1. Amaç

Bu doküman, bilgi güvenliğinin Kütüphane ve Dokümantasyon Daire Başkanlığı'nın bilgi sistemlerinin yaşam döngüsü boyunca bir parçası olmasını sağlamak için gerekli hususları belirlemek amacıyla oluşturulmuştur.

2. Kapsam

SDÜ0PL07 BGYS Sistem Edinimi Bakım ve Geliştirme Politikası, SDÜ6GE01 BGYS Kapsamı dokümanında belirtilen tüm bilgi sistemlerini kapsar.

3. Tanımlar

Kurum: Kütüphane ve Dokümantasyon Daire Başkanlığı

BGYS: Bilgi Güvenliği Yönetim Sistemi

4. Uygulama

4.1 Bilgi Güvenliği Gereksinimleri

Bilgi güvenliğine ilişkin gereksinimler, yeni bilgi sistemleri gereksinimlerine ya da mevcut sistemlerin iyileştirmeleri dahil edilir.

Bilgi güvenliği gereksinimleri belirlenirken, politikalar, düzenlemeler, tehdit modellemesi, zafiyet ve olay analizlerinde yararlanılır. Söz konusu gereksinimler, tüm paydaşlar tarafından onaylanır.

Bilgi güvenliği gereksinimleri ve kontroller, iş etkisi ve işlenen verinin değeri göz önüne alınarak belirlenir.

Bilgi güvenliği gereksinimleri, daha etkili ve düşük maliyetli olmasını sağlamak amacıyla projelerin tasarım aşamasında ortaya konur.

Bilgi sistemlerinin güvenlik gereksinimleri belirlenirken, aşağıdaki hususlar temel alınır.

- Kimlik doğrulama
- Yetkilendirme

- Erişim ve olay kayıtlarının yönetimi
- Kapasite ve performans izleme
- İş Sürekliliği ve felaketten korunma
- Yedekleme

Güvenlik gereksinimleri, satın alma prosesinde teknik şartnamelerde, tedarikçi sözleşmelerinde belirtilir.

Sistemlere ilişkin satın alma, güvenlik gereksinimlerinin karşılandığının belirlenmesi ve bu gereksinimlerin ilgili teknik birimlerce test edilip onaylanması ile gerçekleştirilir.

4.2 Halka Açık Ağlardaki Uygulama Hizmetlerinin Güvenliği

Halka açık ağlar üzerinden geçen uygulama hizmetlerindeki bilgi, yetkisiz erişim ve değiştirme faaliyetlerinden korunur.

Bu kapsamda, aşağıdaki hususlar göz önüne alınır:

Halka açık kritik sistemlerde, uygulama sunucuları DMZ'te veri tabanları ise iç ağda konumlandırılır. Uygulama sunucuları ile veri tabanları ya da diğer iç sistemlerle iletişim, yalnızca gerekli iletişim kanalları aracılığıyla gerçekleştirilir.

Halka açık sistemlerin yönetim panellerine yalnızca kurum iç ağından erişilebilir.

Sözleşme koşulları ve işlenen bilginin değeri ile uyumlu kimlik doğrulama sistemi kullanılır.

İnkâr edilemezliğin söz konusu olduğu uygulamalarda, gerekli teknik kontroller uygulanır.

Sisteme ilişkin yetkilendirme, yılda en az bir kez kontrol edilmek amacıyla paydaşlarla paylaşılır.

Paydaşlara ilişkin ticari, kişisel ve hassas kategorideki verilerin gizliliği sağlanır.

4.3 Uygulama Hizmet İşlemlerinin Korunması

Uygulama hizmet işlemlerindeki bilgi, eksik iletim, yanlış yönlendirme, yetkisiz değiştirme, ifşa ve yeniden oluşturma girişimlerine karşı, SSL protokolleriyle korunur.

İletişimin, gizli kimlik doğrulama bilgilerinin geçerli olması ve doğrulanması ile başlaması sağlanır. Uygulama, kimlik doğrulama yapmadan, anonim erişime kapalı olan servis ve arayüzlere erişimi engelleyecek ya da bu tür erişimlerin denetlenebileceği ve yönetilebileceği mekanizmalara sahip olacak şekilde tasarlanır.

Uygulamanın, müşteri tarafından tanımlanmış olan kritik servisleri ve ayarları için güçlü kimlik doğrulama mekanizmaları tasarlanır.

Uygulama, DOS ya da kaba kuvvet saldırısı ihtimalinin olmadığı ortamlarda, önceden belirlenmiş hatalı kimlik doğrulama deneme eşiğinin aşılmasıyla hesap kilitlenecek ve yeniden aktive edebilecek mekanizmaya sahip olması sağlanır.

Kullanıcıların gizli kimlik bilgilerinin, aktarım sırasında korunabilmesi amacıyla teknik kontroller uygulanır. Kriptografik kontroller, tüm kimlik denetimi prosesi sırasında kullanılacak şekilde tasarlanır.

Kimlik doğrulama sırasında ve hata durumlarında, kullanıcıya mümkün olduğunca az bilgi ile geri bildirim yapılır.

Kimlik doğrulama prosesinde, internet tarayıcılarının kimlik bilgilerini tutması engellenir.

İletişim kanalındaki verinin gizlilik ve bütünlüğünü korumak amacıyla güvenli ağ protokolleri kullanılır ve kriptografik kontroller uygulanır. İletişimde, uçtan uca gizliliği destekleyecek uygulama servisleri kullanılır.

İşlemlere ilişkin verilerin depolanması için halka açık depolama platformları kullanılmaz.

İletişim sırasında güvenli bir sertifika otoritesinin kullanılması durumunda güvenlik, sıra ile tüm sertifika yönetimi süreci boyunca yerleştirilir ve gömülü hale getirilir.

4.4 Uygulama Geliştirme ve Bakımı

Geliştirme ortamının güvenliği sağlanır.

Yazılım geliştirme yaşam döngüsü içinde, güvenli metodolojiler kullanılır

Kullanılan diller için güvenli kodlama kılavuzları izlenir.

Güvenlik gereksinimleri, tasarım aşamasında belirlenir.

Kaynak kodları ve işlenen veri güvenli veri depolarında barındırılır.

Versiyon kontrolünde güvenliği sağlayabilmek amacıyla değişiklik yönetimi uygulanır.

Geliştirme, güvenli kodlama standartları ve tekniklerini kullanan, güvenlik açıklıklarından kaçınma, mevcut açıklıkları bulabilme ve onarabilme yeteneğine sahip kişilerin sorumluluğuna verilir.

Geliştirme yaşam döngüsü içerisindeki sistem değişiklikleri, SDÜ0PL09 BGYS İşletim Güvenliği Politikası kapsamında tanımlanan değişiklik yönetimi prosesi ile gerçekleştirilir.

Uygulamaya ilişkin işletim sistemi, veri tabanı yönetim sistemi ve ara katman platformu gibi işletim ortamlarının değişmesi durumunda, kritik uygulamalar gözden geçirilir ve test edilir.

Paket yazılımlarda, gerekmedikçe değişiklik yapılması engellenir ve değişiklikler sıkı bir şekilde kontrol edilir.

Paket yazılımlarda değişiklik yapılması gerektiğinde aşağıdaki hususlar göz önüne alınır

Diğer uygulamalarla uyumluluk ve bakım gereksinimlerinin maliyeti değerlendirilerek, değişikliğin iç kaynak ya da üretici tarafından gerçekleştirilmesine karar verilir.

Üretici tarafından yapılacak değişikliklerin, güncelleme paketi şeklinde geliştirilmesi sağlanır.

Değişikliğin iç kaynak ile yapıldığı durumda, gerekliyse üreticinin onayı alınır.

Dış kaynaklı geliştirme ve bakım faaliyetlerinde, söz konusu hususların göz önüne alındığı ilgili sözleşme ve kontrollerle sağlanır.

Tedarikçi ya da hizmet sağlayıcılarla yapılacak sözleşmelerle, güvenlik gereksinimleri açıkça belirtilir. Güvenlik kriterlerine uygun olmayan ürünler değerlendirme dışı tutulur.

İhale şartnamelerinde beklenen kurulum, devreye alma, eğitim, bakım ve destek koşulları açıkça belirtilir.

Tedarik edilen sistem ve uygulamaya ilişkin lisans ve kod sahipliği ile fikri mülkiyet haklarına ilişkin detaylı bilgiler, sözleşme ile netleştirilir.

Sistemin hedeflenen çıktıları ve güvenlik seviyesini sağlayabildiğinin kontrolü için, gerekli durumlarda kod ve zafiyet analizi araçlarının da kullanıldığı kabul testleri gerçekleştirilir. Belirlenen zafiyetler kapatılmadan, sistem canlı ortama alınmaz.

Bilinen güvenlik açıklarına karşı korunmanın sağlandığına dair yazılı test sonuçları temin edilir.

Test için kişisel veriler ve gizlilik içeren veriler kullanılmaz. Bu tür verilerin kullanılması gerektiğinde, değiştirme ya da anonimleştirme teknikleri uygulanır.

Canlı verilerden kopya çıkartılarak oluşturulan geliştirme ve test ortamlarında, erişim yetkileri kontrol edilir.

Uygulama bileşenlerinin, silinmiş verilere yeniden ulaşımı engellenir. Bellekte ya da disk sisteminde oluşturulan nesnelerin gizli veri içermemesi sağlanır. Uygulamanın, geri dönüşü olmayacak şekilde silinmiş verilerin, artık uygulama içinde erişilememesini ve yeni üretilen verilerin, geri dönüşü olmayacak şekilde silinmiş bilgi içermemesini garanti etmesi sağlanır.

Son kullanıcının, uygulamayı birden fazla ekranda kullanması durumunda, söz konusu ekranlar ya da raporlama ara yüzleri üzerinden sunulan bilginin tutarlılığı sağlanır.

Uygulamanın etkileşim halinde olduğu sistemin sınır güvenliğini sağlamak için önem arz eden veri akışının kontrolü ile verinin sistem içinde ya da sistemler arasında nerelerde dolaşabileceği belirlenir

Uzaktan çalıştırılabilen ya da sistemin değişik parçaları arasında aktarılan taşınabilir kodların envanteri tutulur.

Uygulama, herhangi bir fonksiyonu çalışmaya başlamadan önce güvenlik fonksiyonlarının çalışır ve ayakta olduğunu garanti edecek şekilde tasarlanır.

Uygulamanın veritabanı gibi kaynaklara erişim için kullandığı parolalar şifrelenmiş şekilde barındırılır.

Uygulamaya, istemci rolüne sahip erişim sağlayan diğer sistemlerin kimlik doğrulama prosesinde kullandıkları parolaların kriptografik özetleri (hash) saklanır. Özet için kuvvetli algoritmalar kullanılır.

Veri dağıtım servisleri kullanan uygulamalar, dağıtık yapıda çalışan servislerin güvenlik zafiyetlerine daha açık durumda olması nedeniyle, erişim için gizliliği korunmuş kanallar aracılığıyla eriştirilir.

Uygulama, performans sorunlarından kaçınmak amacıyla, yetkilendirilmiş kullanıcılara bir kullanıcının açabileceği oturum sayısını yönetebilme olanağını sağlayacak şekilde tasarlanır.

Uygulama, yetkilendirilmiş kullanıcıların olay kayıtlarını saklama süresini ayarlayabilecekleri mekanizmalara sahip olacak şekilde tasarlanır.

Uygulama, denetlenmesi gereken olayların tümü için denetim kaydı tutacak şekilde tasarlanır. Söz konusu kayıtların kullanıcı kimliği ile söz konusu olayları birleştirecek, olayın tarih ve saatini, ne tür bir olay olduğunu, kullanıcı kimliğini ve olayın sonucunu içerecek şekilde olması sağlanır. Uygulamalarda aşağıdaki kayıtların tutulması zorunludur:

- Sunucu ya da bileşenlerinin açılması, kapatılması ve yeniden başlatılması
- Oturum açılış ve kapanışları
- Yetki ve rol güncellemeleri
- Kullanıcı ya da gruplara rol atamaları
- Güvenlik fonksiyonları ile ilgili uygulama ve sistem ayarlarını değiştirme ekranına erişim durumları ve güncellemeler
- İzleme ve denetim fonksiyonlarının açılış ve kapanışları
- Güvenlik fonksiyonu sunan servislere, sayfalara ya da verilere her türlü erişim
- İzleme ve denetim kayıtlarının oluşturulması, silinmesi ya da değiştirilmesi
- Sistemin tarih ve saatinin değiştirilmesi
- Sistem kaynaklarına başarısız erişim denemeleri

Uygulama, zararlı kod enjeksiyonlarından korunmak amacıyla, girdi denetimi yapacak şekilde tasarlanır.

Uygulama, açıklık içermediği bilinen, en güncel üçüncü parti kütüphane sürümlerini kullanarak tasarlanır. Kullanılan tüm üçüncü parti ürünler, periyodik olarak güncellenir.

Uygulama, hakkında mümkün olduğu kadar az bilgi vermek amacıyla, sunucu hatası durumunda, kullanıcılara özel hata mesajları iletilecek şekilde tasarlanır.

Uygulama, kendi oluşturduğu dosyaların izinlerinin bozulması durumunda, yetkileri eski haline getirmeyi mümkün kılan mekanizmalar sunacak şekilde tasarlanır.

Uygulama, gizliliği korumak amacıyla, istemci tarafına gönderilen verilerde kullanıcının ihtiyacı olmayan bilginin bulunmamasını sağlayacak şekilde tasarlanır.