1. AMAÇ

Bu politikanın amacı, Süleyman Demirel Üniversitesi bilgi sistemleri ve bilgi varlıklarında ortaya çıkabilecek teknik zafiyetlerin zamanında tespit edilmesi, değerlendirilmesi, önceliklendirilmesi, giderilmesi ve takip edilmesine ilişkin esasları belirlemektir.

Bu politika kapsamında ayrıca güvenlik yamalarının kontrollü şekilde uygulanması, teknik zafiyetlerin oluşturabileceği risklerin azaltılması, teknik uyum kontrollerinin gerçekleştirilmesi ve zafiyet yönetimi faaliyetlerinin kayıt altına alınması amaçlanmaktadır.

2. KAPSAM

Bu politika,

- Sunucuları,
- Ağ cihazlarını,
- Güvenlik cihazlarını,
- İşletim sistemlerini,
- Veritabanlarını,
- Web uygulamalarını,
- Kurumsal uygulamaları,
- Son kullanıcı cihazlarını,
- Sanal sistemleri,
- Bulut hizmetlerini,
- Diğer bilgi işleme ve iletişim sistemlerini kapsar.

Politika ayrıca bu sistemlere ilişkin teknik zafiyet taramaları, sızma testleri, güvenlik güncellemeleri, yama yönetimi ve teknik uyum gözden geçirmelerini kapsar.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından;

- Bilgi İşlem Daire Başkanlığı,
- İlgili sistem ve varlık sahipleri,
- Sistem yöneticileri,
- Ağ ve güvenlik yöneticileri,
- Yazılım ve uygulama sorumluları,
- BGYS Sorumlusu,
- Bilgi Güvenliği Yönetim Sistemi Ekibi görev ve yetkileri kapsamında sorumludur.

BGYS Sorumlusu, zafiyet yönetimi faaliyetlerinin BGYS süreçleri ile koordinasyonunu ve gerekli durumlarda risk yönetimi süreçleriyle ilişkilendirilmesini sağlar.

4. UYGULAMA

4.1. Teknik Zafiyet Kaynaklarının Belirlenmesi

Teknik zafiyetlerin tespit edilmesinde aşağıdaki bilgi kaynaklarından yararlanılır:

- Zafiyet tarama sonuçları,
- Sızma testi sonuçları,
- Üretici güvenlik duyuruları,
- Güvenlik danışma bildirimleri,
- Ulusal ve uluslararası güvenlik bildirimleri,
- Kullanılan yazılım ve donanım üreticilerinin güvenlik bildirimleri,
- Güvenlik izleme sistemleri,
- Antivirüs sistemleri,
- SIEM ve benzeri güvenlik izleme çözümleri,
- İç ve dış denetim sonuçları,
- Bilgi güvenliği olayları,
- Sistem yöneticileri ve kullanıcılar tarafından bildirilen güvenlik açıkları.

Bilgi İşlem Daire Başkanlığı, Kurum tarafından kullanılan bilgi varlıkları ile ilgili güncel teknik zafiyet bilgilerinin takip edilmesini sağlar.

4.2. Zafiyet Taramalarının Planlanması

1. Teknik zafiyet taramaları, Varlık Envanteri dikkate alınarak planlanır.
2. Taramaların sıklığı ve kapsamı;
    - Varlığın kritiklik seviyesi,
    - İşlenen bilginin hassasiyeti,
    - Sistem üzerinde bulunan kişisel veriler,
    - Sistemin internete açık olup olmadığı,
    - Önceki taramalarda tespit edilen zafiyetler,
    - Güvenlik olayları,
    - Sistem değişiklikleri,
    - Yeni yayımlanan kritik zafiyetler dikkate alınarak belirlenir.
3. Kritik bilgi sistemleri ve internet üzerinden erişilebilen sistemler öncelikli olarak değerlendirilir.
4. Genel zafiyet taramaları, kurumun risk yaklaşımı doğrultusunda planlanır ve gerektiğinde BGYS iç denetimleri öncesinde gerçekleştirilir.
5. Tarama kapsamında incelenecek sistemler; IP adres aralıkları, web uygulamaları, kritik sunucular, ağ cihazları ve diğer bilgi varlıkları dikkate alınarak belirlenir.
6. Zafiyet taramaları, hizmet kesintisi veya veri bütünlüğünün bozulması riskini en aza indirecek şekilde planlanır.
7. Sistem üzerinde değişiklik oluşturabilecek veya hizmet kesintisine neden olabilecek aktif taramalar, ilgili sistem sahibi ile koordinasyon sağlanarak gerçekleştirilir.

8. Tarama yapılacak sistemlerin taramaya hazırlanması ve gerekli erişimlerin sağlanması ilgili sistem/varlık sahibinin sorumluluğundadır.

4.3. Zafiyetlerin Değerlendirilmesi ve Önceliklendirilmesi

Tespit edilen teknik zafiyetler;

- Zafiyetin önem derecesi,
- İstismar edilebilirliği,
- Etkilenen varlığın kritiklik seviyesi,
- İnternete açık olup olmadığı,
- Etkilenen bilginin hassasiyeti,
- Kişisel veri içerip içermediği,
- İş sürekliliğine etkisi,
- Mevcut güvenlik kontrolleri,
- Kurum üzerindeki potansiyel etkisi dikkate alınarak değerlendirilir.

Zafiyetler, kurumun Risk Yönetimi Prosedürü kapsamında risk değerlendirmesine tabi tutulabilir.

4.4. Zafiyetlerin Giderilmesi

1. Tespit edilen zafiyetlerin giderilmesi için gerekli düzeltici veya iyileştirici faaliyetler ilgili sistem sorumluları tarafından gerçekleştirilir.
2. Zafiyetin giderilmesinde öncelikle;
    - Güvenlik yamasının uygulanması,
    - Yazılım veya sistem sürümünün güncellenmesi,
    - Güvenlik yapılandırmasının değiştirilmesi,
    - Gereksiz servis veya portların kapatılması,
    - Yetkilendirme ve erişim kontrollerinin güçlendirilmesi,
    - Gerektiğinde sistemin izole edilmesi gibi uygun tedbirler değerlendirilir.
3. Bir zafiyetin teknik veya operasyonel nedenlerle doğrudan giderilememesi halinde alternatif veya telafi edici güvenlik kontrolleri uygulanır.
4. Zafiyetin kabul edilmesi gerekiyorsa, ilgili Risk Yönetimi Prosedürü kapsamında risk sahibi tarafından değerlendirilir ve gerekli onaylar alınır.
5. Zafiyetlerin giderilmesi için belirlenen faaliyetlerin tamamlanma durumu takip edilir.

4.5. Yama Yönetimi

1. İşletim sistemi, uygulama, ağ cihazı, güvenlik ürünü ve diğer bilgi sistemlerine ilişkin güvenlik yamaları düzenli olarak takip edilir.
2. Güvenlik yamalarının uygulanma önceliği, zafiyetin önem derecesi ve etkilenen sistemin kritiklik seviyesi dikkate alınarak belirlenir.

3. Kritik güvenlik yamaları, risk değerlendirmesine göre rutin yama dönemleri beklenmeden uygulanabilir.
4. Yama uygulanmadan önce, mümkün olan durumlarda test, uyumluluk ve geri dönüş planlaması yapılır.
5. Kritik sistemlerde yama uygulanması planlı bakım pencerelerinde gerçekleştirilir.
6. Yama uygulanmadan önce gerekli olması halinde sistem veya verilerin yedeği alınır.
7. Yama uygulaması sonrasında sistemin çalışabilirliği ve güvenlik durumunun uygunluğu kontrol edilir.
8. Yama uygulanamayan sistemler için gerekçe kayıt altına alınır ve alternatif güvenlik kontrolleri değerlendirilir.
9. BİDB kapsamında işletilmeyen bilgi sistemlerinin yama yönetiminden ilgili sistem/birim sorumlusu sorumludur.
10. Antivirüs, güvenlik duvarı ve saldırı tespit/önleme sistemleri gibi güvenlik ürünlerinin güncellemeleri ilgili teknik ekipler tarafından takip edilir.

4.6. Dış Taraflarca Gerçekleştirilen Zafiyet Taraması ve Sızma Testleri

Kurum içi çalışmalara ek olarak, gerekli görülen durumlarda yetkin ve bağımsız dış hizmet sağlayıcılardan zafiyet taraması ve/veya sızma testi hizmeti alınabilir.

Dış taraflarca gerçekleştirilecek çalışmalar öncesinde;

- Test kapsamı belirlenir,
- Test edilecek sistemler belirlenir,
- Test yöntemi ve çalışma planı oluşturulur,
- Hizmet sağlayıcının yetkinliği değerlendirilir,
- Kullanılacak araç ve yöntemler değerlendirilir,
- Gerekli gizlilik yükümlülükleri belirlenir,
- Çalışma takvimi ilgili taraflarla paylaşılır,
- Gerekiyorsa geçici kullanıcı hesapları oluşturulur.

Çalışma tamamlandığında geçici kullanıcı hesapları kapatılır veya yetkileri kaldırılır.

Sızma testi ve zafiyet taraması sırasında elde edilen bilgi ve raporlar Gizli veya Çok Gizli olarak sınıflandırılabilecek nitelikte ise ilgili bilgi sınıflandırma kurallarına uygun şekilde korunur.

4.7. Raporlama ve Kayıt

1. Zafiyet taraması ve sızma testi sonucunda elde edilen raporlar Bilgi İşlem Daire Başkanlığına teslim edilir.
2. İlgili raporlarda en az;
    - Tespit edilen zafiyet,
    - Etkilenen sistem/varlık,
    - Zafiyetin önem derecesi,

- Olası etkiler,
- Önerilen giderme yöntemi,
- Sorumlu birim/kişi,
- Hedef tamamlanma tarihi,
- Gerçekleştirilen faaliyet,
- Doğrulama sonucu bilgilerinin bulunması sağlanır.

3. Zafiyet raporları yetkisiz erişime karşı korunmalı ve yalnızca görev gereği erişmesi gereken kişiler tarafından erişilebilir olmalıdır.
4. Zafiyet yönetimine ilişkin kayıtlar, ilgili EYS doküman ve kayıt kontrol kurallarına uygun şekilde saklanır.

4.8. Zafiyetlerin Kapatılması ve Doğrulama

1. Giderildiği bildirilen zafiyetler mümkün olduğunda yeniden tarama, manuel kontrol veya ilgili teknik doğrulama yöntemi ile kontrol edilir.
2. Zafiyetin giderildiğinin doğrulanması sonrasında ilgili kayıt kapatılır.
3. Zafiyet giderilememişse ilgili kayıt açık tutulur ve gerekli ek aksiyonlar belirlenir.
4. İş ihtiyacı, teknik kısıt veya hizmet kesintisi riski nedeniyle zafiyetin giderilemediği durumlarda risk değerlendirmesi yapılır ve gerekli telafi edici kontroller uygulanır.
5. Gerekli durumlarda **Düzeltici ve İyileştirici Faaliyet** kaydı açılır.

4.9. Teknik Uyum Gözden Geçirmesi

1. Bilgi sistemlerinin kurum tarafından belirlenen bilgi güvenliği standartları, politika ve prosedürlere teknik açıdan uyumu düzenli olarak gözden geçirilir.
2. Teknik uyum gözden geçirmeleri;
   - Güvenlik yapılandırmalarının kontrolü,
   - Sistem ve uygulama sürümlerinin kontrolü,
   - Güvenlik yamalarının kontrolü,
   - Gereksiz servis ve portların kontrolü,
   - Erişim kontrollerinin kontrolü,
   - Zafiyet taramaları,
   - Sızma testleri,
   - Güvenlik cihazlarının yapılandırma kontrolleri gibi faaliyetleri içerebilir.
3. Teknik uyum kontrolleri uygun araçlarla veya manuel yöntemlerle gerçekleştirilebilir.
4. Kontrol sonuçları raporlanır ve tespit edilen uygunsuzluklar ilgili EYS süreçlerine aktarılır.
5. Gerekli görülmesi halinde teknik uyum kontrolleri bağımsız dış uzman veya kuruluşlar tarafından gerçekleştirilebilir.

4.10. Sonuçların Gözden Geçirilmesi

1. Gerekli görülen durumlarda BGYS Sorumlusu, BİDB ve ilgili sistem sorumluları zafiyet tarama ve yama yönetimi sonuçlarını birlikte değerlendirir.

2. Tekrarlayan zafiyetler, geciken yamalar ve giderilemeyen kritik zafiyetler ayrıca değerlendirilir.
3. Zafiyetlerin nedenleri, alınması gereken aksiyonlar ve risk azaltma yöntemleri belirlenir.
4. Gerektiğinde sonuçlar Yönetimin Gözden Geçirmesi toplantılarında değerlendirilmek üzere raporlanabilir.

5. YAPTIRIM

Bu politikada belirtilen kurallara aykırı hareket edilmesi halinde ilgili EYS süreçleri işletilir ve olayın niteliğine göre Disiplin Prosedürü hükümleri uygulanır.