Privia SECURITY

Sosyal Mühendislik Hizmeti

Profesyonel Offensive Security Hizmetleri

"Çalışanlara Yönelik Tehditleri Simüle Edin!"

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

+90 (216) 514 72 14

www.priviasecurity.com

"Çalışanların siber tehditlere karşı hazırlıklı olmalarını sağlar ve organizasyon içindeki güvenlik bilincini artırır."

Sosyal mühendislik hizmetimiz, çalışanlarınızı hedef alan tehditleri simüle ederek, organizasyonunuzun zayıf noktalarını ortaya çıkarmayı amaçlar. Sosyal Mühendislik hizmeti, insan faktörünün siber güvenlikteki rolünü vurgulamak için kritik bir öneme sahiptir. Gerçekçi senaryolar aracılığıyla, çalışanlarınızın bilgi güvenliği farkındalığını arttırır.

Simülasyonlar, oltalama e-postaları, telefon dolandırıcılığı ve diğer sosyal mühendislik tekniklerini içerecek şekilde tasarlanır. Çalışanlar, bu tür saldırılara karşı nasıl bir tepki vereceklerini deneyimleyerek, bu tehditlere karşı daha hazırlıklı hale gelir. Elde edilen veriler, zayıf noktaların belirlenmesi ve güvenlik eğitimlerinin geliştirilmesi için kullanılır.

Sosyal mühendislik hizmetimiz, sadece zayıflıkları tespit etmekle kalmaz, aynı zamanda organizasyon içinde güvenlik bilincini artırmayı hedefler. Çalışanlar, simülasyonlar sayesinde saldırganların yöntemlerini öğrenir ve bu bilgilerle kişisel güvenliklerini sağlama konusunda daha donanımlı hale gelir. Böylece, organizasyonunuzun siber güvenlik durumu önemli ölçüde güçlendirilmiş olur.

Hizmete Ait Bileşenler

Tehdit Simülasyonları

Tehdit simülasyonları, çalışanlara yönelik potansiyel sosyal mühendislik saldırılarını gerçekçi bir şekilde deneyimleme fırsatı sunar. Bu simülasyonlar, oltalama e-postaları, sahte telefon aramaları ve fiziksel sosyal mühendislik tekniklerini içerir. Çalışanlar, bu tür tehditlere nasıl tepki vereceklerini öğrenerek, potansiyel saldırılara karşı daha hazırlıklı hale gelir.

Farkındalık Eğitimi

Farkındalık eğitimi, çalışanların bilgi güvenliği konusunda bilinçlenmesini sağlamak için kritik bir bileşendir. Eğitim programları, sosyal mühendislik saldırılarının tanınması ve bu saldırılardan korunma yöntemlerini kapsar. Çalışanlar, olası tehditleri tanıyarak, organizasyonun genel güvenliğine katkıda bulunur.

Zayıf Nokta Analizi

Zayıf nokta analizi, gerçekleştirilen simülasyonlar ve eğitimler sonrasında elde edilen verilerin değerlendirilmesiyle yapılır. Yapılan analiz, organizasyonun güvenlik politikalarının ve uygulamalarının ne kadar etkili olduğunu belirler. Tespit edilen zayıf noktalar, güvenlik önlemlerinin iyileştirilmesi için gerekli adımları atmak üzere birçok girdi sağlar.

Raporlama ve Geri Bildirim

Raporlama ve geri bildirim, sosyal mühendislik hizmetinin önemli bir parçasıdır. Gerçekleştirilen simülasyonların sonuçları, ayrıntılı raporlar halinde sunularak, yönetim ve güvenlik ekipleriyle paylaşılır. Sunulan raporlar, zayıf noktaların yanı sıra, güvenlik stratejilerini geliştirmek için öneriler de içerir.

Periyodik Sosyal Mühendislik

Çalışanların siber güvenlik konusundaki farkındalığını artırmak amacıyla düzenli olarak gerçekleştirilen simülasyon ve eğitim süreçlerini içerir. Çalışanların potansiyel sosyal mühendislik saldırılarına karşı sürekli olarak bilinçli kalmasını sağlar ve organizasyonun güvenlik kültürünü güçlendirir. Periyodik olarak yapılan simülasyonlar, zamanla değişen tehdit ortamına uyum sağlamak için güncellenir ve böylece çalışanlar her yeni saldırı tekniği hakkında bilgi sahibi olur.

Sık Sorulan Sorular

Sosyal mühendislik nedir?

Sosyal mühendislik, manipülasyon yöntemleri kullanarak, gizli bilgilere erişmeyi amaçlayan bir tekniktir. Genellikle bilgi güvenliği zafiyetlerinden yararlanarak, hedef kişilerin dikkatini dağıtma veya güvenini kazanma yoluyla gerçekleştirilen saldırılara verilen isimdir.

Sosyal mühendislik saldırıları nasıl gerçekleştirilir?

Sosyal mühendislik saldırıları, genellikle oltalama e-postaları, sahte telefon aramaları ve yüz yüze etkileşimler aracılığıyla yapılır. Saldırganlar, kurbanın güvenini kazanarak kişisel bilgileri veya erişim bilgileri gibi kritik verileri elde etmeye çalışır.

Sosyal mühendislik saldırılarından nasıl korunabilirim?

Çalışanların sosyal mühendislik konusunda eğitilmesi, bu tür saldırılara karşı en etkili korunma yöntemidir. Ayrıca, dikkatli olmak, şüpheli iletileri kontrol etmek ve güvenlik protokollerini takip etmek de önemlidir.

Sosyal mühendislik hizmetleri neleri içerir?

Sosyal mühendislik hizmetleri, tehdit simülasyonları, farkındalık eğitimi, zayıf nokta analizi ve raporlama gibi bileşenleri içerir. Sağlanan hizmet, organizasyonun güvenlik durumunu değerlendirmeye ve zayıf halkayı güçlendirmeye yardımcı olur.

Sosyal mühendislik saldırılarının en yaygın türleri nelerdir?

En yaygın sosyal mühendislik saldırı türleri arasında oltalama (phishing), telefon dolandırıcılığı (vishing) ve önceden planlanmış fiziksel erişim (pretexting) yer alır. Her biri, hedef bireyleri manipüle ederek gizli bilgiyi elde etmeyi amaçlar.

Sosyal mühendislik hizmeti almanın avantajları nelerdir?

Sosyal mühendislik hizmeti almak, çalışanların güvenlik farkındalığını artırır, zayıf noktaları belirler ve organizasyonun uzun vadeli genel güvenlik stratejilerini güçlendirir. Ayrıca, yasal düzenlemelere uyumu artırır ve olası veri ihlallerinin önlenmesine yardımcı olur.

Bir sosyal mühendislik saldırısına maruz kalındığını nasıl anlarım?

Bir sosyal mühendislik saldırısına maruz kaldığınızı anlamanın belirtileri arasında şüpheli e-postalar, beklenmedik istekler veya kimlik doğrulama bildirimleri yer alabilir. Ayrıca, herhangi bir iletişimde güvensizlik hissi veya beklenmedik davranışlar da bu durumu işaret edebilir.

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