1. AMAÇ

Bu politikanın amacı kurumun bilgisayar ağının (firewall, sunucu vs.) güvenlik açıklarına karşı taranması hususunda politika belirlemektir.

Denetim Sebepleri:

- Bilgi kaynaklarının bütünlüğü ve gizliliğini sağlamak,
- Bilgi kaynaklarının bulunduğu ortamlardaki güvenlik açıklarının tespit edilmesi ve bunlarla ilişkili riskleri azaltmak için sistem güncellemelerinin gözden geçirilmesi, değerlendirilmesi, uygulanması ve doğrulanması için kurallar oluşturmak,
- Gerektiği zaman kullanıcıların veya sistemin aktivitelerini kontrol etmek.

2. KAPSAM

Kurum bünyesinde sahip olunan bütün bilgisayar (Sunucu, Güvenlik Kontrol Cihazları vb.) ve haberleşme cihazlarını kapsamaktadır. Bu politika kurumun bünyesinde bulunan fakat kurumun sahip olmadığı herhangi bir sistemi de kapsamaktadır. Denetim yapan kişi veya kurum, hizmetlerin durdurulması aktivitesi yapmayacaktır. Denetim esnasında yapılacak testlerde (DDoS Saldırı Testi vb.) yaşanabilecek hizmet kesintileri bu kapsam dışında olup, yapılan test sonuçlandırıldığında zaman kaybetmeksizin durdurularak, gerekli kontroller ve düzenlemeler yapıldıktan sonra tekrar kontrol edilecektir.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından Bilgi İşlem Daire Başkanlığı sorumludur.

4. UYGULAMA

İstenildiğinde denetim yapan kurumların bireylerine erişim izni verilecektir. Kurumun birimleri denetim yapan kuruma ağ taraması yapması için protokol, adres bilgileri, ağ bağlantıları hakkında bilgi verecektir.

a. Güvenlik Açığı Taraması

Dahili ve harici ağın güvenlik açığı taramaları, ağda önemli bir değişiklik meydana geldiğinde veya yılda en az bir defa yapılacaktır. Kritik veya yüksek olarak derecelendirilen başarısız güvenlik açığı taraması sonuçları düzeltilecek ve tüm kritik veya yüksek riskler çözülene kadar yeniden taranacaktır. Güvenlik açığı taraması sırasında bulunan, güvenliği ihlal

edilmiş veya istismar edilmiş bir bilgi kaynağına ilişkin tüm kanıtlar Yönetim Temsilcisine bildirilmelidir. Yeni güvenlik açığı sorunlarının belirlenmesi durumunda, yapılandırma standartları buna göre güncellenecektir.

b. Penetrasyon(Sızma) testi

Dahili ağın, harici ağın ve barındırılan uygulamaların sızma testi, yılda en az bir kez veya ortamdaki önemli değişikliklerden sonra yapılacaktır. Sızma testi sırasında bulunan tüm açıklardan, yararlanılabilir güvenlik açıkları düzeltilecek ve güvenlik açığının düzeltildiğini doğrulamak için yeniden test edilecektir.

c. Tarama Esnasında Muhatap Olan Kişi: Kurum denetimi yapan firma/kuruma oluşabilecek sorunlar hakkında danışabileceği bir kişiyi yazılı olarak bilgi verecektir.

d. Tarama Periyodu: Kurum ve denetimi yapan firma/kurum denetim yapılacak zamanı yazılı olarak bildirecektir.

e. Gizlilik Anlaşması: Kurum ile güvenlik taraması yapacak firma/kurum, tarama sonucunda elde edilecek bilgilerin hiçbir şekilde üçüncü şahıslara aktarılmayacağına dair gizlilik anlaşması yapacaklardır.