1. AMAÇ

Bu prosedürün amacı, Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde güvenli sistemler tasarlanmasını ve işletilmesini garanti altına almak için Güvenli Sistem Mühendisliği Prensiplerinin tanımlanmasıdır.

2. KAPSAM

Bu prosedürde belirtilen ve uyulması gereken hususlar üçüncü taraf firmalara yaptırılan ve Kurum içinde geliştirilen tüm bilgi sistemleri için geçerlidir.

3. TANIMLAR

4. REFERANSLAR

Bu dokümana ait referans yoktur.

5. UYGULAMA

5.1. Tasarım Aşaması İçin Temel Güvenlik Gereksinim Kriterlerinin Belirlenmesi

Tasarım bileşenleri, bileşenler arasındaki ara yüzler, dış sistemlerle geliştirilecek sistem arasındaki ara yüzlere, satın alınacak hazır ürünler ya da alt yüklenici tarafından geliştirilecek bileşenlere tasarım aşamasında karar verilmekte olup, tasarım kısıtları ortaya çıkartılmaktadır. Oluşturulan tasarım bileşenleriyle ilgili gereksinimler eşleştirilmektedir. Mimari oluşturulurken kabul gören patternlerden ve tasarım standartlarından yararlanılır. Bu faaliyetlerin sonucunda:

- Mimari tasarım için dayanak noktası oluşturulur.
- Tasarım modelleri oluşturulur.
- Gereksinimler, mimari ve tasarım arasında izlenebilirlik oluşturulur.
- Teknik riskler tanımlanır, gerekirse Proje Yönetim Planı güncellenir.
- Ara yüz gereksinimlerini sağlayan tasarım modelleri oluşturulur.
- Entegrasyon için genel kriterler belirlenir.
- Tasarım doğrulama kriterleri oluşturulur.
- Çözümün mantıksal, fiziksel ve veri yapısı oluşturulur.

Faaliyetlerin başarılı bir şekilde uygulanması sonucunda, gereksinimleri karşılayan tasarım birimleri oluşturulmakta olup, değişikliklerin kolayca tasarıma yansıtılabildiği, test sonucunda tasarıma bağlı hataların sürecin önceki sürümlerine göre azaldığı sonuç alınması hedeflenmektedir. Tasarımın değerlendirilmesi aşamasında esneklik, güvenilirlik, güvenlik, test edilebilirlik ve bakım kolaylığı, performans gibi kalite kriterleri kullanılır.

5.2. Güvenlik gereksinimlerinin, tüm sistem tasarım sürecinin ayrılmaz bir parçası olarak göz önünde bulundurulması

Bilgi sistemleri tasarım aşamasında güvenlik gereksinimlerinin, tüm sistem tasarım sürecinin ayrılmaz bir parçası olarak göz önünde bulundurulması gerekmektedir. Bu aşamada gereksinimlerin tasarım modeliyle doğru ve kaliteli bir şekilde karşılandığı ve güvenlik gereksinimlerini sağlamakta olduğu kontrol edilir. Tasarımın,

- Modüler
- Test edilebilir
- Bakımı kolay
- Kullanımı elverişli
- Güvenilir
- Performans sorunu olmayan
- Güvenlik açığı olmayan bir tasarım olması beklenir

Tüm gereksinimlerin tasarımla karşılandığı ve tasarımın mimari gereksinimleri sağladığının doğrulanması amacıyla kabul testleri gerçekleştirilir. Güvenlik kriterlerinin belirlenmesi sayesinde tasarım aşamasında potansiyel tehditler tespit edilerek bilgi sistem açıklıklarına yönelik aksiyonlar alınır ve bu sayede daha ileri fazlarda farkına varılan açıklıklara göre daha az maliyetli bir çalışma sağlanmış olur.

5.3. Bilgi sistemlerine yönelik geliştirme çalışmaları yapan kişilerin güvenli sistem geliştirme konusunda yeterli düzeyde bilgi seviyesine sahip olması

Bilgi sistemlerine yönelik geliştirme çalışmaları yapan personelin güvenli sistem geliştirme konusunda (tasarım, geliştirme, konfigürasyon kontrolü, entegrasyon ve test faaliyetlerine yönelik mühendislik disiplinleri) yeterli düzeyde bilgi seviyesine sahip olmasını garanti altına alacak eğitimler Bilgi İşlem Daire Başkanlığı kararı ile belirlenir ve bu kapsamda eğitim faaliyetleri organize edilir

5.4. İşlenen, transfer edilen ve depolanan bilginin korunması

Bilgi sistemlerinin ve bu sistemler tarafından işlenen, transfer edilen ve depolanan bilginin yetkisiz değiştirilmesi ya da yok edilmesi, eksik iletimi, yanlış yönlendirmeyi, yetkisiz mesaj değiştirmeyi, yetkisiz ifşayı, yetkisiz mesaj çoğaltmayı ya da erişilebilirliğinin zarar görmemesini garanti altına almak adına bilgi ile ilişkili riskler, risk değerlendirme sürecine uygun olarak yönetilir.
Ayrıca iç ya da dış kaynaklar tarafından gerçekleştirilen bilgi sistemlerine yönelik her türlü geliştirme faaliyetinde; girdi, veri transfer, işlem ve çıktı kontrolleri ile verilerin tamlığını, kullanılabilirliğini ve ihtiyaç duyulan seviyede güvenliğinin sağlanması amacıyla uygulanacak kurallar Yazılım Geliştirme Prosedüründe tanımlanmaktadır.

5.5. Güvenlik Kontrollerinin Belirlenmesi

Güvenlik kontrollerinin belirlenmesi aşamasında passive monitoring, active network attacks, exploitation by insiders, the insertion of backdoors and malicious code during information system development and/or distribution gibi potansiyel saldırı türleri göz önünde bulundurulmalıdır.

5.6. Erişim yetkilendirmesine ihtiyaç duyulmayan sistemlerin kritik hassas sistemlerden izole edilmesi

Hassas sistemlerin yalıtılmış bir bilgi işlem ortamına sahip olması sağlanmalıdır. Erişim Kontrolü Politikası ile Kurumun Bilgi Varlıklarına sadece yetkili kişi veya grupların tanımlanan haklar dâhilinde erişebilmesi mümkündür.

Bilgi sistemlerine yönelik faaliyetlerin, ayrıcalıkların ve bilgi güvenliği olaylarının kayıt edilmesini, ileride yapılabilecek soruşturmalar ve erişim kontrolü izlemeye yardımcı denetim mekanizmalarının uygulanması

Verilere erişimde Yetkilendirme Talimatı ile Kurumun bilgi sistemlerine hangi kurallar ve şartlar dahilinde, hangi öznelerin, hangi yetki ve imtiyazlarla erişebileceği bir esasa bağlanmaktadır. Bilgi sistemlerine yapılan tüm başarısız erişimlerin tarih, zaman ve erişilen kaynağın detayı ile ilgili bilgilerinin kayıtları tutulmakta olup; öznelerin sistemde hangi işlemleri yaptıklarının veya hangi nesnelere eriştiklerinin bilinmesi ve gözlenebilmesi mümkün kılınmaktadır.

5.7. Gerektiği Kadar Yetki Prensibinin Uygulanması

Özel olarak yetkilendirme yapılmadığı sürece Kurum kullanıcılarının tüm bilgi sistemlerine erişim sağlanmamakta olup, kullanıcılara sadece iş sorumluluklarını veya iş gereksinimlerini yerine getirmelerine yetecek kadar izin verilmektedir.

Kurum bünyesinde gerçekleştirilmekte olan erişim kontrolü kimlik doğrulama (authentication), yetkilendirme (authorization) ve izlenebilirlik (accountability) kavramlarını içine almaktadır. Her kullanıcının kendine ait ve kendisini benzersiz olarak tanımlayan bir kullanıcı hesabı bulunmakta olup, tüm kullanıcı hesaplarına ait bir parolanın olması sağlanmaktadır.

6. SORUMLULUK

Bilgi İşlem Daire Başkanlığı personeli sistem geliştirmelerini bu prosedüre uygun olarak gerçekleştirmekten sorumludur.

7. KONTROL

Dokümanlar ihtiyaç halinde revize edildiği gibi, yılda bir kez periyodik olarak kontrol edilir.

8. EKLER

Dokümanın eki yoktur.