Privia SECURITY

Siber Risk Analizi Hizmeti

Profesyonel Defensive Security Hizmetleri

"Riski Belirleyin, Uzun Vadeli Stratejiler Kurun!"

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

+90 (216) 514 72 14

www.priviasecurity.com

"Risk belirleme süreci, organizasyonun tehditlere karşı uzun vadeli ve sürdürülebilir bir güvenlik stratejisi geliştirmesine olanak tanır. Stratejiler, güvenlik önlemlerinin uygun bir şekilde planlanmasını ve işletilmesini sağlar."

Siber Risk Analizi Hizmeti, organizasyonların dijital/endüstriyel varlıklarını güvence altına almak için hazırladığımız kapsamlı bir süreçtin. Hizmetin temel amacı, organizasyonun sahip olduğu varlıkları tehdit eden olası güvenlik zafiyetlerini belirlemek, değerlendirmek ve uygun risk yönetim stratejileri geliştirmektir. ISO 27001, NIST SP 800-30 ve PCI-DSS gibi güvenlik standartlarına dayanan bu analiz, varlık envanteri çıkararak değerleme, tehdit analizi, zafiyet tespiti, risk değerlendirmesi ve risk azaltma gibi kritik aşamaları içerir. Risk analizi sürecinde, organizasyonun mevcut güvenlik önlemleri, IT, OT ve IoT altyapısının etkinliği gözden geçirilir. Zafiyetlerin belirlenerek giderilmesi için kapsamlı bir eylem planı hazırlanır.

Analiz süreci, organizasyonların güvenlik zafiyetlerini anlama ve uygun önlemler alma yeteneklerini geliştirir. Mevcut sistemlerin değerlendirilmesi için yapılan denetimlerde, güvenlik protokolleri, kontroller gözden geçirilir ve risk skoru hesaplanır. Organizasyonun risk skoru, belirlenen güvenlik önlemlerinin etkinliğini ve gereksinim duyulan iyileştirme alanlarını yansıtır. Çalışmanın ilk adımı olan sızma testleriyle, altyapının o anlık siber güvenlik fotoğrafı çekilir. Siber Risk Analizi, organizasyonun güvenlik zafiyetlerine yönelik etkin bir çözüm sunar. Analiz sürecinde elde edilen veriler, detaylı raporlar ve öneriler ile birleştirilerek, güvenlik stratejilerinin uygulanabilir hale getirilmesi sağlanır. Siber güvenlik uzmanları tarafından hazırlanan raporlar, yönetim ve teknik ekipler için yol gösterici bir rehber işlevi görür. Riskler, olasılık ve etki bazında sınıflandırarak organizasyonun hangi önlemleri öncelikli olarak alması gerektiğini belirler.

Ayrıca yapılan analizler sayesinde Güvenlik Teknolojileri ve Çözümleri, Ağ Altyapısı, Etki Alanı ve Hesap Yönetimi gibi güvenlik bileşenleri üzerinde detaylı kontroller gerçekleştirilir. Siber risk analizi, teknolojik altyapının sürekli iyileştirilmesi ve güncellenmesi için organizasyonlara rehberlik eder. Belirlenen güvenlik önlemleri, organizasyonun mevcut güvenlik politikalarıyla uyumlu hale getirilir ve her bir varlık için özel koruma stratejileri geliştirilir. Analiz süreci, organizasyonun uzun vadeli güvenlik hedeflerine ulaşmasına yardımcı olur ve güvenlik ihlallerinin etkisini minimize eder.

Hizmete Ait Bileşenler

Varlık Envanteri ve Değerleme

Siber Risk Analizi Hizmeti kapsamında öncelikli adım, organizasyonun dijital/endüstriyel varlıklarının envanterini oluşturmaktır. Süreç, her bir varlığın iş sürekliliği ve güvenlik açısından önemini belirlemeyi içerir. Kritik varlıkların tespiti, hangi varlıkların korunmasının öncelikli olduğunu belirlemeye yönelik temel bir adımdır. Envanterde, fiziksel sunuculardan bulut hizmetlerine kadar tüm varlıklar analiz edilir ve bu varlıkların olası bir saldırılara karşı seviyeleri değerlendirilir.

Penetrasyon (Sızma) Testi

Penetrasyon testi, organizasyonun dijital/endüstriyel varlıklarına yönelik olası tehditleri ve bu tehditlerin oluşturabileceği riskleri anlamaya yönelik bir çalışmadır. Çalışma sırasında siber saldırganların kullanabileceği zafiyetler belirlenir ve bu zafiyetlerin hangi varlıkları etkileyebileceği analiz edilir. Tehdit analizi sürecinde, güvenlik zafiyetleri ve tehdit kaynakları detaylı bir şekilde incelenir. Gerçekleştirilen çalışma, organizasyonun güvenlik altyapısının güçlendirilmesi için gereken önlemlerin belirlenmesine yardımcı olur. Zafiyet analizinde kullanılan araçlar ve yöntemlerle, organizasyonun mevcut güvenlik yapısındaki eksiklikler/hatalar tespit edilir.

Siber Güvenlik Durum Tespiti

Siber Güvenlik Durum Tespiti, organizasyonun mevcut güvenlik seviyesini belirlemeyi ve bu seviyeyi sürekli olarak gözden geçirmeyi amaçlar. Gerçekleştirilen çalışma, sistemdeki güvenlik zafiyetlerini ve potansiyel tehditleri ortaya çıkarmak için detaylı bir güvenlik kontrollerini içerir. Elde edilen sonuçlar, organizasyonun siber güvenlik skoru olarak özetlenir ve bu skor, güvenlik yapısının etkinliğini değerlendirmek için bir referans noktası oluşturur. Durum tespiti, aynı zamanda mevcut güvenlik önlemlerinin performansını değerlendirmek için kritik bir adımdır. Bu sayede güvenlik zafiyeti veya teknolojik eksiklikler hızla tespit edilip iyileştirilebilir.

Risk Değerlendirmesi ve Sınıflandırma

Risk değerlendirmesi, belirlenen tehditlerin gerçekleşme olasılığı ile bu tehditlerin olası etkilerinin değerlendirilmesini kapsar. Değerlendirme, risklerin organizasyonun iş süreçlerine etkilerini anlamak için kritik öneme sahiptir. Riskler, olasılık ve etki bazında Acil, Kritik, Yüksek, Orta veya Düşük olarak sınıflandırılır ve bu sınıflandırma güvenlik önlemlerinin önceliklendirilmesini sağlar. Risk değerlendirmesi ayrıca, organizasyonun stratejik hedefleri doğrultusunda güvenlik önlemlerinin uygunluğunu değerlendirir.

Siber Güvenlik Acil Eylem Planı

Siber Güvenlik Acil Eylem Planı, organizasyonun karşılaşabileceği acil durumlara hazırlıklı olmasını sağlamak için oluşturulan bir stratejik plandır. Acil Eylem Planı, olası güvenlik ihlalleri ve saldırılara karşı atılması gereken adımları detaylandırır. Eylem planı, acil durum senaryolarını içermekte olup, belirli bir zaman çizelgesine göre yürütülür ve her adımda gerekli güvenlik tedbirlerinin alınmasını önerir. Plan kapsamında, organizasyonun mevcut altyapısı gözden geçirilir ve iyileştirme gerektiren alanlar belirlenir. Ayrıca izleme ve alarm sistemlerinin etkinliği değerlendirilir ve gerekli durumlarda bu sistemlerde iyileştirmeler yapılır.

Raporlama

Siber güvenlik risk yönetiminin etkinliği, güvenlik altyapısının sürekli olarak izlenmesi ve periyodik raporlama yapılması ile sağlanır. İzleme süreci, anormal aktiviteleri hızlıca tespit etmek ve güvenlik tehditlerine anında müdahale etmek için kritik bir adımdır. Güvenlik olaylarının logları ve analizleri düzenli olarak gözden geçirilerek sistemdeki olası zafiyetler belirlenir. Raporlama, elde edilen verilerin yönetim ve güvenlik ekipleri ile paylaşılmasını ve gerekli önlemlerin alınmasını sağlar. Süreç, güvenlik politikalarının etkinliğini değerlendirmek ve iyileştirmek için bir geri bildirim mekanizması oluşturur.

Sık Sorulan Sorular

Siber Risk Analizi Nedir ve Neden Önemlidir?

Siber Risk Analizi, organizasyonun dijital/endüstriyel altyapısındaki potansiyel güvenlik zafiyetlerini belirlemek, değerlendirmek ve yönetmek için yapılan kapsamlı bir analiz sürecidir. Siber risk analizi, organizasyonların güvenlik politikalarını güçlendirmesine ve hassas verilerini korumasına katkıda bulunur. Uluslararası güvenlik standartları doğrultusunda yapılan analizler, organizasyonların yasal uyumluluğunu sağlamalarına yardımcı olur.

Siber Risk Analizi Nasıl Yapılır?

Siber Risk Analizi, Sızma Testi, Risk Değerlendirme ve Siber Güvenlik Acil Eylem Planı ve raporlama gibi adımlardan oluşur. İlk adımda, organizasyonun dijital varlıkları detaylı bir şekilde sızma testine tabi tutulur ve her varlığın değeri analiz edilir. Daha sonra olası tehditler ve zafiyetler belirlenir, bu tehditlerin gerçekleşme olasılığı ve etkileri analiz edilir. Risklerin sınıflandırılması aşamasında, en kritik riskler öncelikli olarak değerlendirilir ve uygun güvenlik önlemleri önerilir. Ayrıca Acil Eylem Planı oluşturularak mevcut durum ve teknolojik altyapıya yönelik iyileştirme önerileri sunulur. Son olarak, elde edilen veriler detaylı bir raporla yönetimle paylaşılır.

Risk Değerlendirmesi Neden Önemlidir?

Risk değerlendirmesi, organizasyonun güvenlik önlemlerini önceliklendirmesine yardımcı olarak kaynakları verimli kullanmasını sağlar. Riskler olasılık ve etki seviyesine göre sınıflandırılır, bu sayede kritik riskler öncelikli olarak ele alınır. Risk değerlendirmesi, tehditlerin etkilerini minimize etmek ve güvenlik politikalarını optimize etmek için temel bir adımdır. Bu süreç aynı zamanda, güvenlik yatırımlarının en etkin şekilde kullanılmasına olanak tanır. İş süreçlerinin güvenliğini sağlamak ve operasyonel kesintileri önlemek açısından da büyük önem taşır.

Varlık Envanteri ve Değerleme Neden Yapılır?

Varlık envanteri ve değerleme, organizasyonun sahip olduğu tüm dijital/endüstriyel varlıkların önem derecesini belirlemeyi sağlar. Bu adım, hangi varlıkların korunması gerektiğini ve hangi varlıklara öncelik verilmesi gerektiğini anlamak için önemlidir. Kritik varlıkların belirlenmesi, organizasyonun güvenlik stratejilerini doğru bir şekilde yönlendirmesine yardımcı olur. Değerleme süreci, saldırılardan en çok etkilenebilecek varlıkları ortaya koyar ve bu varlıklar için özel güvenlik önlemleri geliştirilir. Organizasyon, değerli varlıklarını koruyarak veri kaybı veya iş kesintisi gibi riskleri minimize eder.

Siber Güvenlik Acil Eylem Planı Nedir?

Siber Güvenlik Acil Eylem Planı, olası güvenlik ihlalleri ve acil durumlara hazırlıklı olmayı sağlayan stratejik bir plandır. Plan, organizasyonun güvenlik olaylarına hızlı ve etkin bir şekilde yanıt verebilmesi için gerekli adımları belirler. Acil eylem planı, belirli

senaryolar dahilinde alınması gereken önlemleri ve uygulanması gereken prosedürleri içerir. Olası güvenlik ihlalleri durumunda, organizasyonun iş sürekliliğini sağlamak ve veri kaybını önlemek için anında müdahale edilir.

Siber Güvenlik Durum Tespiti Nedir?

Siber Güvenlik Durum Tespiti, organizasyonun mevcut güvenlik duruşunu analiz etmek ve güvenlik seviyesini belirlemek için yapılan bir çalışmadır. Gerçekleştirilen çalışma, organizasyonun sistemlerindeki güvenlik zafiyetlerini belirleyerek, güvenlik yapısının etkinliğini değerlendirir. Durum tespiti, güvenlik skorunun belirlenmesine olanak tanır ve organizasyonun güvenlik stratejilerini iyileştirmesine yönelik rehberlik sağlar. Bu analiz sırasında elde edilen bulgular, güvenlik zafiyetlerini hızlı bir şekilde gidermek için kullanılan bir temel oluşturur.

Penetrasyon Testi (Sızma Testi) Nedir?

Penetrasyon testi, organizasyonun dijital/endüstriyel altyapısına yönelik saldırı simülasyonları yaparak güvenlik zafiyetlerini tespit etmeye yönelik gerçekleştirilen bir güvenlik değerlendirmesidir. Test sırasında siber güvenlik uzmanları, gerçek saldırganların kullanabileceği yöntemleri deneyerek güvenlik zafiyetlerini keşfeder. Penetrasyon testleri, güvenlik zafiyetlerinin hızlı bir şekilde belirlenmesine ve giderilmesine yardımcı olur. Test sonuçları, güvenlik önlemlerinin yeterliliğini değerlendirmek ve iyileştirmek için önemli bir geri bildirim sağlar. Sızma Testi, özellikle yeni güvenlik çözümleri uygulandıktan sonra güvenlik altyapısının etkinliğini doğrulamak için de sıklıkla tercih edilir.

Siber Risk Analizi Hangi Sıklıkla Yapılmalıdır?

Siber Risk Analizi, organizasyonun güvenlik ihtiyaçlarına ve sektörel risk düzeyine göre düzenli olarak yapılması gereken bir süreçtir. Özellikle teknolojik altyapıda yapılan büyük değişiklikler veya yeni güvenlik önlemleri sonrası analizlerin tekrar yapılması önerilir. Yıllık veya altı ayda bir gerçekleştirilen analizler, organizasyonun güvenlik durumunun güncel kalmasını sağlar. Risk analizi, organizasyonun karşılaşabileceği yeni tehditlere göre sürekli güncellenmesi gereken dinamik bir süreçtir.

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