EMA SECURITY

Güvenlik Sıkılaştırma Hizmeti

AI-Powered Defense Service

İletişim

www.emasecurity.com

info@emasecurity.com

Bostancı Mah, Ali Nihat Tarhan Cd, Kahraman Sk,
No:2/D:11, Hoffman Plaza, Kadıkoy/İstanbul

+90 (850) 244 49 26

Güvenlik Sıkılaştırma Hizmeti

Hizmet Tanımı

Güvenlik Sıkılaştırma Hizmeti, kuruluşların BT altyapılarındaki güvenlik açıklarını en aza indirerek siber tehditlere karşı daha dayanıklı bir yapı oluşturmasını sağlayan kapsamlı bir güvenlik çözümüdür. Günümüzde siber saldırılar giderek daha sofistike hale gelirken, yanlış yapılandırılmış sistemler, eski yazılımlar ve güvenlik açıkları kuruluşları büyük risklerle karşı karşıya bırakmaktadır. Güvenlik sıkılaştırma süreci, organizasyonların mevcut sistemlerini en iyi güvenlik uygulamalarına göre optimize etmelerini sağlayarak, tehdit aktörlerinin saldırı vektörlerini en aza indirir ve sistemlerin dayanıklılığını artırır.

Bu hizmet kapsamında, işletim sistemleri, ağ cihazları, uygulamalar, veri tabanları, bulut altyapıları ve uç noktalar gibi kritik bileşenlerin güvenlik yapılandırmaları detaylı bir şekilde analiz edilir ve uluslararası güvenlik standartlarına uygun olarak sıkılaştırılır. Güvenlik sıkılaştırma süreci, ilk olarak mevcut sistemlerin kapsamlı bir güvenlik değerlendirmesinden geçirilmesiyle başlar. CIS Benchmark, NIST, ISO 27001, PCI-DSS ve diğer güvenlik çerçeveleri baz alınarak sistemlerdeki zayıflıklar belirlenir. Bu değerlendirme sürecinde, gereksiz servislerin tespiti, varsayılan yapılandırmaların riskleri, açık portlar ve kullanılmayan yetkilendirmeler gibi güvenlik tehditleri analiz edilir. Daha sonra, risk analizi yapılarak en kritik güvenlik açıkları önceliklendirilir ve uygun sıkılaştırma politikaları oluşturulur.

Bu süreç, güçlü kimlik doğrulama ve erişim yönetimi politikalarının uygulanmasını, gereksiz servislerin ve zayıf protokollerin devre dışı bırakılmasını, sistem yamalarının ve güvenlik güncellemelerinin düzenli olarak uygulanmasını, veri şifreleme mekanizmalarının güçlendirilmesini ve güvenlik konfigürasyonlarının merkezi olarak yönetilmesini kapsar. Özellikle parola politikalarının sıkılaştırılması, ayrıcalıklı hesap yönetimi (PAM) çözümlerinin entegrasyonu, güvenlik duvarı ve ağ erişim kontrollerinin iyileştirilmesi gibi önlemler ile organizasyonların güvenlik duruşu önemli ölçüde güçlendirilir. Ayrıca, olay izleme ve kayıt mekanizmaları optimize edilerek anormal aktivitelerin tespiti ve güvenlik ihlallerinin erken aşamada tespit edilmesi sağlanır.

Güvenlik sıkılaştırma hizmeti, organizasyonların siber saldırı yüzeyini daraltmasına, kritik sistemlerinin güvenliğini artırmasına ve yasal uyumluluk gerekliliklerini eksiksiz şekilde yerine getirmesine yardımcı olur. Bu hizmet, sürekli güvenlik denetimleri, tehdit istihbaratı desteği ve düzenli güvenlik kontrolleri ile desteklenerek organizasyonların değişen tehdit ortamına karşı dinamik ve proaktif bir savunma mekanizması oluşturmasını sağlar. Böylece, organizasyonların siber güvenlik olgunluğu artarken, saldırıların başarıya ulaşma olasılığı büyük ölçüde azaltılmış olur.

Hizmete Ait Bileşenler

Sistem ve Altyapı Analizi

İlk adım olarak, sunucular, istemci cihazları, ağ ekipmanları, veri tabanları ve uygulamalar dahil olmak üzere tüm BT altyapısı kapsamlı bir güvenlik değerlendirmesinden geçirilir. Mevcut yapılandırmaların siber güvenlik standartlarına uygunluğu denetlenerek olası riskler belirlenir.

İşletim Sistemi Sıkılaştırma

Windows, Linux, macOS gibi işletim sistemlerinde gereksiz servislerin kapatılması, varsayılan hesapların kaldırılması, güvenlik güncellemelerinin eksiksiz uygulanması ve erişim kontrollerinin optimize edilmesi sağlanır. CIS Benchmark ve NIST 800-53 gibi güvenlik çerçevelerine uygun yapılandırmalar uygulanır.

Ağ Güvenliği Sıkılaştırma

Güvenlik duvarları, yönlendiriciler, anahtarlar ve VPN sistemleri gibi ağ bileşenlerinin erişim kontrolleri gözden geçirilerek yalnızca yetkili cihaz ve kullanıcıların erişmesine izin verilir. Açık portlar ve gereksiz servisler kapatılır, segmentasyon ve mikro-segmentasyon teknikleri ile saldırı yüzeyi minimize edilir.

Kimlik ve Erişim Yönetimi (IAM)

Yetkilendirme süreçleri güçlendirilerek gereksiz ayrıcalıklar kaldırılır. Çok faktörlü kimlik doğrulama (MFA), ayrıcalıklı hesap yönetimi (PAM) ve rol tabanlı erişim kontrolü (RBAC) gibi yöntemler uygulanarak güvenlik seviyesi artırılır.

Veri Şifreleme ve Koruma

Hassas verilerin şifrelenmesi ve saklanması için güçlü şifreleme algoritmaları uygulanır. Veri kaybı önleme (DLP) çözümleri ile yetkisiz erişim girişimleri engellenir.

Güvenlik Güncellemeleri ve Yama Yönetimi

Sistemlerin en güncel yamalarla korunmasını sağlamak için düzenli olarak güvenlik güncelleme politikaları oluşturulur ve otomatik yama yönetim çözümleri devreye alınır.

Uygulama Güvenliği Sıkılaştırma

Web ve mobil uygulamaların güvenliği değerlendirilerek SQL Injection, XSS, CSRF gibi yaygın güvenlik açıkları kapatılır. Güvenli kod geliştirme ilkeleri (DevSecOps) benimsenerek yazılım güvenliği artırılır.

Olay Günlüğü Yönetimi ve İzleme

SIEM çözümleri ile sistemlerden gelen günlükler toplanır, analiz edilir ve şüpheli olaylar hakkında uyarılar oluşturulur. Logların merkezi bir platformda toplanarak anlık tehdit izleme ve analitik sistemlerle değerlendirilmesi sağlanır.

Güvenlik Sıkılaştırma Metodolojisi

Güvenlik Sıkılaştırma Hizmeti, organizasyonların BT altyapısını en iyi güvenlik standartlarına uygun hale getirmek için aşamalı bir metodolojiyle uygulanır.

1. Keşif ve Değerlendirme: İlk olarak, ağ, sistem ve uygulamalar detaylı bir şekilde analiz edilerek güvenlik açıkları belirlenir. Sızma testleri ve yapılandırma denetimleri yapılır.

2. Güvenlik Açıklarının Önceliklendirilmesi: Tespit edilen güvenlik zafiyetleri etki seviyelerine göre sınıflandırılır ve kritik açıklar öncelikli olarak giderilir.

3. Güvenlik Politikalarının Uygulanması: Erişim kontrolleri, kullanıcı yetkilendirme mekanizmaları ve veri koruma stratejileri belirlenerek uluslararası güvenlik standartlarına uygun hale getirilir.

4. Sistem ve Ağ Güvenliği: Gereksiz servisler kapatılır, ağ segmentasyonu yapılır, güvenlik duvarları ve erişim kontrol mekanizmaları güçlendirilir.

5. Veri Koruma ve Şifreleme: Hassas verilerin korunması için güçlü şifreleme ve veri kaybı önleme (DLP) çözümleri uygulanır.

6. Yama ve Güncelleme Yönetimi: Otomatik yama yönetimi ile güvenlik açıkları kapatılarak sistemler güncel tutulur.

7. Sürekli İzleme ve Olay Yönetimi: SIEM ve anomali tespiti sistemleri ile tehditler gerçek zamanlı izlenir ve otomatik müdahale mekanizmaları devreye alınır.

8. Güvenlik Farkındalığı ve Eğitim: Çalışanlara yönelik eğitimler ve siber güvenlik tatbikatları ile organizasyonun farkındalığı artırılır.

9. Denetim ve Sürekli İyileştirme: Düzenli testler ve güvenlik denetimleri ile sistemler sürekli optimize edilerek yeni tehditlere karşı güncellenir.

Bu süreç sayesinde organizasyonlar, siber tehditlere karşı daha güçlü ve güvenli hale getirilir.

Mevcut Durum Analizi

Güvenlik Sıkılaştırma Hizmeti uygulanmadan önce, kuruluşun mevcut güvenlik yapısı detaylı bir şekilde analiz edilir. Kullanılan güvenlik teknolojileri, erişim kontrol mekanizmaları, ağ güvenliği politikaları, sistem yapılandırmaları ve uç nokta güvenlik çözümleri değerlendirilir. Güvenlik açıklarının belirlenmesi amacıyla sistemler üzerinde yapılandırma denetimleri gerçekleştirilir ve yanlış yapılandırmalar tespit edilir. Zafiyet taramaları ve penetrasyon testleri yapılarak olası saldırı yüzeyi analiz edilir. Mevcut güvenlik politikalarının etkinliği incelenerek, sektöre özgü tehditler ve düzenleyici uyumluluk gereksinimleri göz önünde bulundurulur. Yapılan bu analiz sonucunda, kuruluşun güvenlik riskleri belirlenir ve sıkılaştırma stratejisi oluşturularak iyileştirme planı hazırlanır.

Strateji ve Yol Haritası Belirleme

Güvenlik Sıkılaştırma Hizmeti'nin etkin bir şekilde uygulanabilmesi için kuruluşa özel bir strateji ve yol haritası oluşturulur. Öncelikle, güvenlik sıkılaştırma sürecinin organizasyonel ihtiyaçlara nasıl entegre edileceği belirlenir. Kritik sistemler ve uygulamalar için güvenlik yapılandırmaları, erişim kontrolleri ve veri koruma önlemleri planlanır. SIEM, SOAR ve uç nokta güvenlik çözümleri gibi mevcut güvenlik altyapılarıyla entegrasyon süreçleri netleştirilir. Güvenlik politika ve prosedürlerinin güncellenmesi, konfigürasyon yönetimi ve otomatik güvenlik denetim mekanizmalarının uygulanması hedeflenir. Ayrıca, güvenlik farkındalığının artırılması için çalışanlara yönelik eğitim programları hazırlanır ve teknik ekipler için güvenlik en iyi uygulamaları belirlenir. Yol haritası, kısa, orta ve uzun vadeli hedefler doğrultusunda yapılandırılarak sürekli iyileştirme süreçleriyle desteklenir.

Güvenlik Sıkılaştırma Uygulama Aşamaları

Güvenlik Sıkılaştırma Hizmeti'nin uygulanma süreci, sistemlerin mevcut güvenlik seviyesinin değerlendirilmesi, güvenlik açıklarının belirlenmesi, sıkılaştırma politikalarının uygulanması ve sürekli izleme süreçlerini kapsar. İlk olarak, organizasyonun altyapısındaki güvenlik konfigürasyonları analiz edilir ve eksiklikler tespit edilir. Ardından, kritik sistemler için güvenlik en iyi uygulamalarına dayalı yapılandırma değişiklikleri yapılır ve güçlü kimlik doğrulama, erişim kontrolleri, şifreleme mekanizmaları gibi güvenlik önlemleri devreye alınır. Güvenlik sistemlerine entegre edilen otomatik denetim ve uyumluluk kontrolleri, olası güvenlik ihlallerinin erken tespit edilmesini sağlar. Sürekli güncellenen güvenlik politikaları ve izleme süreçleri sayesinde organizasyonun güvenlik seviyesi korunur ve gelişen tehditlere karşı adaptasyon sağlanır.

Raporlama ve İyileştirme

Güvenlik Sıkılaştırma Hizmeti kapsamında gerçekleştirilen çalışmalar düzenli olarak raporlanır ve analiz edilir. Sistemlerde yapılan güvenlik sıkılaştırmaları, uygulanan güvenlik politikaları ve tespit edilen zafiyetler detaylandırılarak teknik ekipler ve yönetim için özel olarak hazırlanmış raporlar sunulur. Güvenlik önlemlerinin etkinliği değerlendirilerek, sıkılaştırma süreçleri sürekli iyileştirilir. Uluslararası güvenlik standartları ve en iyi uygulamalar takip edilerek sistemlerin güncel tehditlere karşı dayanıklılığı artırılır. Ayrıca, güvenlik farkındalığını artırmak amacıyla periyodik güvenlik denetimleri, çalışan eğitimleri ve bilinçlendirme faaliyetleri düzenlenerek organizasyon genelinde siber güvenlik kültürü güçlendirilir.

Sıkça Sorulan Sorular (SSS)

Güvenlik Sıkılaştırma Hizmeti nedir?

Güvenlik Sıkılaştırma Hizmeti, sistemlerin, ağların ve uygulamaların siber tehditlere karşı daha dayanıklı hale getirilmesi için yapılan yapılandırma ve güvenlik iyileştirme çalışmalarını kapsar.

Güvenlik Sıkılaştırma Hizmeti neden gereklidir?

Siber saldırılar giderek daha sofistike hale geldiğinden, sistemlerin güvenlik açıklarını minimuma indirmek, saldırı riskini azaltmak ve veri güvenliğini sağlamak için gereklidir.

Güvenlik sıkılaştırma hangi sistemleri kapsar?

Sunucular, ağ cihazları, veritabanları, uç noktalar, bulut ortamları ve uygulamalar dahil olmak üzere tüm bilişim altyapısını kapsayacak şekilde uygulanabilir.

Hangi güvenlik standartlarına uygun olarak gerçekleştirilir?

Güvenlik sıkılaştırma süreci, NIST, CIS Benchmarks, ISO 27001, PCI-DSS ve diğer uluslararası güvenlik standartlarına uygun olarak gerçekleştirilir.

Mevcut sistemlerime zarar verir mi?

Hayır, güvenlik sıkılaştırma işlemleri, sistemlerin stabilitesi ve iş sürekliliği gözetilerek gerçekleştirilir. Öncesinde detaylı testler yapılır ve gerekli durumlarda geri dönüş mekanizmaları uygulanır.

Güvenlik sıkılaştırma hizmeti sonrası performans kaybı yaşanır mı?

Uygulanan güvenlik önlemleri performans üzerinde minimum etki bırakacak şekilde optimize edilir. Gerektiğinde donanım ve sistem konfigürasyonları gözden geçirilerek performans dengelemesi sağlanır.