MAKÜ

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

BİLGİ SİSTEMLERİNİN GÜVENLİK GEREKSİNİMLERİ PROSEDÜRÜ

İçindekiler

1 Amaç

Bu dokümanın amacı, kapsam analizi dokümanında belirtilen birimlerde bilgi güvenliğinin, bilgi sistemlerinin tüm yaşam döngüsü boyunca dâhili bir parçası olmasını sağlamak ve halka açık ağlar üzerinden hizmet sağlayan bilgi sistemleri gereksinimlerini karşılamaktır.

2 Kapsam

Bu doküman, kapsam analizi dokümanında belirtilen tüm bilgi varlıklarını kapsamaktadır.

3 Sorumluluk

Görev / Rol/Unvan	Dokümanın Hazırlanması	Dokümanın Kontrolü	Dokümanın Onaylanması	Dokümanın Yayınlanması	Dokümanın Güncellenmesi	Dokümanın Uygulanması	Dokümanın Uygulamadan Kaldırılması
Üst Yönetim			X			X	X
Üst Yönetim Temsilcisi			X			X	X
BGYS Yöneticisi	X	X		X	X	X	
BGYS Birim Sorumlusu	X	X				X	
Diğer Çalışanlar						X	

4 Tanımlamalar ve Kısaltmalar

Terim	Tanım/Açıklama
Kurum	Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri
BGYS	Bilgi Güvenliği Yönetim Sistemi
Demo	Ürün özelliklerini ve işlevlerinin tanıtılması ve test edilmesi
Firmware	Donanımın işlevini yerine getirmesi için gerekli yazılım

5 İşlem Detayı

5.1 Bilgi Güvenliği Gereksinimleri Analizi ve Belirtimi

Bilgi güvenliği ile ilgili gereksinimler, yeni bilgi sistemleri gereksinimlerine veya var olan bilgi sistemlerinin iyileştirmelerine dâhil edilmelidir. Yeni edinimler için yapılan kontroller geliştirme ve kullanılan sistemler içinde geçerlidir.

Yeni edinimlerde resmi bir test süreci takip edilmelidir. Tedarikçi ile sözleşmelerle belirlenen güvenlik gereksinimlerini ele almalıdır. Teklif edilen ürünün güvenlik işlevselliği belirtilen gereksinimi karşıladığı tekrar gözden geçirilmelidir.

Ürünleri satın almadan önce kabul kriterleri tanımlanmalı ve değerlendirilmelidir. Ek işlevsellik önemli olmadığı sürece kabul edilmemeli eğer edilecek ise ek riskler oluşmadığından emin olmak için gözden geçirilmelidir.

1. Herhangi bir sistem yeni alınacaksa alım işlemi yapılmadan önce gerekli şartlar uygun olduğu takdirde öncelikle demo yapılmalı ve yeni bilgi sisteminin gerekliliğine karar verildikten sonra ihtiyacalar kurum dışından karşılanacak ise şartnameler ile bilgi sisteminin bakım, kurulum ve destek kısımları açıkça belirtilecek şekilde alım yapılır.
2. Fiziksel bir donanım canlı ortama aktarılmadan önce gerekli tüm güncelleştirmeleri (Firmware, yama, anti virüs) yapılmalı, uygulama ajanları yüklenmeli ve gerekli olan diğer konfigürasyonlar tamamlanmalıdır.
3. Yeni bilgi sistemleri canlı ortama aktarılmadan önce zafiyet testleri yapılmalı, güvenlik gereksinimlerini karşılamak için tespit edilen açıklıklar kapatıldıktan sonra çalışan ortama aktarılır.
4. Kurum tarafından geliştirilen veya üçüncü taraflardan temin edilen her türlü yazılım veya yeni bilgi sistemi öncelikle test ortamında çalıştırılmalı ve kullanıcılar tarafından test ortamında gerekli testler yapıldıktan sonra herhangi bir sorunla karşılaşılmadığı takdirde var olan canlı ortama aktarılır.
5. Yapılan değişiklikler “İşletim Prosedürleri ve Sorumlulukları Prosedürü” ’ne göre yapılır.

Bilgi güvenliği gereksinimleri, politikalar ve düzenlemeler, tehdit modelleri olay yorumları, ya da güvenlik açığı eşikleri gibi kaynaklar kullanılarak tespit edilir. Sonuçlar tüm paydaşlar tarafından belgelenir ve gözden geçirilir.

Bilgi güvenliği gereksinimleri tanımlanmalı ve yönetim bilgi sistemleri projelerinin erken aşamalarında entegre edilmelidir. Bilgi güvenliği gereksinimleri ilgili süreçlerin erken aşamalarında almak, (Örnek; Tasarım) aşamasında daha etkin ve düşük maliyetli çözümlere elde edilmesini sağlar. Proje aşamasında aşağıdaki ihtiyaçlar göz önünde bulundurulur;

- Kimlik doğrulamaya ilişkin ihtiyaçların analizi
- Uygulamaya ilişkin roller ve sorumlulukların analizi
- Roller ve sorumluluklara ilişkin tüm yetkilerin analizi
- Uygulamalar üzerinde hangi seviyede kayıt(log) alınacağının analizi
- Uygulamalar/varlıkların gizlilik, bütünlük ve erişilebilirlik açısından analizi

5.2 Halka Açık Uygulama Servislerinin Güvenliği

Halka açık sistemlerin güvenliği için aşağıdaki konular göz önünde bulundurulur;

1. Yayınlanmadan önce kurumun ilgili süreçler için gerekli prosedürlere uygun olduğu kontrol edilir.
2. Gerekli tüm alanlar ve bileşenler için kimlik doğrulama mekanizmalarının ihtiyaç duyulan seviyede uygulanır.
3. Halka açık sistemler üzerinde yetkilendirmeler ihtiyacı kadar bilme prensibine göre yapılandırılır.
4. Halka açık sistemler üçüncü taraflarca kullanılacaksa, verilen yetkiler hakkında bilgilendirme yapılır.
5. Halka açık kimlik doğrulama adımı içeren tüm bileşenler üzerinde trafik şifreli olarak iletilir ve tüm iletişim için şifreli kanallar kullanılır.
6. Halka açılan verinin gizliliği göz önünde bulundurulur.
7. Halka açık uygulamaların yönetim panellerine sadece kurum iç ağından erişilir.
8. Form alanları dolandırıcılığa karşı korunmak için uygun olarak seçilir.
9. Kritik uygulama sunucuları DMZ üzerinden konumlandırılır. Veri tabanına doğrudan erişim verilmez. Veri tabanı üzerindeki kritik veriler hashlenerek saklanır.
10. Halka açık sistemler üzerinde, IP adresi, erişim bilgisi, yapılan istekler loglanır. Sistemler ek log yönetimi ihtiyacı varlık sahibi veya ilgili varlığın operasyon sorumlusu tarafından analiz edilir.

5.3 Uygulama Hizmet İşlemlerinin Korunması

Uygulama servislerinin iletişiminde, uygulamanın hassaslığına göre aşağıdaki konu başlıkları dikkate alınır;

1. Güvenilir bir otorite (dijital imza ve dijital sertifikaların verilmesi) kullanıldığı durumlarda güvenlik uçtan uca sertifika / imza yönetimi süreç boyunca entegre olarak sağlanır.
2. Veri tabanı bileşenlerinin doğrudan internete açılmaması sağlanır.
3. İlgili tüm taraflar arasında iletişim kurmak için kullanılan protokoller sabitlenir.
4. Kullanıcı kimlik doğrulama bilgilerinin doğru ve geçerli olduğu doğrulanır.
5. İletimin/iletişimin güvenilir olduğu doğrulanır.
6. İletim kanallarının şifreli olması sağlanır.

Revizyon Kayıtları

Rev. No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No	Onaylayan	İmza
1					
2					
3					
4					
5					