BGYS POLİTİKASI

Politika Numarası	PLTK-14
Politika Tanımı	Teknik Güvenlik Açıklarının Yönetimi Politikası
Amaç ve İlkeler	Teknik açıklıklardan yararlanmayı önlemektir. Firmamızın güvenlik açıklarını tespit ederek bunları hızlı bir şekilde ele almak ve düzeltmeyi sağlayarak güvenliği artırmayı amaçlar.
Sorumluluklar	**Bilgi İşlem Personeli:** Teknik güvenlik açıklarının tespiti engellenmesi amacıyla sistemin kurulması ve denetlenmesinden sorumludur.
Sapma ve Özel Durumlar	Bu politikanın ihlali, disiplin önlemleri ve iş sürekliliğine bağlı kayıplara neden olabilir.

UYGULAMA

- **Güvenlik açıklarının tanımlanması ve sınıflandırılması:** Bilgi sistemlerindeki potansiyel güvenlik zayıflıklarının belirlenmesi ve bunların ciddiyetine göre sınıflandırılması.
- **Güvenlik açıklarının değerlendirilmesi**: Belirlenen güvenlik açıklarının analiz edilmesi ve risk değerlendirmesi yapılması.
- **Güvenlik açıklarının ele alınması:** Öncelikli güvenlik açıklarının düzeltilmesi veya kapatılması için uygun önlemlerin alınması.
- **Güvenlik açıklarının izlenmesi ve yönetimi**: Belirlenen güvenlik açıklarının düzeltilmesi sonrasında sürekli olarak izlenmesi ve yönetilmesi.

Bu süreç, bilgi sistemlerindeki güvenlik açıklarını etkin bir şekilde yöneterek siber saldırılara karşı dirençlerini artırılmasına yardımcı olmakla birlikte düzenli güncellemeler ve güvenlik önlemleri ile bilgi sistemlerinin sürekli olarak korunmasını sağlar.

Teknik Güvenlik Açığı Yönetimi ile İlgili Sorumluluklar ve Roller:

Güvenlik Açığı İzleme ve Değerlendirme

Bilgi İşlem Bölümü tarafından, sürekli olarak sistemlerde ve yazılımlarda potansiyel güvenlik açıkları izlenir ve belirlenir. Bu izleme süreci, güncel tehditlerin ve zafiyetlerin takip edilmesini sağlanır. Risk değerlendirmesi yaparak, tespit edilen güvenlik açıklarının ciddiyeti ve etkileri değerlendirilir.

Firmamız, güvenlik açıklarını belirlemek için endüstri standardı güvenlik açığı tarama araçlarından yararlanır. Bu araçlar, ağlarımızdaki ve sistemlerimizdeki potansiyel güvenlik zayıflıklarını tespit etmek için düzenli olarak kullanılır. Kullanılan güvenlik açığı tarama araçları, kurumumuzun mevcut teknolojik altyapısına uyumlu olmalıdır. Bu nedenle, araçların kurulumu ve kullanımı için uygun teknik gereksinimler ve uyumluluk kontrolleri yapılır.

Firmamız, güvenlik açıklarının tespitini desteklemek amacıyla yetkin ve yetkili kişiler tarafından planlanmış ve doküman haline getirilmiş sızma testleri veya güvenlik açığı değerlendirmeleri gerçekleştirir. Bu faaliyetler, güvenlik ekibimiz tarafından önceden belirlenen bir plan ve yönteme göre yapılır ve sonuçları dokümante edilir.

Sızma testleri veya güvenlik açığı değerlendirmeleri, konusunda uzmanlaşmış ve bu tür faaliyetlerde deneyimi olan yetkin kişiler tarafından gerçekleştirilir. Bu kişiler, güvenlik testleri konusunda uygun eğitim ve sertifikasyona sahip olmalıdır. Sızma testleri veya güvenlik açığı değerlendirmeleri düzenli aralıklarla tekrarlanır ve sürekli olarak güncellenir. Bu, güvenlik açıklarının zaman içinde değişen tehditlere karşı güncel ve etkin bir şekilde tespit edilmesini sağlar.

Testler, üretim sistemlerinde değil, genellikle ayrı bir test ortamında veya kontrollü bir ortamda gerçekleştirilir. Ayrıca, testler sırasında potansiyel risklerin ve olası etkilerin değerlendirilmesine özel önem verilir.

YAYIMLANMA TARİHİ	REVİZYON NO/TARİHİ	HAZIRLAYAN	ONAYLAYAN
26.04.2018	01/29.01.2024	Mehmet YALÇIN BGYS Temsilcisi	Yusuf KAYA Genel Müdür Yardımcısı

BGYS POLİTİKASI

Firmamız, güvenlik açıkları için kullanılan üçüncü taraf kütüphaneler ve kaynak kodunun izlenmesini sağlar. Bu, dış kaynaklardan alınan kütüphanelerin ve kodun güvenliği konusunda sürekli bir denetim ve gözlem sürecini içermektedir.

Üçüncü taraf kütüphanelerin ve kaynak kodunun kullanımı, güvenli kodlama ilkeleriyle uyumlu olmalıdır. Güvenli kodlama ilkeleri, yazılım geliştirme sürecinde güvenlik açıklarının en aza indirilmesini sağlamak için kullanılan bir dizi prensiptir. Bu prensipler, güvenli yazılım geliştirme yaşam döngüsünün her aşamasında uygulanır ve üçüncü taraf kaynakların izlenmesi sürecinde de dikkate alınır.

Üçüncü taraf kütüphaneler ve kaynak kodu için güvenlik güncellemeleri düzenli olarak takip edilir ve uygulanır.

Güncelleme ve Yama Yönetimi

Güvenlik açıkları tespit edildiğinde, Bilgi İşlem Bölümü tarafından hızlı bir şekilde uygun güncellemeleri ve yamaları uygulamakla sorumludur. Bu süreç, sistemlerin ve yazılımların güncel ve güvenli bir şekilde tutulmasını sağlar. Ayrıca, uygun yama yönetimi politikaları ve prosedürleri oluşturularak, güvenlik açıklarının kapatılması için zamanında ve etkili bir şekilde hareket edilir.

Güvenlik açıklarının kapatılması için uygulanan yamaların başarıyla uygulanıp uygulanmadığını doğrulamak için güvenlik açığı tarama araçları kullanılır. Bu araçlar, sistemlerdeki güvenlik yamalarının etkinliğini test eder ve varsa eksiklikleri veya hataları raporlayarak yama uygulamasının doğrulması gerçekleştirilir.

Varlık İzleme ve Envanter Yönetimi

Bilgi İşlem Bölümü, kuruluş içindeki tüm varlıkları (donanım ve yazılım) izler ve belirler. Bu, güvenlik açıklarının tespit edilmesi ve yönetilmesi sürecinde önemli bir adımdır. Varlık envanteri, güvenlik açıklarının etkilerini değerlendirmek ve uygun önlemleri almak için temel bir bilgi kaynağıdır.

Koordinasyon ve İletişim Sorumluluğu

Bilgi İşlem Bölümü, güvenlik açıklarıyla ilgili olarak farklı departmanlar arasında etkili iletişim ve koordinasyonu sağlar. Güvenlik açıklarının tespit edilmesi, değerlendirilmesi ve kapatılması süreçlerinde ilgili paydaşlarla düzenli iletişim ve işbirliği önemlidir. Ayrıca, güvenlik açıklarının yönetimi için belirlenen politika ve prosedürlerin tüm departmanlar tarafından uygun şekilde uygulanmasını sağlarlar.

Bu roller ve sorumluluklar, teknik güvenlik açığı yönetimi sürecinde etkili bir işleyişin sağlanmasını ve kurumun güvenlik risklerinin minimize edilmesini amaçlar. Bu şekilde, kuruluş, teknik açıklıklardan kaynaklanan riskleri azaltarak güvenli bir bilgi ortamı oluşturabilir.

Yazılım ve diğer teknolojiler için Güvenlik Açıklığı İzleme ve Bilgi Kaynakları:

- **Güvenlik Açıklığı Veritabanları:** Örneğin, Common Vulnerabilities and Exposures (CVE) veritabanı ve National Vulnerability Database (NVD) gibi kaynaklar
- **Yazılım ve Üretici Bildirimleri**
- **Güvenlik Blogları ve Forumlar**
- **Güvenlik Bilgilendirme Abonelikleri**
- **Yerel ve Ulusal Güvenlik Kurumları**

Firmamız, bilgi sistemi tedarikçileriyle yapmış olduğu sözleşmelerde güvenlik açığı raporlama, ele alma ve ifşa süreçlerinin detaylarını içeren hükümler bulundurmalıdır. Sözleşmeler, tedarikçilerin güvenlik açıklarını rapor etme ve bu açıklarla ilgili işbirliği yapma yükümlülüklerini belirler.

YAYIMLANMA TARİHİ	REVİZYON NO/TARİHİ	HAZIRLAYAN	ONAYLAYAN
26.04.2018	01/29.01.2024	Mehmet YALÇIN BGYS Temsilcisi	Yusuf KAYA Genel Müdür Yardımcısı

BGYS POLİTİKASI

Tedarikçiler, keşfettikleri güvenlik açıklarını derhal kurumumuza bildirmekle yükümlüdürler. Tedarikçilerin raporladığı güvenlik açıkları, firmamız tarafından hızlı bir şekilde ele alınır ve gerekli önlemler alınarak kapatılır. Tedarikçilerle işbirliği

Teknik güvenlik açıklarını ele almak için uygun önlemlerin alınması için aşağıdaki adımların izlenmesi gerekmektedir:

- Yazılım güncelleme yönetim süreci uygulanması
- Orijinal yazılımın korunması ve değişikliklerin belirlenmiş bir kopyaya uygulanması
- Değişikliklerin tam olarak test edilmesi ve dokümantasyonun yapılması
- Bağımsız değerlendirme kuruluşu tarafından test edilmesi ve geçerli kılınması (gerekirse)

Yazılım tedarikçisi veya diğer güvenilir kaynaklar tarafından önerilen geçici çözümler, güvenlik açığı kapatılana kadar geçici bir önlem olarak uygulanır. Bu çözümler, riskin azaltılmasına ve sistemin güvenliğinin korunmasına yardımcı olur.

Güvenlik açığı olan hizmetler veya yetenekler, mümkünse geçici olarak kapatılır. Bu, saldırı vektörlerinin kapatılmasına ve olası saldırıların önlenmesine yardımcı olur.

Güvenlik duvarları gibi ağ sınırlarında erişim kontrol mekanizmaları, güvenlik açığı tespit edildiğinde uyarlanabilir veya eklenir. Bu, potansiyel saldırganların ağa girişini engeller ve sistemi korur.

Hassas sistemler veya uygulamalar için uygun trafik filtreleri konuşlandırılır. Bu, saldırıların sistemlere ulaşmasını engeller ve hassas verilerin korunmasını sağlar.

Güvenlik açığı tespit edildiğinde, sistemlerin ve ağların izlenmesi artırılır. Bu, gerçek saldırıları tespit etmeye ve müdahale etmeye yardımcı olur.

Kullanıcılara ve personelinin güvenlik açığı hakkında bilgilendirilmesi ve farkındalık yaratılması sağlanır. Bu, sistemi korumak için alınan önlemlerin etkili bir şekilde uygulanmasına yardımcı olur. Tedarik edilen yazılımlarda güvenlik güncellemeleri hakkında düzenli olarak bilgi yayımlayan tedarikçilerle çalışma tercih edilir ve bu tür güncellemelerin otomatik olarak yüklenmesi için uygun bir kolaylık sağlanır. Bu şekilde, sistemlerin güvenliği sürekli olarak korunur ve güncel tutulur.

Teknik güvenlik açığı yönetimi süreci, etkinliğini ve verimliliğini sağlamak için düzenli olarak izlenmekte ve değerlendirilmektedir. Bu değerlendirme sürecinde, mevcut güvenlik açıkları ve alınan önlemler gözden geçirilerek, sürecin daha etkin hale getirilmesi için gereken düzeltme ve iyileştirmeler belirlenmektedir.

Şirketimiz, üçüncü taraf bir bulut hizmeti sağlayıcısı kullanması durumunda, bulut hizmeti sağlayıcısının kaynaklarının teknik güvenlik açığı yönetimini sağlaması beklenmektedir. Bulut hizmeti sağlayıcısının, teknik güvenlik açıklarıyla ilgili eylemlerini düzenli olarak raporlaması ve güncellemesi gerekmektedir. Bu sorumluluklar, bulut hizmeti sözleşmesinin bir parçası olarak belirlenmekte ve bulut hizmeti sağlayıcısı ile yapılan anlaşmalara dahil edilmektedir.

Otomatik güncelleme seçenekleri sunulduğunda, kullanıcılarımıza güncellemelerin otomatik olarak uygulanması veya kullanıcının tercihine göre manuel olarak gerçekleştirilmesi konusunda seçenekler sunulmaktadır. Böylece, güncellemelerin ne zaman gerçekleştirileceği konusu kullanıcıların kontrolünde gerçekleştirilmektedir.

YAYIMLANMA TARİHİ	REVİZYON NO/TARİHİ	HAZIRLAYAN	ONAYLAYAN
26.04.2018	01/29.01.2024	Mehmet YALÇIN BGYS Temsilcisi	Yusuf KAYA Genel Müdür Yardımcısı