1. Amaç - Kapsam

Kurumumuzun veya hizmet verdiğimiz kurumlarımızdaki bilgi kaynaklarının bütünlüğünü ve gizliliğini sağlamak, kurumumuzun veya kurumların güvenlik politikalarına uyumunu kontrol etmek, sistemlerin güvenlik açıklarını tespit etmek, kullanıcıların veya sistemin aktivitelerini kontrol etmek amacıyla kurumumuzun veya kurumların bilgi ve iletişim altyapılarının (Uygulama Yazılımı, Veri tabanı, PC, sunucu, firewall, ağ anahtarı vs) güvenlik açıklarına karşı taranması hususunda kuralları tanımlamaktır.

2. Sorumlular

Bu prosedürün oluşturulmasından ve uygulanmasından Ağ (network) Hizmetleri Birimi Ve Sistem Hizmetleri Birimi sorumludur.

3. Uygulama

Genel Kurallar

Bu prosedür kurumun bünyesinde bulunan fakat kurumun sahip olmadığı herhangi bir sistemi de kapsamaktadır.

Sistem güvenliği denetimleri yapılacaktır. Sistemlerin güvenliğini artırmak, olası bilişim güvenliği problemlerini tespit edip çözülmesine ilişkin Internet Güvenlik Denetimi ve Intranet Güvenlik Denetimi olmak üzere iki aşamalı bir çalışma yaptırılacaktır.

Uygulamaların güvenliği ve Veri güvenliği denetimleri yapılacaktır. Uygulamanın kod güvenliği ve yetkilendirme güvenliğinin tespit edilmesi yanında gizlilik, bütünlük, erişilebilirlik ve kurtarılabilirlik özelliklerinin de gerçekleştirilebildiği test edilmelidir

Kurumumuz tarafından istenildiği takdirde denetim yapan firma personeline sistemlere erişim izni verilecektir. Kurumumuz denetim yapan firmaya ağın taranması için uygulama yazılımları, protokol, adres bilgileri, ağ bağlantıları vs. hakkında bilgi verecektir.

Denetim yapacak firmaya verilecek bilgiler ve istekler aşağıdaki hususları kapsamalıdır.

- Bilgisayar veya ağ cihazlarına yapılan kullanıcı ve/veya sistem seviyeli erişim bilgileri.
- Kurumun bünyesindeki üretilen, iletilen veya saklanan bilgilere, uygulamalara (elektronik, hardcopy vs) erişim hakkı.
- Çalışma alanlarına erişim (ofisler, sistem odaları, bilgi depolama alanları vs).
- İletişim ağının trafiğini etkileşimli olarak gözlemleme ve trafiğin logolanması isteği.

Veri ve Yazılım Kod Güvenliği Denetimi

Veri güvenliğini denetlerken verilerin bulunduğu noktalara erişim durumları gözden geçirilmelidir. Verilerin daimi depolanma alanı, geçici olarak bulundukları swap, hafıza, internet hattı, pc geçici alanı gibi alanların denetlenmesi gerekmektedir.

Yazılım kodlarının güvenlik açıklarına yol açabilecek “zayıflıklar”ın belirlenmesinde en az aşağıdaki metotlar takip edilmelidir.

- Tampon taşması
- Mimari yanlışları
- Yanlış transaction kullanımı
- Biçim kelimesi problemleri
- Sayı taşmaları (Integer Overflow)
- SQL sokuşturma
- Komut sokuşturma
- Hataların ele alınmaması
- İstisnaların ele alınmaması
- Çapraz site betikleri
- Ağ trafiğine sonsuz güven
- URL bazlı veri girdisi
- Uygunsuz SSL kullanımı
- Zayıf şifre yapıları
- Güvensiz veri saklama
- Veri sızıntısı
- Uygunsuz dosya erişimi (veri kaybı)
- Yarış durumları
- Yetkilendirilmemiş anahtar değişimleri
- Kriptografi için yetersiz rastgelelik
- Kullanışsızlık

Veri Güvenliği ve Yazılım Kod Güvenliği Denetim Raporu:

Denetim firmasının sunacağı Final raporu ile beraber yapılan işler, uygulanan yöntemler, bunların çıktıları, çıktı analizleri ve öneriler yer almalıdır. Bunlar;

- Problem İsmi
- Risk Seviyesi
- Problemin Düzeltilme Durumu
- Problem Sınıfı (Integrity, availability, accountability, secrecy, recovery)
- Problemin Etkisi
- Problemli Noktalar
- Problemi kullanabilecekler (Son kullanıcı, yazılımcı, bilgisayar saldırganı, suç organizasyonları, istihbarat kuruluşları)
- Problemin Kısa Tanımı
- Kısa Vadeli Çözüm Yöntemi ve Aksiyonlar (devre dışı bırakma, bölümü durdurma, hızlı ve kirli çözüm, bütün çözüm)

İnternet Üzerinden Sistem Güvenlik Denetimi

Internet tarafından kurumumuza bakıldığı zaman ulaşılabilen bilgileri saptamaya yönelik güvenlik sorgulama servisidir.

Bu çalışma kapsamında, kurumumuz tarafından Internet'e açılmış olan uygulamaların ve sunulan servislerin özel yetkiye sahip olmayan bir kullanıcı gözüyle güvenlik açıkları ve olası tehditler belirlenmiş olacaktır.

Faaliyetler

İnternet üzerinden yapılacak güvenlik denetiminde aşağıdaki faaliyetler yer alacaktır.

- Kurumun İzinin Araştırılması
- Ağ Haritasının Çıkarılması
- Servis ve Sistemlerin Tespiti
- Zafiyet Taraması ve Doğrulaması
- Yönlendirici Testleri
- Firewall Testleri
- Saldırı Tespit Sistemi Testleri
- Sızma Testleri
- WEB Uygulamaları Güvenliği Testleri
- Web uygulamalarının ve sunucuların yaygın açıklarına karşı testler

İntranet Üzerinden Sistem Güvenlik Denetimi

Kurumumuz Intranet'inde yer alan çeşitli yetki seviyelerindeki kullanıcılar tarafından ulaşılabilen bilgileri saptamaya yönelik güvenlik sorgulama servisidir.

Bu çalışma kapsamında, Kurum içerisinde kullanılan uygulamaların ve sunulan servislerin çeşitli yetki seviyelerindeki kullanıcılar gözüyle güvenlik açıkları ve olası tehditler belirlenmiş olacaktır.

Faaliyetler

İntranet üzerinden yapılacak güvenlik denetiminde aşağıdaki faaliyetler yer alacaktır.

- DNS / DHCP / WINS araştırması ve kontrolleri.
- Uygulama/Database/File sunucularının araştırması ve kontrolleri
- Intranet üzerindeki aktif ve pasif ağ cihazlarının incelenmesi ve kontrolleri
- Kurum intranetinde alınmış güvenlik önlemleri ve bölgelendirmelerin kontrolleri
- Intranet sunucu kontrolleri
- Intranet'te kritik istemcilerin taranması
- Kullanıcı profilinin çıkarılması
- Şifre politikalarının incelenmesi ve mevcut şifre sisteminin denetlenmesi
- Güvenilir Sistem Testleri (Trusted Systems)
- Kötü içerikli kod (malware) testleri
- Log taramaları
- Uygulamaya özel güvenlik problemleri kontrolü

İnternet veya İntranet üzerinden Sistem Güvenlik Denetimi Çıktıları

Denetim sonuç raporunda aşağıdaki çıktılar yer alacaktır.

- Ağ profili
- Sunucu ve sistem tanımları

- Bilgi profili
- Zaafiyet tanımları
- Sızma testi sonuçları (Güvenlik açıklarının taşıdıkları riskler itibariyle önceliklerinin belirlenmesi)
- Çözüm önerileri (Zaafiyetlerin giderilmesine yönelik genel öneriler)

Tarama Esnasında Muhatap Olan Kişi

Kurumumuz denetimi yapacak firmaya oluşabilecek sorunlar hakkında danışabileceği bir kişiyi yazılı olarak tanımlayacaktır.

Tarama Periyodu

Kurum ve denetimi yapan firma denetim yapılacak zamanı email veya telefon olarak bildireceklerdir.

Gizlilik Anlaşması:

Kurum ile güvenlik taraması yapacak firma, tarama sonucunda elde edilecek bilgilerin hiçbir şekilde üçüncü şahıslara aktarmayacağına dair gizlilik anlaşması yapacaktır.

4. BGYS Kayıtları

-

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
BİLGİ İŞLEM DAİRE BAŞKANLIĞI	KURUMSAL KALİTE GELİŞTİRME VE AKREDİTASYON KOORDİNATÖRLÜĞÜ	KURUMSAL YETKİLİ