Privia SECURITY

Acil Eylem Planı Hizmeti

Profesyonel Defensive Security Hizmetleri

"Siber Krizler Yaşanmadan, Eylem Planınızı Oluşturun!"

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

+90 (216) 514 72 14

www.priviasecurity.com

"Güçlü bir eylem planı, organizasyonların olası siber saldırılara ve veri ihlallerine karşı güvenli kalmasını sağlar. Kriz anında hızlı karar alabilmek ancak önceden planlanan bir eylem süreciyle mümkündür."

Acil Eylem Planı Hizmeti, organizasyonların siber tehditlere karşı hazırlıklı olmalarını sağlayan bir güvenlik stratejisidir. Saldırıya uğrama durumunda hızlı müdahale için gerekli olan prosedürleri, sorumlulukları ve eylemleri belirler. Güvenlik ihlalleri sırasında, organizasyonların veri kaybı yaşamaması ve itibarını koruması için tasarlanmış bu plan, olası tüm tehdit senaryolarını dikkate alır. Organize ve sistematik bir şekilde oluşturulan acil eylem planları, organizasyonun güvenlik ekibinin hızla harekete geçmesine olanak tanır. Bu hizmet, güvenlik önlemlerini optimize ederek organizasyonun risklere karşı direncini güçlendirir.

Acil Eylem Planı Hizmeti, güvenlik ekiplerine kriz anında uygulayacakları kapsamlı bir yol haritası sunar. Olası bir saldırı sırasında hızlı ve etkili bir yanıt verilmesi için gerekli olan kaynakları belirler ve bu kaynakların nasıl yönetileceğini tanımlar. Çeşitli tehdit senaryoları üzerinde yapılan çalışmalar, eylem planının doğruluğunu ve etkinliğini artırır. Eylem planları, organizasyonun siber güvenlik altyapısının güçlü kalmasına yardımcı olur. Bu hizmet sayesinde organizasyon, siber tehditler karşısında kayıplarını minimize eder ve siber dayanıklılığını artırır.

Acil eylem planı oluşturulurken, organizasyonun ihtiyaçlarına göre özelleştirilmiş bir yaklaşım benimsenir. Bu süreçte güvenlik zafiyetleri değerlendirilir, mevcut güvenlik politikaları gözden geçirilir ve tüm güvenlik unsurları stratejik olarak planlanır. Güvenlik önlemlerinin yerinde olması, organizasyonun olası saldırılara karşı daha hazırlıklı olmasını sağlar. Ayrıca, eylem planı düzenli olarak güncellenir ve değişen tehdit ortamına göre uyarlanır. Böylece organizasyon, güvenlik ihlalleri karşısında daima güncel bir koruma seviyesine ulaşır.

Bu hizmet, organizasyonun iç iletişim yapısını düzenleyerek kriz anında hızlı karar alınmasını kolaylaştırır. Eylem planı doğrultusunda belirlenen sorumluluk alanları, kriz anında koordinasyonu sağlar. Güvenlik ihlalinin boyutuna bağlı olarak farklı departmanlar arasında etkin bir iletişim ağı kurulur. Bu, organizasyonun operasyonel sürekliliğini korumasına yardımcı olur. Aynı zamanda, organizasyonun müşteri ve iş ortaklarına karşı güvenilirliğini korur.

Acil Eylem Planı Hizmeti, siber güvenlik risklerini minimuma indirirken organizasyonun iş sürekliliği hedeflerini destekler. Organizasyonun tüm katmanlarında uygulanabilir güvenlik önlemleri sunar ve güvenlik stratejilerini sürdürülebilir kılar. Bu hizmet, organizasyonun siber tehditlere karşı önceden hazırlıklı olmasını ve uzun vadeli güvenlik stratejilerini güçlendirmesini sağlar. İş sürekliliğini desteklemek için güvenlik önlemlerini optimize eden bu plan, güvenliğinizi her açıdan güçlendirir. Güçlü bir eylem planı, organizasyonun siber saldırılara karşı hazırlıklı ve dayanıklı kalmasına olanak tanır.

Hizmete Ait Bileşenler

Varlık Envanteri ve Değerleme

Siber Risk Analizi Hizmetinin ilk aşamasında, organizasyonun sahip olduğu dijital ve endüstriyel varlıkların kapsamlı bir envanteri çıkarılır. Bu adımda, her bir varlığın iş sürekliliği ve güvenlik açısından taşıdığı önem belirlenir. Kritik varlıkların tanımlanması, hangi unsurların korunmasının öncelikli olduğunu anlamak açısından temel teşkil eder. Fiziksel sunuculardan bulut hizmetlerine kadar tüm varlıklar detaylı olarak incelenir ve bu varlıkların saldırılara karşı direnci değerlendirilir.

Penetrasyon (Sızma) Testi

Penetrasyon testi, organizasyonların dijital ya da endüstriyel varlıklarına yönelik mevcut tehditlerin tespit edilmesi ve bu tehditlerin yaratabileceği potansiyel risklerin anlaşılması amacıyla yürütülen bir siber güvenlik çalışmasıdır. Penetrasyon testi sürecinde, siber saldırganların kullanabileceği güvenlik zafiyetleri belirlenir ve hangi varlıkların bu zafiyetlerden etkilenebileceği tespit edilir. Tehdit değerlendirme aşamasında, güvenlik açıkları ve tehdit kaynakları detaylı bir incelemeye tabi tutulur. Yapılan analizler, organizasyonun güvenlik altyapısını güçlendirmek için alınması gereken tedbirlerin belirlenmesine katkı sağlar. Zafiyet analizi sırasında kullanılan araçlar ve yöntemler, organizasyonun mevcut güvenlik yapısındaki eksiklikleri ve potansiyel riskleri tespit etmek üzere özel olarak yapılandırılmaktadır.

Siber Güvenlik Durum Tespiti

Siber Güvenlik Durum Tespiti, organizasyonun mevcut güvenlik seviyesini belirlemeyi ve bu seviyeyi değerlendirmeyi hedefleyen bir çalışmadır. Siber Güvenlik Ekibimiz, sistem genelinde detaylı güvenlik kontrolleri yaparak güvenlik zafiyetlerini ve potansiyel tehditleri belirler. Elde edilen sonuçlar, organizasyonun siber güvenlik durumunu gösteren bir güvenlik skoru ile özetlenir ve bu skor, güvenlik yapısının etkinliğini değerlendirmede referans noktası olarak kullanılır. Durum tespiti, aynı zamanda mevcut güvenlik önlemlerinin işlevselliğini değerlendirmek için de büyük önem taşır. Siber Güvenlik Durum Tespiti Hizmetimiz sayesinde olası güvenlik zafiyetleri veya teknolojik eksiklikler hızlıca tespit edilip iyileştirilebilir.

Risk İzleme

Güvenlik ihlali durumunda tüm risklerin ve olayların izlenmesi ve raporlanması, acil eylem planının temel unsurlarından biridir. İzleme süreci, güvenlik ekiplerinin olaylara hızlı yanıt vermesini ve olayın etkilerini değerlendirmesini sağlar. Güvenlik olaylarının raporlanması, eylem planının etkinliğini artırmak için yapılan analizlerde kritik veriler sunar. Raporlama süreci, organizasyonun güvenlik durumunu analiz etmek ve iyileştirmek için yol gösterici bilgiler sağlar. İzleme ve raporlama, güvenlik ihlallerine dair detaylı veriler sunarak gelecek stratejilerin belirlenmesine katkıda bulunur.

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.

Düzenli Test ve Tatbikatlar

Acil eylem planının etkinliğini sağlamak için düzenli olarak testler ve tatbikatlar gerçekleştirilir. Bu tatbikatlar, güvenlik ekibinin kriz anında nasıl hareket edeceğini anlamasına yardımcı olur ve gerekli yetkinlikleri kazandırır. Tatbikatlar, güvenlik ekipleri arasındaki koordinasyonu güçlendirir ve eylem planının etkinliğini ölçümler. Düzenli testler, planın eksik yönlerinin tespit edilmesini ve gerekli güncellemelerin yapılmasını sağlar. Organizasyonun olası bir güvenlik ihlali durumunda hazırlıklı kalmasına katkıda bulunur.

Sık Sorulan Sorular

Siber Güvenlik Acil Eylem Planı neden gereklidir?

Siber Güvenlik Acil Eylem Planı, bir organizasyonun olası siber saldırılara karşı hazırlıklı olmasını sağlar. Eylem planı, güvenlik ihlalleri durumunda operasyonel aksaklıkları minimuma indirmek için kritik öneme sahiptir. Veri ihlallerinin hızlıca yönetilmesi ve veri kayıplarının önlenmesi açısından da önemli bir araçtır. Siber tehditlerin giderek daha karmaşık hale gelmesi, hızlı ve etkili bir müdahale gerektirir. Acil eylem planı, olay yönetiminde koordinasyonu sağlayarak zararları en aza indirir.

Acil eylem planı hazırlarken hangi siber tehditler göz önünde bulundurulmalıdır?

Acil eylem planı hazırlanırken, öncelikle organizasyonun karşılaşabileceği olası tehditler analiz edilmelidir. Kimlik avı, fidye yazılımları, DDoS saldırıları, iç tehditler gibi siber saldırı türleri dikkate alınmalıdır. Ayrıca güvenlik zafiyetleri ve yapılabilecek saldırılar öncelikli olarak göz önünde bulundurulmalıdır. Bulut sistemleri, IoT cihazları gibi daha geniş bir teknoloji ekosistemine sahip organizasyonlarda bu tehditler daha karmaşık hale gelir. Risk değerlendirmesi yapılarak organizasyon için en kritik tehditlerin tanımlanması önemlidir.

Bir siber güvenlik acil eylem planında hangi adımlar bulunmalıdır?

Bir siber güvenlik acil eylem planı, her aşamada detaylı ve kapsamlı adımlara sahip olmalıdır. İlk adımda, potansiyel risklerin analiz edilmesi ve hangi olayların acil durum olarak kabul edileceği belirlenir. Ardından olay tespiti için izleme mekanizmaları devreye alınır ve belirlenen tehditler için müdahale prosedürleri geliştirilir. İletişim adımı da planın önemli bir bileşenidir. Kriz durumunda iç ve dış paydaşlarla hızlı ve doğru bilgi paylaşımını sağlar. Hasar kontrol adımı, saldırının etkilerini minimize etmeye yönelik aksiyonları içerir. Toparlanma süreci, olay sonrası sistemlerin hızlı bir şekilde normale döndürülmesini kapsar. Düzenli tatbikatlarla planın işlevselliği test edilir.

Olası bir siber saldırı durumunda kimler bilgilendirilmeli ve nasıl bir iletişim yolu izlenmelidir?

Olası bir siber saldırı durumunda ilk olarak organizasyonun içindeki ilgili güvenlik ve BT ekipleri bilgilendirilmelidir. Yönetim durumdan haberdar edilmeli ve olaya müdahale süreci hakkında bilgi sahibi olmalıdır. Gerektiğinde yasal düzenleyici kurumlar ve güvenlik ortakları da bilgilendirilir. Bilgi paylaşımı yapılırken gizliliğe önem verilmeli, sadece yetkili kişilerle bilgi paylaşılmalıdır. İletişim protokollerine göre, kriz anında kullanılacak iletişim kanalları ve süreçler önceden belirlenmelidir.

Siber saldırı sırasında alınacak ilk müdahale adımları nelerdir?

Siber saldırı sırasında ilk müdahale adımları, saldırının boyutuna ve türüne göre değişiklik gösterir. Öncelikle saldırı tespit edilir edilmez, etkilenen sistemler izole edilerek yayılma riski kontrol altına alınmalıdır. İkinci adımda, saldırının kaynağını

belirlemek ve hangi verilerin etkilendiğini analiz etmek önemlidir. Sistemlerin logları incelenerek saldırının izleri takip edilir ve saldırının tipi belirlenir. Ayrıca SOME ekibi hızlıca bilgilendirilmeli ve olay müdahale süreci başlatılmalıdır. Toparlama süreci için gerekli adımlar planlanarak sistemlerin normale döndürülmesi sağlanır. Müdahale sürecinin sonunda, olay hakkında kapsamlı bir raporlama yapılır.

Siber Güvenlik Acil Eylem Planı nasıl test edilmeli ve ne sıklıkla güncellenmelidir?

Siber Güvenlik Acil Eylem Planı, düzenli tatbikatlar ve sızma testleriyle değerlendirilmelidir. Planın etkinliği, siber saldırı simülasyonları ve tatbikatlarla ölçülür. Gerçekleştirilen testler, organizasyonun kriz anında nasıl tepki verdiğini anlamak için gerçekleştirilir ve eksiklikler tespit edilir. Elde edilen bulgulara göre, planın güncellenmesi gereken noktalar düzeltilir. Ayrıca güvenlik tehditleri ve teknolojiler sürekli değiştiği için, plan en az yılda bir kez gözden geçirilmelidir. Değişen düzenlemeler veya yeni tehditler göz önünde bulundurularak güncellemeler yapılmalıdır. Tatbikatlar, güvenlik ekipleri arasında koordinasyonu artırarak müdahale sürecini hızlandırır.

Eylem planının etkinliğini sağlamak için çalışanlara ne tür eğitimler verilmelidir?

Eylem planının etkinliği, çalışanların bilgi ve farkındalık düzeyi ile doğrudan ilişkilidir. Çalışanlara siber saldırı senaryolarına karşı nasıl hareket edeceklerini öğreten kapsamlı eğitimler verilmelidir. Kimlik avı gibi yaygın saldırılara karşı farkındalık eğitimleri, güvenlik farkındalığını geliştirme açısından önemlidir. Güvenlik ekiplerine ise teknik eğitimler sunularak acil durumlarda nasıl müdahale edecekleri detaylı bir şekilde anlatılır. Düzenli aralıklarla yapılan tatbikatlar, çalışanların öğrendiklerini uygulayarak pekiştirmelerine olanak tanır.

Eylem planı uygulanırken hangi teknolojiler ve araçlar destekleyici olarak kullanılabilir?

Siber güvenlik acil eylem planı kapsamında SIEM (Güvenlik Bilgi ve Olay Yönetimi) gibi araçlar kullanılarak olaylar gerçek zamanlı olarak izlenebilir. EDR (Uç Nokta Tespiti ve Yanıt) çözümleri, uç noktalardaki şüpheli hareketleri tespit eder ve hızlı müdahale sağlar. Ağ güvenliği cihazları, saldırganların sisteme giriş yollarını engelleyerek koruma sağlar. Güvenlik tehditlerine hızlı yanıt vermek için otomatikleştirilmiş SOAR çözümleri de devreye alınabilir. Ayrıca log yönetimi araçları sayesinde güvenlik ihlallerinin izleri daha hızlı bir şekilde incelenebilir. Siber tehdit istihbaratı platformları, organizasyonun yeni tehditleri takip etmesine ve gerekli önlemleri almasına yardımcı olur. Kriz anında etkili bir koordinasyon sağlamak için iletişim yazılımları kullanılabilir.

Siber Güvenlik Acil Eylem Planı'nın oluşturulması organizasyona nasıl bir maliyet sağlar ve hangi faydaları getirir?

Siber güvenlik acil eylem planı oluşturmanın maliyeti, organizasyonun büyüklüğüne ve mevcut altyapısına göre değişiklik gösterir. Eylem planının hazırlanması, güvenlik uzmanlarının eğitimi ve teknolojik araçların kullanımı gibi faktörlere bağlı olarak bütçelendirilir. Güvenlik ihlali durumunda hızlı müdahale sayesinde olası veri kayıpları

ve iş kesintileri minimum seviyeye indirilir. Planın etkinliği sayesinde, düzenli iş sürekliliği sağlanır. Teknolojik kaynakların verimli kullanılması ile maliyet optimizasyonu yapılır.

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