1. AMAÇ

Bu Politika, Kurum'daki bilgi sistemlerinde yaşanabilecek teknik açıklıkların yönetimini ve tetkik kontrolleri ile ilgili hususları belirtmek amacıyla yazılmıştır.

2. KAPSAM

Bu Politika Kurum Bilgi Güvenliği Yönetim Sistemi kapsamına giren sistemlerde yaşanabilecek teknik açıklıklarla ilgili yürütülen faaliyetleri kapsamaktadır.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığı Bilişim Hizmetleri Şube Müdürlüğü sorumludur.

4. UYGULAMA

4.1. Teknik Açıklık Taramalarının Planlanması

- Teknik açıklıkları belirlemek için kullanılacak bilgi kaynakları; varlık envanter listesinde bulunan tüm yazılım ve donanımlar kullanılarak tanımlanmalıdır.
- Teknik açıklık taramalarının sıklığı, sistemin ilişkili olduğu verinin kritikliğine göre, varlığın sahibi ve Bilgi İşlem Daire Başkanlığı tarafından belirlenir.
- Kurum genelindeki izleme, yama, varlık izleme ve teknik açıklık yönetimi Some Sorumlusu koordinasyonunda gerçekleştirilir.
- Genel sistem taramaları için BGYS iç denetiminden önce açıklık tarama planlaması yapılır ve uygulamaya alınır.
- Tarama kapsamında incelenecek sistemler, Bilgi İşlem Daire Başkanlığı tarafından IP adres aralığı, web uygulamaları, kritik sunucular ve diğer parametreler göz önünde bulundurularak belirlenir. Kritik olarak belirlenen sistemler öncelikli olarak tanımlanmalıdır.
- Taramalar, karşılaşılabilecek hizmet kesinti riskini en aza indirecek şekilde planlanır.
- Çalışan sistemlerde kesintiye sebep olacak, sistem yapılandırmalarında veya tutulan verilerde değişikliğe sebep olabilecek taramalardan zorunlu olmadıkça kaçınılır, zorunlu durumlarda bu taramalar ilgili sistem sahibi tarafından onaylanır.
- Tarama yapılacak sistemlerin taramaya hazır olmasının sağlanması ve zamanının belirlenmesi ilgili varlık sahibinin sorumluluğundadır.

4.2. Dış Taraflarca Yapılan Açıklık Taraması

Kurum içi yapılan çalışmalara ek olarak, bağımsız ve yetkin kurum/kuruluş tarafından teknik açıklıkların tespiti amacıyla hizmet alımı yapılabilir. Alınan hizmet kapsamında sistem açıklık raporu hazırlanır ve gerekli aksiyonların alınması için ilgili ekiplere bilgilendirme yapılır. Bu durumda Bilgi İşlem Daire Başkanlığı tarafından;

- Test kapsamı ve testi yapılacak sistemlerin gerekli bilgileri belirlenir.
- Sızma testi ve/veya açıklık taramasını yapacak firma çalışanlarının yetkinlik belgeleri istenir.
- Sızma testi ve/veya açıklık taraması için iş planları ve kullanacakları araçların listesi istenir. Kullanılacak açıklık tarama araçlarının sektörde kabul görmüş lisanslı araçlar olup olmadığı kontrol edilir.
- Yapılacak çalışmanın takvimi hakkında Kurum Yönetimi bilgilendirilir.
- Çalışmayı yapacak firma çalışanlarına test ve taramalar için kullanıcı hesabı oluşturulur. Tarama bitiminde kullanıcı hesapları pasif hale getirilir.
- Teknik açıklık taramalarının karşılıklı gizliliğini sağlamak amacıyla gerekli eklemelerle Gizlilik Sözleşmesi imzalanır. Çalışmayı yapacak firma çalışanlarının kullanımı için uygun bir fiziksel bir ortam ayrılır. Bu ortamın Kurum personelinin çalışma ofislerine uzak bir noktada olması tercih edilir.

4.3. Raporlama

- Denetim sonucunda tespit edilen teknik zafiyetleri ve çözüm önerilerini içeren raporlar Bilgi İşlem Daire Başkanlığı'na teslim edilir, BGYS Proje Sorumlusu bilgilendirilir.
- Bilgi İşlem Daire Başkanlığı raporların güvenli ortamda saklanmasından sorumludur. Raporlar güvenli bir ortamda saklanır ve erişimler kısıtlanır.
- Denetim sırasında tespit edilen açıklıklar, etki dereceleri ve gerçekleşme ihtimallerine göre sınıflandırılır.
- BİDB personeli, tespit edilen teknik açıklıkların belirlenmesinden sonra kuruluş ilişkili risklerin ve alınması gereken eylemlerin (Aksiyon) Risk Yönetimi Prosedürü'ne göre tanımlanmasını sağlar.

4.4. Teknik Açıklıkların Kapatılması

- Tespit edilen açıklıkların ortadan kaldırılması için gerekli düzeltici / iyileştirici aksiyonlar, Düzeltici ve İyileştirici Faaliyet Prosedürü referans alınarak, ilgili sistem sorumluları tarafından gerçekleştirilir. Yama yüklenmesi gereksinimi var ise Madde 4.5 Yama Yönetimi süreci işletilir. İş ihtiyacı veya sistem kesintisi ihtimali sebebiyle kapatılamayacak açıklıklar için Bilgi İşlem Daire Başkanlığı'nın onayı alınır.

4.5. Yama Yönetimi

- İşletim sistemi güvenlik yamaları aylık rutin güvenlik güncellemeleri kapsamında kontrollü olarak yüklenir. Bu işin takibinden ilgili Bilgi İşlem Daire Başkanlığı sorumludur.
- Bilgi İşlem Daire Başkanlığı kapsamında olmayan işletim sistemlerinin ve Bilgi İşlem Daire Başkanlığı'nın işletmediği yama yönetiminden ilgili birimler sorumludur.
- Kurumsal anti-virüs ve saldırı tespit sistemi yazılım güncellemeleri iş bilgisayarlarına ve sunucu sistemlerine Bilgi İşlem Daire Başkanlığı tarafından yüklenir.

4.6. Sonuçların Değerlendirilmesi

- Gerekli durumlarda, BGYS Sorumlusu, tarama sonuçlarını Bilgi Güvenliği Yönetim Sistemi Ekibi ile değerlendirir.
- BGYS Sorumlusu ve BİDB personeli teknik açıklık tetkik raporunu ve değerlendirme toplantıları sonuçları doğrultusunda tespit edilen güvenlik açıklıklarının giderilmesi için düzeltici faaliyetleri belirler ve iş birliği içinde kendi yetki alanlarına giren işler için ilgili personeli görevlendirir ve sonuçlarını takip eder.

4.7. Takip Denetimi

- Tespit edilen açıklıkların kapatılma durumu tekil kontroller ile takip edilir.
- Takip denetimi ihtiyaç olması durumunda gerçekleştirilir. Takip denetimi Bilgi İşlem Daire Başkanlığı tarafından yapılır.
- Takip denetimi sonrasında tespit edilen uygunsuzluklar için "Düzeltici ve İyileştirici Faaliyet" kaydı açılır.

4.8. Teknik Uyum Gözden Geçirmesi

- Kurumda kullanılan bilgi güvenliği standartları ile bilgi sistemleri faaliyetlerinin uyumluluğu düzenli bir şekilde gözden geçirilmelidir. Teknik uyum gözden geçirmeleri sızma testleri, açıklık değerlendirmeleri gibi faaliyetleri kapsamalıdır.
- Gözden geçirmeler teknik uzman tarafından araç yardımı ile veya manuel olarak yapılmalı ve sonuçları raporlanmalıdır.
- Gerekli görülen durumlarda teknik uyum gözden geçirmeleri Kurum dışı bağımsız bir firma veya uzmana yaptırılabilir, bu durumda Madde 4.2'de belirtilen kurallar dikkate alınmalıdır.