Privia SECURITY

Altyapı Güvenliği Test Hizmeti

Profesyonel Offensive Security Hizmetleri

"Sağlam Altyapı, Sağlam Güvenlik!"

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

+90 (216) 514 72 14

www.priviasecurity.com

“Güçlü bir altyapı, sadece bugünün değil, geleceğin risklerine karşı da hazırlıklı olmanızı sağlar.”

Altyapı güvenliği test hizmetimiz, kurumların IT, OT ve IoT ağlarında yer alan varlıklarının tüm katmanlarını kapsamlı bir şekilde analiz ederek, güvenlik zafiyetlerini belirlemeye odaklanır. Kritik ağ cihazlarından sunuculara, veri merkezlerinden kontrol sistemlerine kadar geniş bir yelpazede yapılan testler, operasyonel sürekliliği korumak ve zayıf noktaları önceden tespit etmek için tasarlanmıştır. Altyapı güvenliği test hizmeti, modern siber tehditlerle başa çıkmak için en iyi güvenlik standartlarına (OSSTMM, NIST, ISO 27001) uygun bir şekilde yürütülür.

Uzman ekibimiz, saldırgan bakış açısıyla çalışarak, altyapıda bulunan tüm olası zafiyetleri keşfeder. Gerçek dünya senaryolarını simüle eden testlerimiz ile hem iç hem de dış ağlarda detaylı analizler gerçekleştiririz. Ağ cihazlarının konfigürasyonundan erişim kontrol politikalarına kadar her detay titizlikle incelenir. Elde edilen tüm bilgi, belge ve bulgular, güvenliği iyileştirmek için özelleştirilmiş çözümlerle birlikte sunulur.

Hizmet kapsamında kurumların güvenlik politikalarının ne kadar etkin olduğu da ölçülür. Süreç sonunda hazırlanan detaylı raporlar ve aksiyon planları, sistemleri sürekli olarak iyileştirme imkânı sunar. Altyapınız ne kadar güçlü olursa, riskler o kadar azaltılır. "Sağlam Altyapı, Sağlam Güvenlik" anlayışıyla organizasyonların güvenlik riskleri minimize edilir.

Hizmete Ait Bileşenler

Ağ Yapısı ve Konfigürasyon Testleri

Ağ cihazlarının (router, switch, firewall) aktif davranışlarını incelenerek zafiyetleri belirlenir. Yanlış yapılandırmaların risklerini minimize etmek ve güvenlik politikalarının etkinliğini ölçmek için detaylı analizler gerçekleştirilir.

Erişim Kontrolü Testleri

Kritik sistem ve veri erişimlerini denetlenerek kimlerin, neye, nasıl erişebildiği test edilir. Zayıf parola politikaları, gereksiz yetkilendirmeler gibi güvenlik zafiyetleri tespit edilir.

Güvenlik Duvarı ve VPN Testleri

Güvenlik duvarı ve VPN yapılandırmalarını saldırgan bakış açısıyla değerlendirir. Kurum dışı bağlantıların ne kadar güvenli olduğunu test edilerek, siber saldırı yüzeyini minimize edilir.

Yama Yönetimi

Yazılım, donanım ve işletim sistemlerinin güncelliğini kontrol ederek yama eksiklikleri tespit edilir. Eksik yamalar nedeniyle oluşabilecek zafiyetlerin siber saldırılarda nasıl kullanılabileceği ve olası etkileri analiz edilir.

Ağ Segmentasyonu ve İzolasyon Testleri

Kritik sistemlerin ayrıştırılması ve trafiğin kontrollü bir şekilde yönlendirilmesi için ağ segmentasyonu test edilir. İzole edilmemiş sistemlerin güvenlik risklerini ve saldırıların yayılma potansiyeli tespit edilir. Güvenli segmentasyon ile saldırı yüzeyini daraltmaya yönelik öneriler sunulur.

İz Kayıt Yönetimi

Kritik logların doğru tutulup saklandığını ve olay müdahale süreçlerinde kullanılabilirliğini değerlendirilir. Güçlü iz kayıt yönetimiyle saldırıların erken tespiti ve hızlı müdahale için yönlendirmeler yapılır.

Aksiyon Planı ve Kapanış

Tespit edilen zafiyetlere yönelik çözüm önerileri ve aksiyon planları hazırlanır. Testler sonrasında organizasyonun güvenlik seviyesini artırmak için iyileştirme adımları önerilir. Hazırlanan detaylı raporlar, güvenlik stratejilerinin gözden geçirilmesine ve yeni önlemler alınmasına için referans sağlar.

Sık Sorulan Sorular

Altyapı güvenliği testi nedir?

Altyapı güvenliği testi, ağ ve sistemlerin zayıf noktalarını belirlemek ve güvenlik zafiyetlerini kapatmak için yapılan kapsamlı bir test sürecidir. Test kapsamında sunucular, ağ cihazları ve veri iletişim protokolleri incelenir. Altyapı güvenliği testi, olası tehditleri önceden belirleyerek operasyonel kesintileri önlemek için kritik öneme sahiptir.

Bu testlerin amacı nedir?

Amacı, siber saldırganların kullanabileceği zafiyetleri önceden keşfetmek ve önleyici tedbirler almaktır. Sistemlerin güvenilirliğini artırmak ve bilgi sızıntılarını önlemek de önemli amaçlar arasındadır.

Hangi standartlar kullanılır?

ISO 27001, NIST SP 800-115 ve OSSTMM gibi uluslararası kabul görmüş standartlar kullanılır. Bu standartlar, testlerin kapsamını ve test metodolojisini belirler. Tespit edilen zafiyetlerin nasıl giderileceğine yönelik en iyi çözüm yollarını sunar.

Test süresi ne kadar sürer?

Testin süresi, altyapının büyüklüğüne ve kapsamına göre değişiklik gösterir. Küçük sistemler için birkaç gün sürebilirken, büyük ve karmaşık ağlar için bu süre birkaç haftayı veya ayı bulabilir. Sürecin her adımı organizasyonun ekibiyle karşılıklı bir planlama çerçevesinde yürütülür.

Test sırasında sistem kesintisi olur mu?

Testler, genellikle operasyonel aksaklık yaşanmadan gerçekleştirilir. Kritik sistemler üzerinde test yapılırken güvenlik önlemleri alınarak kesinti riski en aza indirilir. Testler boyunca, iş sürekliliği sağlanırken sistemlerin güvenliği de artırılır.

Hangi bileşenler test edilir?

Ağ cihazları, sunucular, güvenlik duvarları, VPN altyapısı ve erişim kontrol sistemleri test edilir. Bu bileşenlerin yapılandırmalarının doğru olup olmadığı kontrol edilerek zafiyetler tespit edilir. Gerçekleştirilen testler sonucunda hem iç hem dış tehditlere karşı önlemler alınır.

Sonuçlar nasıl raporlanır?

Testin sonunda, tespit edilen tüm zafiyetleri ve çözüm önerilerini içeren detaylı bir rapor organizasyonun güvenlik ekibine sunulur. Rapor, sistem iyileştirmeleri için gerekli adımları içermektedir. Ayrıca, uzun vadeli güvenlik stratejilerinin geliştirilmesine katkı sağlar.

Testler ne sıklıkla yapılmalıdır?

Testlerin yılda en az iki kez veya önemli sistem değişikliklerinden sonra tekrarlanması önerilir. Sürekli gelişen tehditler karşısında düzenli testler, sistemlerin her zaman güvende kalmasını sağlar. Gerçekleştirilen testler uyumluluk gereksinimlerinin karşılanmasına da katkıda bulunur.

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