Sızma Testi

BT altyapısının olası siber saldırılara karşı güvende olmasını sağlamak tüm kurumlar için sürekli devam eden bir mücadeledir. Ancak binlerce çalışana, yüzlerce bilgi sistemine ve dünya genelinde birçok iş yerine sahip büyük şirketler için bu mücadele çok daha zorlayıcıdır.

Sızma testi, kötü amaçlı bir aktörün önemli sistemlerde yüksek ayrıcalıklar elde etmek için ağınızdaki güvenlik kontrollerini atlatmaya çalıştığı olası bir saldırı senaryosunun uygulamalı gösterimidir.

Kaspersky Lab'in Sızma Testi; güvenlik açıklarını ortaya çıkararak, farklı saldırı biçimlerinin olası sonuçlarını analiz ederek, mevcut güvenlik önlemlerinizin etkililiğini değerlendirerek ve onarımla ilgili önlemler ve iyileştirmeler önererek altyapınızdaki güvenlik hatalarını daha iyi anlamanızı sağlar.

Sızma testi Hizmetleri

Kaspersky Lab'in Sızma Testi size ve kurumunuza şu konularda yardımcı olur:

- **Ağınızdaki en zayıf noktaları belirleyin**. Bu sayede gelecekteki riskleri azaltmak için dikkatinizi ve bütçenizi toplamanız gereken alanlar konusunda daha bilinçli kararlar alabilirsiniz.
- **Siber saldırıların neden olduğu finansal ve işlemsel zararları ve itibar kayıplarını önleyin.** Güvenlik açıklarını proaktif bir şekilde tespit ederek ve düzelterek bu saldırıların gerçekleşmesini tamamen önleyin.
- **Resmi, sektörel ve kurumsal standartlara uyum sağlayın**. Bu tür bir güvenlik değerlendirmesi gerektiren standartlara uyum sağlayın (örneğin, Ödeme Kartı Sektörü Veri Güvenliği Standartları (PCI DSS)).

Hizmetin kapsamı ve seçenekler

İhtiyaçlarınıza ve BT altyapınıza bağlı olarak aşağıdaki hizmetlerden herhangi birini veya tümünü kullanmayı tercih edebilirsiniz:

- **Dışarıdan sızma testi:** Sisteminiz hakkında hiçbir ön bilgisi olmayan bir "saldırganın" internet üzerinden düzenlediği saldırı sonucu yapılan güvenlik değerlendirmesi.
- **İçeriden sızma testi:** Ofisinize yalnızca fiziksel erişimi olan bir ziyaretçi veya sınırlı sistem erişimi olan sözleşmeli bir çalışan gibi içeriden bir saldırgana dayalı senaryolar.
- **Sosyal mühendislik testi:** Kimlik avı, e-postalarla sahte kötü amaçlı bağlantılar gönderilmesi ve şüpheli ekler gibi sosyal mühendislik saldırılarını taklit ederek personeliniz için güvenlik farkındalığı değerlendirmesi.
- **Kablosuz ağ güvenliği değerlendirmesi:** Uzmanlarımız şirketinizi ziyaret ederek WiFi güvenlik kontrollerinizi analiz eder.

BT altyapınızın istediğiniz kısmını sızma testinin kapsamına alabilirsiniz. Ancak tüm ağı veya en büyük bölümlerini bu testte değerlendirmenizi öneririz. Çünkü uzmanlarımız, olası bir saldırganla aynı koşullar altında çalıştığında her zaman daha yararlı sonuçlar elde edilir.

Sızma testi sonuçları

Bu Hizmet, kritik ağ bileşenlerine yetkisiz erişim sağlamak amacıyla yararlanılabilecek güvenlik eksikliklerini ortaya çıkarmak için tasarlanmıştır. Bu güvenlik açıkları şunları içerebilir:

- Savunmasız ağ mimarisi, yetersiz ağ koruması
- Ağ trafiğinin engellenmesine ve yeniden yönlendirilmesine neden olabilecek güvenlik açıkları
- Farklı hizmetlerdeki yetersiz doğrulama ve yetkilendirme
- Zayıf kullanıcı kimlik bilgileri
- Aşırı kullanıcı ayrıcalıkları dahil olmak üzere yapılandırma hataları
- Uygulama kodundaki hatalardan kaynaklanan güvenlik açıkları (kod enjeksiyonu, dizin gezinimi, müşteri tarafı güvenlik açıkları vb.)
- Yeni güvenlik güncellemelerine sahip olmayan eskimiş donanımların ve yazılım sürümlerinin kullanılmasına dayalı güvenlik açıkları
- Bilgilerin ifşa edilmesi

Sonuçlar; test sonuçlarının genel hatlarını ve saldırı vektörlerini gösteren bir yönetici özetinin yanı sıra test süreci, sonuçları, ortaya çıkarılan güvenlik açıkları ve onarım için öneriler ile ilgili detaylı teknik bilgileri içeren nihai bir rapor olarak sunulur. Ayrıca gerektiği takdirde teknik ekibiniz veya üst düzey yöneticileriniz için videolar ve sunumlar hazırlanabilir.

Kaspersky Lab'in sızma testlerine yaklaşımı hakkında

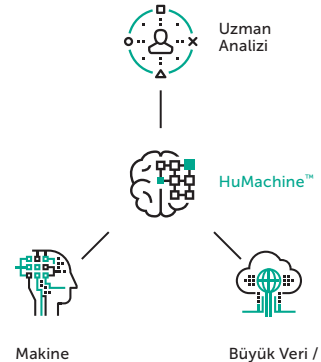
Sızma testleri, gerçek hacker saldırılarını taklit etmesine rağmen bu testler son derece sıkı bir şekilde kontrol edilir. Testler, Kaspersky Lab güvenlik uzmanları tarafından sistemlerinizin gizliliğine, bütünlüğüne ve kullanılabilirliğine özen gösterilerek ve aşağıdakiler dahil olmak üzere uluslararası standartlara ve en iyi uygulamalara uygun olarak gerçekleştirilir:

- Sızma Testi Uygulama Standardı (PTES)
- NIST Özel Yayınları 800-115 Bilgi Güvenliği Testi ve Değerlendirmesi İçin Teknik Kılavuz
- Açık Kaynak Güvenlik Testi Metodolojisi El Kitabı (OSSTMM)
- Bilgi Sistemleri Güvenlik Değerlendirmesi Çerçevesi (ISSAF)
- Web Uygulama Güvenliği Konsorsiyumu (WASC) Tehdit Sınıflandırması
- Açık Web Uygulamaları Güvenlik Projesi (OWASP) Test Kılavuzu
- Yaygın Güvenlik Açıkları Puanlama Sistemi (CVSS)

Proje ekip üyeleri, alan hakkında kapsamlı, güncel ve kullanışlı bilgilere sahip deneyimli uzmanlardır. Bu uzmanlar Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens ve SAP dahil olmak üzere endüstri liderlerine güvenlik danışmanlığı yapan saygın kişilerdir.

Hizmetin sunulma seçenekleri

Güvenlik değerlendirmesinin türüne, sistemlerinize özgü özelliklere ve çalışma pratiklerine bağlı olarak güvenlik değerlendirmesi hizmetleri uzaktan veya yerinde yapılabilir. Birçok hizmet uzaktan gerçekleştirilebilir, hatta içeriden sızma testi bile VPN erişimiyle gerçekleştirilebilir. Ancak bazı hizmetlerin (kablosuz ağ güvenliği değerlendirmesi gibi) şirket içinde sunulması gerekir.



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