Privia SECURITY

DoS-DDoS Test Hizmeti

Profesyonel Offensive Security Hizmetleri

"İş Süreçleriniz Kesintisiz Devam Etsin!"

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

+90 (216) 514 72 14

www.priviasecurity.com

"DoS/DDoS Test Hizmeti, sisteminizi en zorlu trafik koşullarında sınayarak, altyapınızın performansını ve güvenilirliğini artırır."

DoS/DDoS Test Hizmeti, ağınızı sahte trafikle zorlayarak altyapınızın dayanıklılığını ölçer ve performans sınırlarınızı belirler. Günümüzde siber saldırıların başlıca yöntemi olan DDoS saldırıları, iş süreçlerini aksatabilir ve sistem kesintilerine neden olabilir. Bu testlerle olası zafiyetler önceden tespit edilir, gerekli iyileştirmeler yapılarak kesintisiz bir hizmet deneyimi sağlanır.

Yoğun trafik koşullarında ağınıza zarar vermeden gerçekleştirilen testlerle, sisteminizin maksimum yük altında nasıl davrandığı analiz edilir. Kritik iş süreçleri aksamasın diye erken uyarı mekanizmaları test edilerek trafik yönlendirme ve filtreleme çözümleri gözden geçirilir. Ayrıca hizmet kapsamında, saldırı anında müdahale senaryoları geliştirilerek altyapınızın hazırlığı test edilir.

DoS/DDoS Test hizmetiyle sadece mevcut güvenlik açıkları tespit edilmez, aynı zamanda gelecekteki saldırılara karşı önleyici stratejiler oluşturulur. DDoS saldırılarına karşı güçlü bir savunma kurmak, iş sürekliliği ve müşteri memnuniyeti açısından kritik önem taşır.

Hizmete Ait Bileşenler

Trafik Simülasyonu

Bu evrede, farklı trafik senaryoları kullanılarak sistemin sınırları test edilir. Gerçek saldırı koşullarına benzer yoğun trafik durumları yaratılarak performans darboğazları ve tepki süreleri değerlendirilir. Elde edilen sonuçlar, altyapının iyileştirilmesi ve hizmet sürekliliği stratejilerinin geliştirilmesi için katkıda bulunur.

Kapasite Ölçümleme

Sistemlerin ne kadar trafiği kaldırabileceğini belirlemek için gerçekleştirilir. Sistem üzerinde artan yük koşullarında oluşabilecek hatalar ve performans sorunları değerlendirilir. Amaç, kritik eşiklerin belirlenerek ağ altyapısının ihtiyaç duyduğu iyileştirmelerin tespit edilmesidir.

Filtreleme Kontrolleri

CDN, güvenlik duvarları, yük dengeleyiciler ve diğer ağ cihazlarının etkinliği analiz edilir. Trafik yönlendirme stratejileri, hizmet sürekliliğini sağlamak ve zararlı trafiği etkili şekilde izole etmek için öneriler sunulur. Yapılan kontroller, olası saldırıların erken tespit edilmesine ve durdurulmasına olanak tanır.

Uyarı Mekanizmaları

Saldırı anında müdahale sürelerini optimize etmek için izleme ve uyarı araçlarının performansı test edilir. Sistemlerin tehditlere ne kadar hızlı tepki verdiği analiz edilerek erken uyarı mekanizmalarının doğruluğu değerlendirilir.

Müdahale ve Kurtarma Planları

DDoS saldırıları sırasında ve sonrasında uygulanacak müdahale ve kurtarma planlarının geliştirilmesi için öneriler sunar. Uygulanacak planlar, sistemlerin en kısa sürede normale dönmesini sağlayarak iş sürekliliğini garanti altına alır.

Sık Sorulan Sorular

DDoS saldırısı nedir?

DDoS (Distributed Denial of Service) saldırısı, bir sistemin kaynaklarını aşırı yükleyerek hizmet vermesini engellemek amacıyla gerçekleştirilen bir saldırı türüdür.

DDoS ve DoS saldırıları arasındaki fark nedir?

DoS (Denial of Service) saldırıları tek bir kaynaktan gelirken, DDoS saldırıları birden fazla cihaz (botnet) aracılığıyla gerçekleştirilir ve bu nedenle tespit edilmesi ve durdurulması çok zordur.

DDoS saldırısı nasıl önlenir?

Güvenlik duvarları, CDN'ler, yük dengeleyiciler ve trafik filtreleme gibi koruma yöntemleriyle DDoS saldırıları önemli ölçüde önlenebilir.

Bir DDoS saldırısı sırasında ne yapılmalıdır?

Saldırı tespit edilir edilmez trafiği analiz etmek ve zararlı trafiği filtrelemek en önemli kriterdir. Servis sağlayıcıya iletişime geçmek ve güvenlik ekibine bildirimde bulunmak, bu saldırının etkilerini hafifletici ve en önemli unsurlar arasında gelir.

DDoS koruma hizmetleri nasıl çalışır?

Anormal trafik akışlarını tespit edilerek filtreleme ve engelleme sistemleri devreye girer ve sistemlerin aşırı yüklenmesini önler.

DDoS saldırıları hangi katmanları hedefler?

DDoS saldırıları, OSI modelinin farklı katmanlarında gerçekleşebilir. En yaygın olanları ağ (Layer 3), taşıma (Layer 4) ve uygulama (Layer 7) katmanlarıdır.

DNS Amplifikasyon saldırısı nedir?

DNS Amplifikasyon, saldırganın küçük bir sorgu gönderip çok büyük bir yanıt almasını sağlayarak hedef sunucuya bu yanıtları yönlendirdiği bir saldırı türüdür. Bu saldırılar, sistemin bant genişliğini büyük bir hızla tüketir.

DDoS koruması için ücretsiz çözümler var mı?

Bazı hizmet sağlayıcılar (AWS Shield Standard gibi) temel DDoS korumasını ücretsiz sunar. Ancak daha gelişmiş koruma için genellikle ücretli çözümler kullanılır.

DDoS saldırıları işletmeler için neden tehlikelidir?

DDoS saldırıları, hizmetlerin kesintiye uğramasına ve müşteri memnuniyetinin azalmasına yol açar. Kritik altyapı sunan finans ve enerji gibi sektörlerde en ufak bir kesinti büyük maliyetlere yol açabilir.

DDoS saldırıları ne kadar sürer?

DDoS saldırının süresi değişkendir. Bazı saldırılar birkaç dakika sürebilirken, bazı saldırılar saatler hatta günlerce devam edebilir. İyi bir koruma altyapısı, bu saldırıların etkilerini hızla hafifletir ve en az zararla atlatılmasını sağlar.

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