Privia SECURITY

Donanım Sızma Testi Hizmeti

Profesyonel Offensive Security Hizmetleri

"Firmware'den Çipe, Her Katmanda Güvenlik!"

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

+90 (216) 514 72 14

www.priviasecurity.com

"Donanım sızma testi, donanımların tüm bileşenlerinde (çip, arka kapı, firmware ve devre) yetkisiz erişim ve manipülasyona karşı açıkları ortaya çıkararak güvenlik risklerini minimize eder."

Donanım sızma testi, fiziksel donanımların güvenlik zafiyetlerini ortaya çıkarmak amacıyla gerçekleştirilen kapsamlı bir test sürecidir. Donanım Sızma Testi; EKS (SCADA), IT, IoT donanımlarından ağ ekipmanlarına, gömülü sistemlerden kritik altyapı donanımlarına kadar geniş bir yelpazeyi kapsar. Test sırasında donanımın portları, çipleri, veri yolları, gömülü işletim sistemi ve firmware katmanları incelenerek hem yetkisiz erişim hem de veri manipülasyonu gibi riskler tespit edilir.

Fiziksel tehditlerin artan önemi, yalnızca yazılım değil, donanım katmanında da güçlü bir güvenlik gerektirir. Donanım Sızma testiyle, donanımların PCB devreleri, bağlantı noktaları, olası arkakapılar ve donanım tabanlı kimlik doğrulama mekanizmaları saldırgan bakış açısıyla analiz edilir. Side-Channel saldırıları, Sahtecilik (Tampering/Forgery) ve tersine mühendislik (Reverse Engineering) teknikleriyle uluslararası standartlara uygun denetimler gerçekleştirilir. Özellikle firmware güvenliği üzerinde yoğunlaşarak güncellenebilirlik ve bütünlük gibi kritik unsurlar da gözden geçirilir.

Bu kapsamlı hizmet sayesinde, şirketler ve kuruluşlar (kolluk kuvvetleri, kritik altyapılara sahip kamu ve özel şirketler) donanımlarının dayanıklılığını artırarak olası tehditlere karşı hazırlıklı olur. Donanım sızma testi, zafiyetleri önceden tespit ederek, güvenlik açıklarının giderilmesini ve yasal düzenlemelere uyum sağlanmasını mümkün kılar. Böylece, güçlü savunma stratejileri geliştirilerek altyapı güvenliği ve sistem sürekliliği sağlanır.

Hizmete Ait Bileşenler

Fiziksel İnceleme ve Manipülasyon Testleri

Bu evrede donanımın dış gövdesi, bağlantı noktaları ve iç bileşenleri detaylı şekilde analiz edilir. Etiketler, mühürler veya fiziksel koruma önlemlerinin manipüle edilip edilmediği tespit edilir. Sahte donanım parçalarının eklenmesi, kablo girişlerine müdahale gibi tehditler incelenerek, donanımın fiziksel bütünlüğü değerlendirilir.

Port ve Bağlantı Noktaları Güvenliği Testleri

USB, Ethernet, JTAG, UART ve SPI gibi bağlantı noktaları üzerinden yetkisiz erişim veya Exfiltration (Veri Çıkışı/Sızdırılması) girişimleri test edilir. Açık portlar ve gereksiz servislerin varlığı kontrol edilerek saldırganların bu yolları kullanarak sisteme erişip erişemeyecekleri incelenir. Donanımın dışa açılan bağlantı noktalarının yapılandırma hataları belirlenir ve güvenlik açıkları ortaya çıkarılır.

Firmware Analizi ve Tersine Mühendislik

Bu evrede donanımın firmware yazılımı incelenir ve sahte güncellemelerin yüklenip yüklenemeyeceği test edilir. Firmware'de arka kapı (backdoor) veya zararlı kod bulunup bulunmadığı analiz edilir. Tersine mühendislik teknikleri kullanılarak iç yazılımdaki hassas verilerin (şifreler, anahtarlar) sızdırılabilirliği değerlendirilir. Ayrıca güncelleme mekanizmasının güvenliği incelenir ve veri bütünlüğünün korunması sağlanır.

Side-Channel Analizi ve Elektromanyetik Testler

Donanımın güç tüketimi, zamanlama farkları ve elektromanyetik yayılımları analiz edilerek Side-Channel saldırılarına karşı dayanıklılığı test edilir. Bu tür saldırılar, donanımın fiziksel performansına yönelik ipuçları kullanılarak şifreleme anahtarları veya hassas bilgiler elde etmeye yöneliktir. Yapılan çalışmalarla, Side-Channel saldırılarıyla ele geçirilebilecek bilgilerin güvenliği sağlanır.

Kimlik Doğrulama ve Güvenlik Mekanizmalarının Testleri

Donanım üzerinde kullanılan güvenlik teknolojileri, kimlik doğrulama süreçleri, kimlik saklama yöntemleri ve koruma mekanizmaları incelenir. Secure boot, TPM ve biyometrik doğrulama sistemlerinin güvenilirliği test edilir. Ayrıca donanımın sahteciliğe karşı algılama sistemleri ve fiziksel bütünlük koruma önlemleri değerlendirilir. Tüm bu kontroller, donanımın yetkisiz erişime karşı ne kadar dirençli olduğunu tespit etmek amacıyla gerçekleştirilir.

Sık Sorulan Sorular

Donanım sızma testi nedir?

Donanım sızma testi, donanımların fiziksel ve dijital bileşenlerinde güvenlik açıklarını tespit etmek için yapılan bir güvenlik denetimidir. Bağlantı noktaları, firmware ve Side-Channel saldırılarına karşı donanımların mevcut durumunun ortaya çıkarıldığı test yöntemidir.

Neden donanım sızma testi yaptırılmalı?

Potansiyel saldırıları donanım seviyesinde tespit ederek veri sızıntılarını, arka kapı risklerini ve sistem aksaklıklarını önler. Donanım sızma testleri özellikle askeri sistemler, kritik altyapılar, silah sistemleri, savunma alt yapıları, elektrik üretim tesisleri, doğalgaz arama donanımları gibi bir çok farklı alanda gerçekleştirilerek, ulusal güvenliğin sağlanması noktasında önemli bir hizmettir.

Donanım sızma testinde hangi araçlar kullanılır?

Donanım sızma testlerinde kullanılan araçlar, hem yazılım hem de donanım katmanında geniş bir yelpazeye yayılır. Ağ analiz araçları olarak Wireshark ve tcpdump, veri trafiğini izleyerek donanımların hangi protokollerle çalıştığını, açık portların varlığını ve şüpheli ağ aktivitelerini tespit etmek için kullanılır. Aynı zamanda, THC Hydra gibi araçlar, donanımların kimlik doğrulama sistemlerini kırmak için kullanılabilir.

Fiziksel arayüz testlerinde JTAG ve UART analizörleri, donanım bileşenlerine doğrudan erişim sağlayarak donanımın iç yapısının debug edilmesine ve arka kapıların tespit edilmesine olanak tanır. Side-Channel saldırılarının analizinde ise osiloskoplar ve elektromanyetik alan ölçüm donanımları kullanılarak, güç tüketimi ve sinyal yayılımları incelenir. Firmware analizinde ise Binwalk ve Ghidra gibi araçlar kullanılarak, donanımın iç yazılımının tersine mühendislik yöntemiyle analiz edilmesi sağlanır.

Donanım sızma testi ne kadar sürer?

Testin süresi, donanımın karmaşıklığına ve kapsamına bağlı olarak değişir. Genellikle birkaç gün ile birkaç hafta arasında süren bu süreç, keşif, test ve raporlama aşamalarını içerir.

Hangi tür donanımlar için sızma testi gereklidir?

IT, OT ve IoT donanımları, ağ donanımları, akıllı kartlar, endüstriyel kontrol sistemleri ve gömülü sistemler gibi kritik altyapıya sahip donanımlar, sızma testine tabi tutulmalıdır.

Sızma testi raporu neleri içerir?

Raporlar, tespit edilen güvenlik açıklarının detaylarını, potansiyel etkilerini ve çözüm önerilerini içerir. Ayrıca, donanımın hangi bileşenlerinde güvenlik zafiyeti bulunduğu ve alınması gereken önlemleri açıklar.

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