MAKÜ

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

TEKNİK AÇIKLIKLARIN KONTROLÜ PROSEDÜRÜ

İçindekiler

1 Amaç

Bu dokümanın kapsam analizinde belirtilen birimlerde gerçekleştirilecek teknik açıklık kontrol ve yönetim prosedürünü açıklamaktır.

2 Kapsam

Bu doküman Bilgi Güvenliği Kapsam Analizi dokümanında yer alan birimlerdeki bilgi varlıklarını kapsar.

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
Zafiyet Tarama Yazılımı	Varlıklar üzerindeki açıkları kontrol etmek için kullanılan yazılımlar.
Teknik Varlıklar	Sunucular, aktif cihazlar, router, switch, vb.
OWASP, OSSTMM	Teknik testler için uygulanabilecek metodolojiler
Yama	Teknik varlıklarda bulunan açıkların kapatılması için kullanılan düzeltmeler**.**
Test Sorumlusu	Testi yapan kişi veya ekip lideri

5 İşlem Detayı

5.1 Bilgi Güvenliği Denetimlerini Planlama

1. Kurumda teknik açıklıkların testleri BGYS Üst Yönetim Temsilcisinin atadığı personeller ya da 3. taraflar ile gerçekleştirir.
2. Sistemler en az yılda 1 defa olmak üzere düzenli şekilde Kurum iç ağına ve Kurumun sahip olduğu dış IP'lerine yapılan teknik açıklık testleriyle kontrol edilecek ve test sonuçlarına göre gerekli önlemler **Risk Yönetimi Prosedürü** ne göre alınır.
3. Sisteme yeni varlıklar eklenmesi ya da sistemlerde anormallikler görülmesi durumunda süreç dışında da güvenlik testleri yapılır.
4. Testlerden önce, ayrıcalıklı olacak varlıklar mevcut ise varlık sahiplerinin varlık bilgisini iletmesi beklenir. Teste tabi tutulmayacak varlıklar için bilgi iletilmemesi durumunda ayrıcalıklı bir varlık olmadığı kabul edilir.
5. Düzenli yapılan testler dışında gelebilecek test istekleri ve ayrıcalık tanımlamaları mail yolu ile iletilecek ve talep edilecektir.
6. Teknik testler sırasında oluşan her türlü sorun derhal test sorumlusuna bildirilecek, test sorumlu gerekli iletişimleri sağlayarak durumun yönetilmesinden sorumlu olacaktır.
7. Taramalar sonucu çıkan raporlar test sorumlusu tarafından incelenecek ve gerekli görüldüğünde 3. taraflardan destek alınabilir.
8. Raporlarda çıkan zafiyetlerin giderilmesi uygulama veya sistemin sahibi birimin sorumluluğundadır.
9. Sıkılaştırma çalışmaları sonucunda bulunan zafiyetleri kapsayan ikinci bir test, birinci test sonuçlarını kontrole yönelik olarak tekrar edilecektir.

5.2 Bilgi Güvenliği Denetimlerini Uygulama ve Raporlama

1. Teknik açıklık denetimleri sırasında kullanılan tüm bilgi ve belgeler "Gizli" gizlilik derecesine sahiptir ve buna göre işlem yapılacaktır.
2. Yapılacak güvenlik denetimleri yalnızca Bilgi İşlem ya da yetkilendirilmiş 3. taraflarca yapılabilir.

3. Yapılacak testler varlık envanterine göre yapılır ve varlık envanterinin güncelliği varlık sahipleri ile birlikte kontrol edilir.
4. Denetim sırasında denetlenecek sistemlerin denetlemeye hazır olmasının sağlanması varlık sahiplerinin sorumluluğundadır.
5. 3. tarafların yapacakları güvenlik denetimleri öncesinde Bilgi İşlem'den onay alınması zorunludur.
6. Güvenlik denetimleri için uygulanacak metodoloji aşağıdaki metodolojiler incelenerek Kuruma özel hale getirilmiştir.

   Metodolojinin oluşturulmasında OWASP (Open Web Application Security Project), OSSTMM (The Open Source Security Testing Methodology Manual) metodolojileri incelenmiştir. Testler esnasında prosedür dışında bu metodolojilerden faydalanılabilecektir.

   a. SİSTEM HAKKINDA BİLGİ TOPLAMA;

      Saldırı için kullanılabilecek veriyi elde etmek için toplanabilecek bilgilerin tespit edilmesi. Bu işlem için aktif ve pasif olmak üzere iki yöntem kullanılır. Bilgi toplama için Shodan arama motoru, the harvester, dns kullanılabilecek araçlardır.

   b. AĞ TOPOLOJİSİNİN OLUŞTURULMASI;

      Teknik testler ile tespit edilebilecek Sistem ağ yapısı belirlenir. Bu kapsamda kullanılan cihazlar sunucular ve bunlara ait açık olan portlarının tespit edilmesi, Networkte bulunan ağların çıkartılması. Ağlar için alınan önlemlerin belirlenmesi ve varlık envanteri dışında bulunan cihazların tespiti yapılır. Bu işlemlerin yapılması için kurumsal zafiyet analiz yazılımı kullanılır. Çıkan sonuçları kontrol etmek için gerek görüldüğünde NMAP, Netscan gibi açık kaynak kodlu araçlar kullanılır.

   c. ZAFİYET ANALİZİ;

      Bu aşamada tespit edilen varlıkların içerdikleri zafiyetler belirlenir. Sızma süreci için gerekli bilgileri toplanır. Bu işlemlerin yapılması için kurumsal zafiyet analiz yazılımı kullanılır.

      Test kapsamında; güvenlik duvarı, yük dengeleyiciler, mantıksal erişim alanları, ağ yönlendiricileri, sunucular (veritabanı sunucuları, e-posta sunucuları, internet

sunucuları vb.), sunucu yönetimsel erişimleri, sunucu üzerindeki uygulamalar ve servisler, erişim sağlanabilen kullanıcı bilgisayarları, işletim sistemleri (sunucu & kullanıcı bilgisayarları) anahtarlama cihazları ve ağ yazıcıları gibi birimler üzerinde zafiyet ve sızma testi gerçekleştirilir.

d. SIZMA;

Bu sürece kadar elde edilen bilgiler ve zafiyetler kullanılarak sitem kaynaklarınla erişme, yetki ele geçirme, bilgi erişimi gibi işlemler yapılır. Bu çalışmalar yapılırken sisteme zarar verebilecek işlemler için önceden onay alınır ya da eş bir test sistemi üzerinde işlem yapılır. Gerçekleştirilen eylemler için objektif kanıtlar toplanır. Bu aşamada Metasploit, Core Impact, SqlMap gibi araçların yanında test uzmanın oluşturduğu scriptler de kullanılabilir.

7. Zafiyet analizleri sonucunda Yönetimsel ve Teknik rapor olmak üzere 2 adet rapor oluşturulacaktır. Yönetimsel rapor zafiyetlerin özeti şeklinde oluşturulurken teknik rapor detaylı şekilde zafiyet temelli raporlama olacaktır.
8. Teknik raporda bulunan zafiyetler ile birlikte bu zafiyetlerin giderilmesi için uygulanacak yöntemlerde bulunacaktır.

Revizyon Kayıtları

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