Uygulama Güvenliği Değerlendirmesi

Kurumsal uygulamalarınızı ister şirket içinde üretin ister başka bir firmadan satın alın, tek bir kodlama hatasının sizi saldırılara açık bırakacak bir güvenlik açığı oluşturduğunu unutmayın. Böyle bir güvenlik açığı yüzünden ciddi finansal zararlara ve itibar kaybına uğrayabilirsiniz. Bir uygulamanın yaşam döngüsü boyunca, yazılım güncellemeleri veya güvenli olmayan bileşen yapılandırması aracılığıyla uygulamada yeni güvenlik açıklıkları oluşabilir veya yeni saldırı yöntemleri gelişebilir.

Kaspersky Lab'in Uygulama Güvenlik Değerlendirme Hizmetleri; büyük bulut tabanlı çözümler, ERP sistemleri, çevrimiçi bankacılık ve diğer özel işletme uygulamaları gibi her türlü uygulamanın yanı sıra farklı platformlarda (iOS, Android ve diğerleri) yer alan mobil ve gömülü uygulamalardaki güvenlik açıklarını ortaya çıkarır.

Uzmanlarımız, pratik bilgileri ve deneyimleri, uluslararası en iyi uygulamalarla birleştirerek kurumunuzu aşağıdaki tehditlere karşı savunmasız hale getirebilecek güvenlik kusurlarını tespit eder:

- Gizli bilgileri çekmek
- Verilere ve sistemlere sızmak ve bunları değiştirmek
- Hizmeti engelleme saldırıları başlatmak
- Dolandırıcılık faaliyetleri gerçekleştirmek

Tavsiyelerimize uyduğunuz takdirde uygulamalarda ortaya çıkarılan güvenlik açıkları düzeltilebilir ve bu tür saldırılar önlenebilir.

Hizmetin avantajları

Kaspersky Lab Uygulama Güvenliği Değerlendirme Hizmetleri, uygulama sahiplerine ve geliştiricilerine şu konularda yardımcı olur:

- **Finansal ve işlemsel zararları ve itibar kayıplarını önleyin**. Uygulamalara karşı düzenlenen saldırılarda kullanılan güvenlik açıklarını proaktif bir şekilde tespit eder ve düzeltir
- **Onarım masraflarından tasarruf edin**. Henüz geliştirilme veya test etme aşamasında olan uygulamalardaki güvenlik açıklarını takip eder ve uygulamalar, kullanıcı ortamına ulaşmadan onları düzeltir. Aksi takdirde bu uygulamaları onarmak, ciddi karışıklıklara ve masraflara neden olabilir.
- **Güvenli bir yazılım geliştirme yaşam döngüsünü (S-SDLC) destekler**. Güvenli uygulamaların geliştirilmesine ve korunmasına bağlıdır.
- **PCI DSS veya HIPAA gibi uygulama güvenliğini kapsayan devlet, endüstri ve şirket kurumsal standartlarına uyum sağlar**

Hizmetin kapsamı ve seçenekler

Değerlendirilen uygulamalar, gömülü ve mobil uygulamalar dahil olmak üzere standart veya bulut tabanlı resmi web sitelerini ve işletme uygulamalarını kapsar.

İhtiyaçlarınıza ve uygulamanın özelliklerine uygun hale getirilebilen hizmetler şunları içerebilir:

- **Black-box testi**: Dış saldırgan taklit edilir
- **Grey-box testi**: Çeşitli profillere sahip geçerli kullanıcılar taklit edilir
- **White-box testi**: Kaynak kodlar dahil olmak üzere uygulamaya tam erişim analizi; bu yaklaşım güvenlik açığı sayısının ortaya çıkartılması açısından en etkili yöntemdir
- **Uygulama Firewall etkililiği değerlendirmesi**: Güvenlik açıklarını bulmak ve açıklardan yararlanan yazılımların engellenip engellemediğini doğrulamak için uygulamalar, koruma duvarı koruması etkinken ve devre dışıyken test edilir

Sonuçlar

Kaspersky Lab Uygulama Güvenliği Değerlendirme Hizmetleri tarafından tanımlanabilecek güvenlik açıkları şunları içerir:

- Çok faktörlü doğrulama dahil olmak üzere doğrulama ve yetkilendirme konusundaki kusurlar
- Kod enjeksiyonu (SQL Enjeksiyonu, İşletim Sistemi Komutları vb.)
- Dolandırıcılığa yol açan mantıksal güvenlik açıkları
- Müşteri tarafı güvenlik açıkları (siteler arası komut çalıştırma, siteler arası istek sahteciliği vb.)
- Zayıf şifreleme kullanımı
- Müşteri tarafı iletişimlerinde güvenlik açıkları
- Ödeme sistemlerinde PAN maskeleme eksikliği gibi veri depolamanın ve aktarımının güvenli olmaması
- Oturum saldırılarına yol açanlar dahil olmak üzere yapılandırma kusurları
- Hassas bilgilerin ifşa edilmesi
- WASC Tehdit Sınıflandırması v2.0 ve OWASP İlk 10 gibi projelerin listelerindeki tehditlere yol açan diğer web uygulaması güvenlik açıkları.

Sonuçlar, yönetimle ilgili noktaları vurgulayan bir yönetici özetinin yanı sıra değerlendirme süreçleri, sonuçları, ortaya çıkan güvenlik açıkları ve onarım için önerileri içeren bir nihai rapor olarak sunulur. Ayrıca gerektiği takdirde teknik ekibiniz veya üst düzey yöneticileriniz için videolar ve sunumlar hazırlanabilir.

Kaspersky Lab'in Uygulama Güvenliği Değerlendirmesine Yaklaşımı Hakkında

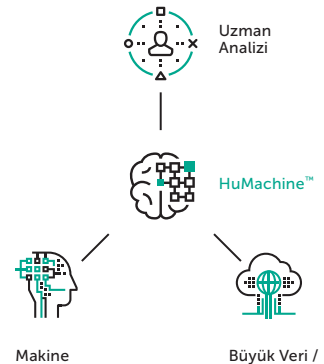
Uygulamaların güvenlik değerlendirmeleri Kaspersky Lab'in güvenlik uzmanları tarafından hem manuel olarak hem de otomatik araçlar kullanılarak gerçekleştirilir. Bu test sırasında sistemlerinizin gizliliğine, bütünlüğüne ve kullanılabilirliğine özen gösterilir ve aşağıdaki uluslararası standartlar ile en iyi uygulamalara uyum sağlanır:

- Web Uygulama Güvenliği Konsorsiyumu (WASC) Tehdit Sınıflandırması
- Açık Web Uygulamaları Güvenlik Projesi (OWASP) Test Kılavuzu
- OWASP Mobil Güvenlik Test Kılavuzu
- Kurumunuzun sektörüne ve konumuna göre diğer standartlar

Proje ekip üyeleri farklı platformlar, programlama dilleri, çerçeveler, güvenlik açıkları ve saldırı yöntemleri dahil olmak üzere alanlarında kapsamlı ve kullanışlı bilgilere sahip deneyimli uzmanlardır. Uzmanlarımız, önemli uluslararası konferanslarda sunumlar yapmaktadır ve Oracle, Google, Apple, Facebook ve PayPal dahil büyük uygulama ve bulut hizmetleri tedarikçilerine güvenlik danışmanlığı hizmeti vermektedir.

Hizmetin sunulma seçenekleri

Güvenlik değerlendirme hizmetleri; hizmet kapsamındaki sistemlerin özelliklerine, güvenlik değerlendirme hizmetinin türüne ve çalışma koşulları gerekliliklerinize bağlı olarak uzaktan veya şirket içinde sağlanabilir. Bu hizmetlerin birçoğu uzaktan yürütülebilir.



Kaspersky Lab
Enterprise Cybersecurity:**www.kaspersky.com.tr/enterprise**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenliği Haberleri: **www.business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.com.tr