Privia SECURITY

Ağ Güvenliği Test Hizmeti

Profesyonel Offensive Security Hizmetleri

"Güvenli Ağ, Güvenli İletişim!"

Küçükbakkalköy Mah. Kocasinan Cad.
Privia Plaza No:42 Ataşehir, İstanbul

+90 (216) 514 72 14

www.priviasecurity.com

"Güvenli iletişim sağlamak için sızma testleriyle ağdaki zafiyetleri ortaya çıkarıyor ve tehditlere karşı önlemler alınmasını sağlıyoruz."

Ağ güvenliği, günümüzün dijital dünyasında işletmelerin en kritik ihtiyaçlarından biridir. Alanında uzman siber güvenlik ekiplerimiz tarafından gerçekleştirilen kapsamlı ağ tabanlı sızma testlerimiz, siber tehdit aktörü bakış açısıyla ağ altyapınızı değerlendirerek güvenlik açıklarını tespit eder.

Ağ güvenliği hizmetimiz, DDoS saldırı simülasyonları, yük testleri, kablosuz ağ güvenlik testleri ve Ortadaki Adam (MITM) saldırıları gibi bir çok saldırı tekniğinin simüle edildiği kapsamlı bir test biçimidir. Her bir teknik, ağınızın farklı yönlerini değerlendirmeyi ve olası saldırı vektörlerini belirlemeyi amaçlar. Attack Surface Assessment ile tüm varlıklarınızı analiz ederek, saldırganların erişim sağlayabileceği zayıf noktaları ve protokolleri test edilerek riskler ortaya çıkartılır.

Tüm süreç boyunca ekibimiz, tespit edilen zafiyetlerin teknik ayrıntılarını ve çözüm önerilerini içeren detaylı bir rapor sunar. Ağ Güvenliği Hizmetimizle amacımız yalnızca zafiyetleri bulmak değil, aynı zamanda bu zafiyetleri kapatmanız için en uygun stratejiyi geliştirmenize destek olmaktır.

Hizmete Ait Bileşenler

DDoS Testleri

DDoS (Distributed Denial of Service) testleriyle sistemlerin yoğun trafik saldırılarına karşı dayanıklılığı ölçülür. Gerçekleştirilen testler sırasında sunuculara ve ağlara sahte trafik yönlendirilerek sunucuların performansları belirlenir. Olası kesintilere karşı güvenlik önlemlerinin planlanmasını sağlar. Test çıktılarına göre kapasite artırımı ve güvenlik duvarı optimizasyonu gibi öneriler sunulur.

Kablosuz Ağ Güvenlik Testleri

Kablosuz ağlar, çeşitli şifreleme standartları (WEP, WPA, WPA2 gibi) hedef alınarak alınarak analiz edilir. Testler sırasında yetkisiz erişim denemeleri ve parolaların kırılma olasılığı değerlendirilir. Sinyal gücü ve erişim noktalarına yönelik zafiyetler tespit edilerek riskler ortaya çıkarılır. Güvenlik politikalarının güçlendirilmesi için öneriler sunulur.

MITM Testleri

MITM testleri ile saldırganların iletişim akışına müdahale etme riskleri test edilerek veri gizliliği incelenir. Kullanıcı bilgileri, parolalar ve hassas verilerin ele geçirilme ihtimalleri değerlendirilir. Şifreleme protokollerinin etkinliği test edilir ve zayıf yönler tespit edilir. İletişim güvenliğinin artırılması için uygulanabilir önlemler önerilerek, veri transferinin kaynak ve hedef arasında güvenle iletilmesi sağlanır.

Attack Surface Assessment

Attack Surface Assesment, kurumun dijital ekosistemindeki tüm varlıkların saldırgan perspektifiyle incelenmesini sağlar. İnternet erişimli servisler, açık portlar, eski yazılım sürümleri ve yanlış yapılandırmalar titizlikle analiz edilerek zafiyetlerin keşfedilmesi amaçlanır. Yapılan değerlendirme, ağın en savunmasız noktalarının da ortaya çıkarılmasını ve risklerin önceliklendirilmesini mümkün kılar. Elde edilen bilgi, belge ve bulgulara dayanarak, saldırıya açık alanların azaltılması ve varlıkların güvenliğinin güçlendirilmesi için kapsamlı öneriler sunulur.

Raporlama

Ağ Güvenlik testleri neticesinde, tespit edilen tüm zafiyetler ve olası güvenlik riskleri detaylı raporlar halinde sunulur. Her bir bulgu, teknik açıklamalar ve iş süreçlerine etkileriyle birlikte değerlendirilir. Zafiyetlerin giderilmesi için önerilen çözüm yolları, kurumun güvenlik ekibiyle paylaşılır. Raporlar, yalnızca mevcut açıkların kapatılmasını değil, uzun vadeli iyileştirme stratejilerini de içerir.

Sık Sorulan Sorular

Ağ güvenliği testi nedir?

Ağ güvenliği testi, ağ altyapısındaki zafiyetleri ve olası tehditleri belirlemek için gerçekleştirilen bir değerlendirme hizmetidir. Testler firewall, router, sunucu ve ağ cihazlarının güvenlik açıklarını analiz ederek, bu açıkların istismar edilmeden önce giderilmesine olanak tanır.

Network Pentest neden önemlidir?

Ağ sızma testi, gerçek dünyadaki saldırganların kullandığı yöntemleri kullanarak güvenlik açıklarını keşfeder. Ağ sızma testleriyle kurumlar, saldırı gerçekleşmeden önce riskleri belirleyip gerekli önlemleri alarak veri ihlallerini ve operasyonel kesintileri önler.

DDoS saldırı simülasyonları nasıl yapılır?

DDoS (Distributed Denial of Service) testleri, sistemleri büyük miktarda sahte trafik ile baskı altına alarak yanıt verme kapasitelerini test eder. Süreç, hizmet kesintilerini önlemek için gerekli altyapı optimizasyonlarını belirlemeye yardımcı olur.

Kurum içi ve kurum dışı ağ güvenlik testleri arasındaki fark nedir?

Kurum içi testler, iç ağdan gelecek tehditleri değerlendirmeyi amaçlarken, kurum dışı testler internet üzerinden erişilebilen hizmetlere odaklanır. Bu iki yaklaşım, farklı tehdit vektörlerine karşı tam koruma sağlamak için bir arada kullanılır.

Kablosuz ağların güvenliği neden kritik öneme sahiptir?

Kablosuz ağlar, fiziksel koruma sınırlamalarından dolayı saldırganlar için cazip hedeflerdir. Yanlış yapılandırılmış bir kablosuz ağ, saldırganların ağda serbestçe dolaşmasına ve kritik verilere erişmesine yol açabilir.

Siber Güvenlikte Doğru Çözüm Ortağınız

2018 yılında siber güvenliğin geleceği için yola çıkan Privia Security, kuruluşundan bu yana, müşterilerine yüksek kaliteli hizmet sunmayı amaçlamaktadır. Güçlü ve yetenekli ekibimiz, siber güvenliğin her alanında hizmet verdiğimiz organizasyonlara en güvenilir ve kapsamlı çözümleri sunarak, organizasyonların dijital dünyadaki güvenlik ihtiyaçlarını karşılamaktadır.

Günümüzde hızla gelişen ve karmaşık hale gelen siber tehditlerle mücadele etmek giderek zorlaşıyor. Bu noktada Privia Security olarak, müşterilerimize ihtiyaç duydukları hem defansif hem de ofansif siber güvenlik stratejilerini en ileri teknolojiyle sunuyoruz. İnovatif AR-GE ürünlerimiz ve stratejik danışmanlığımız sayesinde organizasyonların siber güvenlik olgunluğunu artırmayı ve onlara proaktif çözümler sunmayı hedefliyoruz. Şu anda 300'den fazla büyük kuruluşun güvenliğini sağlamaktan gurur duyuyoruz.

Uluslararası ve Yerel Siber Güvenlik Çözümleri

Privia Security olarak, Avrupa, Asya, Ortadoğu ve Amerika dahil olmak üzere geniş bir coğrafyaya siber güvenlik hizmetleri sunmaktayız. Offensive, Defensive ve Forensic alanlarında uzmanlaşmış ekiplerimiz, kritik altyapılar, aviyonik sistemler, kurumsal ağlar ve askeri alanlar gibi farklı sektörlerde faaliyet gösteren organizasyonlara özel çözümler geliştirmektedir.

Ayrıca savunma kapasitelerini güçlendirmek isteyen ülkelere yönelik geliştirdiğimiz PriviaHub siber savaş simülasyonu ile siber savaş stratejilerinin test edilmesi, tatbikatların yürütülmesi ve uzmanların niteliklerinin ölçülmesi için kapsamlı çözümler sunuyoruz. Bu inovatif platform özel sektör, akademi ve askeri alanlarda tatbikat ihtiyaçlarını karşılamak üzere tasarlanmıştır.

İleri Teknoloji ile Güvenli Gelecek

İstanbul, Ankara, Londra ve Cumhuriyet Teknopark'taki Ar-Ge merkezimizde, müşterilerimize değer katan projeler geliştiriyoruz. Penetrasyon testleri, Red Team operasyonları, siber güvenlik eğitimleri ve kurumlara özel siber güvenlik çözümlerimizle sektörde fark yaratmaya devam ediyoruz. "Privacy For You" sloganımızla, güvenlik ve gizliliğe yenilikçi bir bakış açısı getiriyor ve müşterilerimizin dijital geleceğini güvence altına alıyoruz.

Privia
SECURITY