güvensiz haklar verilmemelidir.

5.8.7 Bir öğeye özellikle bir nesne üzerinde erişim verilmemiş ise bu öğeye erişimde olmamalıdır.

5.8.8 Bir nesnenin varsayılan erişimi "*hiç*" olmalıdır.

5.8.9 Parola süresinin dolması, karmaşıklık kontrolü gibi kontroller varsayılan durum olmalıdır.

5.8.10 Kriptografik algoritmaların çalışma kümesi varsayılan olarak en güvenli küme olmalıdır.

5.8.11 Kimlik denetiminde en güvenli faktör varsayılan olarak kullanılmalıdır.

5.9 Kaynaklara erişen mekanizmalar ortak kullanılmamalıdır. (paylaşılan dosyalar gibi.) Ayrıca Ortak kanallardaki bilgi akışından kaynaklanan bilgi sızması/bozulması problemleri ve yan kanal saldırıları gibi problemlere neden olmaktadır. Ayrıca sistem ve yazılım içerisinde farklı bileşenler arasında da yalıtım sağlanmalıdır.

5.10 Zayıf halka tespit edilip güçlendirilmelidir. Güvenlik analizi aşamasında bu halka kendisine yönelik riski karşılayabilecek şekilde yeniden tasarlanıp gerçeklenmelidir.

5.11 Saldırı yüzeyi azaltılmalıdır. Bu yüzey yetkisiz bir kullanıcının ya da saldırganın yazılım ortamından veri alabileceği, veri girebileceği veya yetkisiz işlem yapabileceği noktaların tümüdür. Uygulamaya gereksiz özellikler eklenmemeli. İletişim yapılacak noktalar sınırlanmalıdır. Saldırı yüzeyi tasarım aşamasında belirlenmeli ve sürekli olarak izlenmelidir.

5.12 Savunma derinliği oluşturulmalıdır. Savunma derinliği, savunma mekanizmalarının peş peşe uygulanmasından oluşur. Bu şekilde bir savunma mekanizması aşıldığında, sistem tamamen savunmasız kalmaz. Bu durumda aşağıdaki hususlar dikkate alınmalıdır:

5.12.1 Yazılımdaki güvenlik mekanizmalarının, sistemdeki güvenlik mekanizmalarıyla entegrasyonu sağlanmalıdır.

5.12.2 Güvenlik politikalarının tüm bileşenlerde dikkate alınması ve zorunlu olarak uygulanması sağlanmalıdır.

5.13 Basit Güvenlik Mekanizması Tasarlanmalıdır. Bu şekilde hata olasılığının daha az olması sağlanır, hatalar oluştuğunda anlaşılması ve düzeltmesi kolaylaşır. Bu kapsamda özellikle arayüzlerin mümkün olduğunca basit olmalı ve dokümantasyon yapıılmalıdır.

5.14 Anlaşılabilir ve Kolay Kullanılabilir Güvenlik Mekanizması Tasarlanır. Kullanıcıyla etkileşim gerektiren güvenlik mekanizmaları anlaşılabilir ve kolay kullanılabilir olmalıdır. Aksi takdirde kullanıcı güvenlik mekanizmalarının etrafından dolaşmak için yollar arayabilir. Bu bağlamda aşağıdaki hususlar dikkate alınmalıdır:

5.14.1 Kullanıcı işini en kolay şekilde ancak en az yetkiyle yapabilmelidir.

5.14.2 Kullanıcı yapacağı işe ilişkin güvenlik politikalarını tanımlayabilmelidir.

5.14.3 Kullanıcının izin verdiğini gösteren eylemleriyle yetkilendirme otomatik olarak verilebilmelidir.

5.10.4 Kullanıcı daha önce verdiği yetkileri geri alabilmelidir.

5.14.5 Kullanıcı verdiği yetkileri görebilmelidir.

5.15 Tedarik edilen veya hizmet alımı ile geliştirilen uygulamalar için yazılımın kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) içermediğine/içermeyeceğine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde taahhütname alınmalıdır.

5.16 Geliştirme ve/veya test ortamında kullanılacak veriler gerçek veri olmamalıdır. Bu kapsamda, ilgili ortamlarda kullanılması için amaca uygun veriler üretilmelidir.

5.17 Üretici tarafından sunulan teknik desteği sona ermiş, güvenlik açığı barındıran veya teknolojisi zaman aşımına uğramış sunucu veya istemci teknolojileri kullanılmamalıdır.

5.18 Devreye alınan veya güncellenen uygulamalarda sızma testleri ve uygulama güvenliği testleri yapılmalıdır. Tedarik edilen uygulamalar üzerinde sızma testleri gerçekleştirilmelidir.

5.19 Kurumun kaynak koduna sahip olduğu tüm uygulamalar devreye alım öncesinde kaynak kod analizinden geçirilmelidir.

5.20 Güvenli yazılım geliştirme süreçleri ve olgunluk modellerinden faydalanılarak kurumsal yazılım geliştirme süreçleri güncellenmeli ve güvenli yazılım geliştirme yaşam döngüsü uygulanmalıdır.

SORUMLULUK

Bu prosedürün işletilmesinden Bilgi İşlem Daire Başkanlığındaki tüm personel sorumludur.

EK

ZBEÜ_FR_19-01 Canlıya Alma Formu