1. AMAÇ

Bu politikanın amacı; Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında kullanılan bilgi teknolojileri varlıkları, ağ altyapısı, sunucular, güvenlik cihazları, uygulamalar ve haberleşme sistemlerinde bulunabilecek güvenlik açıklarının sistematik olarak tespit edilmesi, değerlendirilmesi, raporlanması ve giderilmesinin takip edilmesine ilişkin esasları belirlemektir.

Bu politika ile;

- Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin korunması,
- Bilgi sistemleri ve ağ altyapısındaki güvenlik açıklarının zamanında tespit edilmesi,
- Güvenlik açığı tarama ve sızma testi faaliyetlerinin kontrollü şekilde yürütülmesi,
- Tespit edilen güvenlik açıklarının ilgili risk ve yama yönetimi süreçlerine aktarılması,
- Gerçekleştirilen düzeltmelerin gerektiğinde yeniden test edilerek doğrulanması amaçlanmaktadır.

2. KAPSAM

Bu politika; Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi kapsamında kullanılan veya yönetilen;

- Sunucu sistemlerini,
- Masaüstü ve dizüstü bilgisayarları,
- Ağ ve haberleşme cihazlarını,
- Güvenlik duvarı ve diğer güvenlik kontrol cihazlarını,
- Sanal sistemleri,
- Web uygulamaları ve diğer kurumsal uygulamaları,
- Ağ altyapısını,
- Kurum bünyesinde barındırılan üçüncü taraflara ait sistemleri kapsar.

Kurum tarafından işletilen ancak mülkiyeti üçüncü taraflara ait olan sistemlerde yapılacak güvenlik açığı tarama ve sızma testi faaliyetleri, ilgili sözleşme, protokol ve yetkilendirmeler doğrultusunda gerçekleştirilir.

3. SORUMLULUKLAR

3.1. Bilgi İşlem Daire Başkanlığı

- Güvenlik açığı tarama ve sızma testi faaliyetlerinin planlanmasını ve koordinasyonunu sağlamak,
- Taranacak sistem, IP adresi, uygulama ve ağ bileşenlerini belirlemek,
- Testlerin yetkilendirilmiş kişi veya kuruluşlar tarafından gerçekleştirilmesini sağlamak,
- Test sonuçlarını değerlendirmek ve ilgili birimlere iletmek,
- Tespit edilen güvenlik açıklarının Zaafiyet ve Yama Yönetimi Politikası kapsamında değerlendirilmesini sağlamak,
- Gerekli durumlarda düzeltme sonrasında yeniden test yapılmasını sağlamak,

- Test ve tarama sonuçlarının gizliliğini ve güvenliğini korumak.

3.2. Sistem ve Uygulama Sorumluları

- Kendi sorumluluk alanlarındaki sistemlerle ilgili gerekli teknik bilgileri sağlamak,
- Güvenlik açığı tespit edilmesi halinde ilgili düzeltme çalışmalarına destek olmak,
- Yapılan düzeltmelerin doğrulanması için gerekli teknik desteği sağlamak.

3.3. Güvenlik Açığı Taraması veya Sızma Testi Yapan Kişi/Kuruluşlar

- Yalnızca yetkilendirilen sistem ve kapsam üzerinde çalışma yapmak,
- Test faaliyetlerini onaylanan plan ve yöntemlere uygun yürütmek,
- Test sırasında elde edilen bilgi ve bulguların gizliliğini korumak,
- Yetkisiz sistemlere erişim sağlamamak,
- Test sonucunda elde edilen bilgi ve kanıtları Üniversitenin belirlediği kişilere raporlamak,
- Hizmet sürekliliğini gereksiz yere riske atacak işlemlerden kaçınmak.

4. UYGULAMA

4.1. Güvenlik Açığı Taraması

- İç ve dış ağların güvenlik açığı taramaları, risk durumu ve sistemlerin kritiklik seviyesi dikkate alınarak yılda en az bir kez ve ayrıca önemli sistem, ağ, yazılım veya yapılandırma değişikliklerinden sonra gerçekleştirilir.
- Güvenlik açığı taramalarında kullanılan araçlar ve yöntemler, taranacak sistemin özellikleri ve olası hizmet etkileri dikkate alınarak belirlenir.
- Tarama sonucunda tespit edilen güvenlik açıkları önem derecesine göre sınıflandırılır ve ilgili kayıtlar oluşturulur.
- Kritik veya yüksek seviyedeki güvenlik açıkları öncelikli olarak değerlendirilir.
- Tespit edilen güvenlik açıklarının giderilmesi Zaafiyet ve Yama Yönetimi Politikası kapsamında yürütülür.
- Giderilen kritik ve yüksek seviyeli güvenlik açıklarının gerektiğinde yeniden tarama veya doğrulama yoluyla kapatıldığı kontrol edilir.
- Güvenliği ihlal edilmiş veya istismar edilmiş olabileceği değerlendirilen bir bilgi varlığı tespit edilmesi halinde durum Bilgi Güvenliği Olay Yönetimi Prosedürü kapsamında değerlendirilir.

4.2. Penetrasyon(Sızma) testi

- Kurumun iç ve dış ağları ile kurumsal uygulamalarına yönelik sızma testleri yılda en az bir kez ve ayrıca önemli sistem veya mimari değişikliklerden sonra gerçekleştirilir.
- Sızma testinin kapsamı, test yöntemi, test edilecek sistemler, test zamanı ve yetkili test ekibi çalışma başlamadan önce belirlenir ve onaylanır.
- Sızma testleri yalnızca Üniversite tarafından yetkilendirilen kişi veya kuruluşlar tarafından gerçekleştirilir.

- Test sırasında gerçek hizmetleri etkileyebilecek veya veri kaybına neden olabilecek işlemler kontrollü şekilde gerçekleştirilir.
- Hizmet kesintisine neden olabilecek yük testi, stres testi veya DDoS benzeri testler ancak önceden yazılı olarak planlanması, yetkilendirilmesi ve gerekli önlemlerin alınması halinde gerçekleştirilir.
- Test sırasında kritik bir hizmetin güvenliğini veya erişilebilirliğini ciddi şekilde etkileyebilecek bir durum oluşması halinde test durdurulur ve ilgili teknik sorumluya bilgi verilir.
- Sızma testi sonucunda elde edilen bulgular raporlanır ve tespit edilen güvenlik açıkları ilgili risk ve zaafiyet yönetimi süreçlerine aktarılır.
- Giderilen kritik bulgular için gerektiğinde yeniden sızma testi veya doğrulama testi gerçekleştirilir.

4.3. Test Öncesi Planlama ve Yetkilendirme

Güvenlik açığı taraması veya sızma testi başlamadan önce aşağıdaki hususlar belirlenir:

- Testin amacı ve kapsamı,
- Test edilecek IP adresleri, sistemler, uygulamalar ve ağ bileşenleri,
- Test yöntemi,
- Test başlangıç ve bitiş zamanı,
- Testi gerçekleştirecek kişi veya kuruluş,
- Kurum içindeki teknik muhatap,
- Acil durumda iletişim kurulacak kişiler,
- Hizmet kesintisi veya teknik sorun oluşması halinde uygulanacak yöntem,
- Test sonuçlarının teslim şekli.

Test kapsamı dışında kalan sistemlere yönelik işlem yapılmaz.

4.4. Test Sırasında Teknik Muhatap

Üniversite tarafından, güvenlik açığı taraması veya sızma testi sırasında oluşabilecek teknik sorunlar ve acil durumlar için test ekibinin iletişim kurabileceği yetkili bir teknik personel belirlenir.

4.5. Tarama ve Test Periyodu

Güvenlik açığı taraması ve sızma testlerinin tarihleri, kapsamı ve çalışma saatleri ilgili birim ile test hizmetini gerçekleştiren kişi veya kuruluş arasında önceden planlanır.
Kritik sistemlerde gerçekleştirilecek testlerin hizmet sürekliliği üzerindeki olası etkileri değerlendirilir.

4.6. Bulguların Raporlanması

Güvenlik açığı taraması ve sızma testi sonucunda;

- Tespit edilen güvenlik açığının tanımı,
- Etkilenen sistem veya varlık,
- Güvenlik açığının önem derecesi,
- Olası etkisi,
- Varsa teknik kanıt,
- Önerilen düzeltme veya önlem,

- Yeniden doğrulama durumu raporlanır.

Test sonuçları yalnızca yetkilendirilmiş kişi ve birimlerle paylaşılır.

4.7. Gizlilik

Güvenlik açığı taraması ve sızma testi sırasında elde edilen sistem bilgileri, yapılandırmalar, kullanıcı bilgileri, güvenlik açıkları, test sonuçları ve diğer kurumsal bilgiler gizli kabul edilir.

Üçüncü taraf kişi veya kuruluşlarla gerçekleştirilen çalışmalarda, ihtiyaç duyulması halinde hizmet başlamadan önce gizlilik hükümleri veya gizlilik sözleşmesi oluşturulur.

Test sonuçlarının yetkisiz kişilerle paylaşılmasına izin verilmez.

4.8. Kayıtların Korunması

Güvenlik açığı tarama ve sızma testi faaliyetlerine ilişkin raporlar, bulgular, yeniden test sonuçları, yetkilendirmeler ve ilgili kayıtlar EYS doküman ve kayıt yönetimi kurallarına uygun olarak korunur.

5. YAPTIRIM

Bu politika kapsamında belirlenen kurallara aykırı uygulamalar EYS kapsamında uygunsuzluk olarak değerlendirilir ve gerekli durumlarda Düzeltici Faaliyet Prosedürü uygulanır. Çalışanların politika hükümlerine aykırı hareket etmesi halinde ilgili mevzuat, Üniversite düzenlemeleri ve Disiplin Prosedürü hükümleri uygulanır. Yetkisiz güvenlik testi veya tarama gerçekleştirilmesi halinde olay, gerekli durumlarda Olay İhlal Prosedürü kapsamında değerlendirilir.