1. BİLGİ SİSTEMLERİ EDİNİM, GELİŞTİRME VE BAKIMI

Bilişim sistemleri içerisinde güvenliğin temin edilmesi, uygulama sistemlerindeki kullanıcı verilerinin kaybedilmesini, değişmesini ya da hatalı kullanımının önlenmesi, bilginin gizliliği, aslına uygunluğu ya da bütünlüğünün korunması, IT projelerinin ve destek etkinliklerinin güvenli bir şekilde yürütülmesini temin etmek ve uygulama yazılımının ve bilgilerin güvenliğini sağlamaktır.

1.1. BİLGİ SİSTEMLERİNİN GÜVENLİK GEREKSİNİMLERİ

Güvenlik Gereksinimlerinin Analizi ve Özelleştirilmesi

- Yeni sistemlerin geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır.
- Ortaya konan güvenlik gereksinimleri bilgi varlıklarının değerini ve bir güvenlik açığı dolayısıyla oluşabilecek zararı yansıtıyor olmalıdır.
- Sistem geliştirilirken işin başından itibaren güvenlik ihtiyaçları göz önünde bulundurulmalıdır.
- Satın alınan ürünler için resmi bir test ve tedarik süreci işletilmelidir.

1.2. UYGULAMALARIN DOĞRU ÇALIŞMASI

Girdi Verilerinin Kontrolü

- Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontrol yapılmalıdır.
- Ne tür kontroller yapılıyor?
- İş hareketlerinin daimi veri (isim, adres, vb) ve parametre tabloları (döviz kurları, vergi oranları gibi) girişlerine kontroller uygulanıyor olmalıdır.

İç İşleyişin Kontrolü

- Doğru girilmiş bilginin işlem sırasında hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmelidir.
- Uygulamalar, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmış olmalıdır.

Mesaj Bütünlüğü

- Mesaj bütünlüğü gereksinimini belirlemek için güvenlik ihtiyaçları değerlendirilmiş ve gereken önlemler alınmış olmalıdır.
- Mesaj doğrulama yöntemi olarak kriptografik teknikler kullanılmalıdır.

Çıktı Verilerinin Kontrolü

- Saklanan bilgilerin üstünde gerçekleştirilen işlemlerin doğru ve şartlara uygun olduğundan emin olmak için uygulama çıktılarının denetimi yapılmalıdır.
- Bu çerçevede çıktı verilerin makul değerler alıp almadığı, tüm verinin işlenip işlenmediği, çıktı veriyi işleyen sisteme verinin bütünlüğünü ve doğruluğunu sınamasını sağlayacak bilginin verilip verilmediği kontrol edilebilir.

1.3. KRİPTOGRAFİK KONTROLLER

Kriptografik Kontrollerin Kullanımına İlişkin Politika

- Bilginin korunması için kriptografik kontrollerin kullanılmasını düzenleyen politika geliştirilmiş ve uygulamaya alınmış olmalıdır.
- Politika oluşturulurken bilginin korunması ile ilgili genel prensipler ve yönetimin konuya yaklaşımı göz önünde bulundurulmalıdır.
- Kullanılacak güvenlik seviyesine karar vermek için risk değerlendirmesi yapılmış olmalıdır.
- Taşınabilir ortamlar ve iletişim kanallarındaki hassas bilginin korunması için kriptografik kontrollerin uygulanması düşünülmüş olmalıdır.
- Anahtar yönetimi ile ilgili güvenlik hususları düzenlenmelidir. (anahtarın saklanması, anahtarın kaybolması durumunda şifrelenmiş bilginin kurtarılması vb)
- Roller ve sorumluluklar tanımlanmalıdır.

Kriptografik Anahtar Yönetimi

- Kurumun kriptografik teknikleri kullanmasına imkân sağlamak için anahtar yönetimi gerçekleştiriliyor olmalıdır.
- Anahtar yönetim sistemi tanımlı standartlar, prosedürler ve güvenli yöntemler esas alınarak oluşturulmuş olmalıdır.
- Algılanan risk ve kullanım şartları uyarınca anahtarların sınırlı bir süre boyunca kullanılabilmesi için gereken düzenlemeler yapılmış olmalıdır.

1.4. SİSTEM DOSYALARININ GÜVENLİĞİ

Çalışmakta Olan Yazılımın Kontrolü

- Çalışan sistemlere yazılım yüklenmesini bozulma riskini asgariye indirmek için, düzenleyen prosedürler olmalıdır.
- Yazılım yükleme, eğitimli sistem yöneticileri tarafından ve sadece yönetim yetkilendirmesi ile yapılmalıdır.
- Çalışan sistemde geliştirilmekte olan yazılım ve derleyici bulunmaması sağlanmış olmalıdır.
- İşletim sistemi ve uygulama yazılımlarının iyice test edilmeden yüklenmemesine dikkat edilmelidir.

- Konfigürasyon kontrol sistemi aracılığı ile eski ve yeni yazılım sürümleri, yazılımla ilgili dokümantasyon ve konfigürasyon bilgileri ve sistem dokümantasyonu saklanıyor olmalıdır.
- Üçüncü taraflardan alınmış yazılımın kullanılması, güvenliği ve bakımı ile ilgili riskler göz önünde bulunduruluyor olmalıdır.

Sistem Test Verilerinin Korunması

- Sistem testi için kullanılan veri dikkatle oluşturuluyor ve korunuyor olmalıdır. (Kişisel bilgiler ve diğer hassas bilgileri içeren aktif veri tabanının sistem testi için kullanılmasından kaçınılmalı, canlı sistem bilgileri test sırasında kullanılacaksa içindeki gizli bilgiler çıkarılmalıdır.)

Program Kaynak Kütüphanesine Erişim Kontrolü

- Program kaynak kodlarının bulunduğu kütüphanelere erişim sıkı bir şekilde denetlenmelidir. (Bu önlem yetkilendirilmemiş, kontrolsüz değişikliklere engel olmak içindir).

1.5. GELİŞTİRME VE DESTEK SÜREÇLERİNDE GÜVENLİK

Değişim Kontrol Prosedürleri

- Bilgi sistemleri üzerinde yapılacak değişiklikler resmi kontrol prosedürleri aracılığı ile denetleniyor olmalıdır.
- Yeni sistem ilaveleri ve büyük değişiklikler resmi bir belgeleme, tarif, test ve kalite kontrol süreci uyarınca gerçekleştiriliyor olmalıdır.

İşletim Sistemi Değişikliklerinin Ardından Uygulamaların Teknik Olarak Gözden Geçirilmesi

- İşletim sisteminde yapılan değişikliklerin ardından kritik uygulamaların gözden geçirilip test edilmesini sağlayan süreç veya prosedürler geliştirilmiş olmalıdır.
- Değişiklik gerçekleştirilmeden belli bir zaman önce ilgili yerlere haber verilerek test ve gözden geçirmelerin yapılması sağlanmalıdır.

Yazılım Paketlerinde Yapılacak Değişikliklerin Kısıtlanması

- Yazılım paketleri üzerinde değişiklik yapılması gerçekten gerekli olduğu durumlar dışında engellenmelidir. (Hazır yazılımlar mümkün olduğu sürece değiştirilmeden kullanılmalıdır.)
- Değişikliğin kaçınılmaz olduğu durumlarda programın gömülü kontrollerine ve bütünlüğüne ilişkin süreçlerin tahrip edilmemesine, üreticiden izin almak gerekip gerekmediğinin düşünülmesine, gerekli değişikliklerin üretici tarafından standart yazılım güncellemeleri çerçevesinde gerçekleştirilip gerçekleştirilemeyeceğinin soruşturulmasına, değişiklik sonucunda yazılımın bakımının kuruluş tarafından sürdürülmesi gerekirse bu durumun kabul edilebilir olup olmadığının değerlendirilmesine dikkat edilmelidir.

Bilgi Kaçağı

- Bilgi kaçağına karşı denetim olmalıdır.
- Kurum dışına çıkan ortamların denetlenmesi, personel ve sistem aktivitelerinin izlenmesi ve bilgisayar ortamındaki kaynak kullanımının izlenmesi gibi denetimler yapılmalıdır.
- Sistem ve yazılım bütünlüğü yönünden açıklığı düşük olan (ISO/IEC 15408 Ortak Kriterler standardına uygun) ürünlerin kullanılması tercih edilmelidir.
- İzleme yapan kişi veya kurumların bilgi edinmesine engel olmak için sistem ve iletişim karakteristiği maskeleniyor olmalıdır.

Dış Kaynaklı Yazılım Geliştirme

- Dış kaynaklı yazılım geliştirme faaliyetleri izleniyor ve denetleniyor olmalıdır.
- Lisans anlaşması, fikri mülkiyet hakları, kalite güvencesi, denetleme için erişim hakkı, kurulum öncesi "Trojan" kod araması için test hususları düşünülmüş olmalıdır.

1.6. TEKNİK AÇIKLIK YÖNETİMİ

Teknik Açıklıkları Kontrolü

- Kullanılan bilgi sistemlerinin teknik açıklıkları ile ilgili bilgiler zamanında toplanıyor, bunlara bağlı olarak kurumun nasıl etkileneceği değerlendiriliyor ve riski azaltmak için uygun tedbirler alınıyor olmalıdır.
- Varlık envanterinin güncel ve eksiksiz olarak tutulmasına özen gösterilmelidir.
- Teknik açıklık yönetimi ile ilgili rol ve sorumluluklar belirlenmiş olmalıdır. (Yazılım şirketleri yama çıkarma konusunda zaman zaman büyük baskı altında kalmakta ve çıkardıkları yamalar problemlere çözüm getiremeyebilmektedir. Bu konuda "Değişiklik Yönetimi" başlığı altındaki prosedürler göz önünde bulundurulabilir)