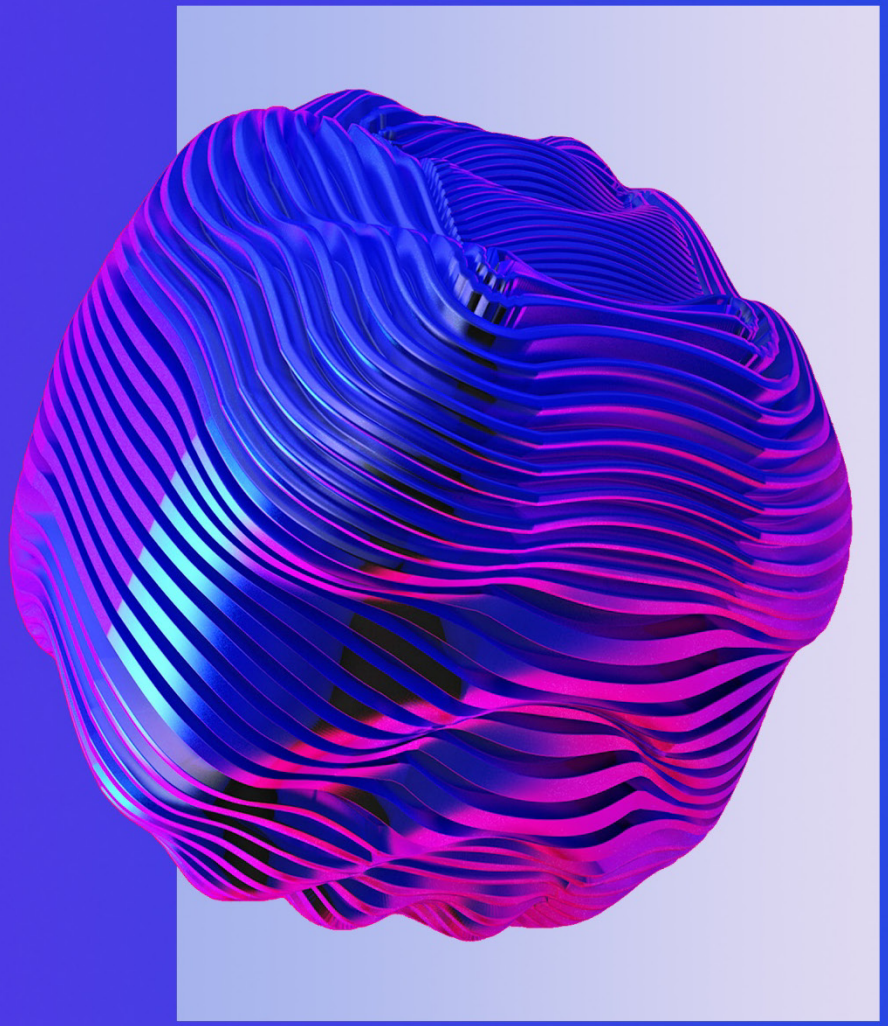
SAP sistemleriniz siber risklere karşı yeterince güvenli mi?



KPMG SAP Ortam Güvenliği Hizmet Yaklaşımı

—

Ocak 2024

SAP Ortamınızın Güvenliğinin Önemini Kavrayın

- ## Bir siber saldırı hedefi olarak SAP

Siber saldırganlar, SAP'nin teknik ve altyapı katmanlarındaki bilinen güvenlik açıklarını kullanarak organizasyon açısından kritik SAP verilerini ve bileşenlerini hedef almaktadır.

- ## SAP ortamını koruma ihtiyacı

Organizasyonlar, SAP altyapılarını güvence altına almak için tüm SAP bileşenlerini koruyan bütünsel bir SAP güvenlik ve yönetişim stratejisini benimsemelidir.

- ## SAP güvenlik stratejisi oluşturma

SAP güvenliği yalnızca kullanıcı erişimini kontrol etmek, görevler ayrılığı çatışmalarını ortadan kaldırmak ve güçlü değişiklik kontrolü uygulamaktan öte daha kapsamlı ve bütüncül bir strateji ile ele alınmalıdır.

Rakamlarla SAP Güvenliği

92%

Forbes Global 2000 listesinde yer alan şirketlerin %92'si SAP kullanıyor.

64%

Son 24 ayda ERP sistemlerinin (SAP dahil) %64'ü tehdit ve zafiyetlere maruz kalmıştır.

50.000

$ - Saatlik

ERP sisteminin kullanılamaması durumunda ortalama saatlik maliyet

768

Yıllık güvenlik notları (yama) ortalaması

Ponemon Institute: 2024 Cost of a Data Breach Report

S/4 HANA Geçişinde Potansiyel Riskler

S/4HANA, dijital dönüşümü hızlandırmak için yeni işlevsel ve teknik yenilikler sunar. Ancak önemli değişiklikler, güvenlik yeterince dikkate alınmadığında yeni riskleri ortaya çıkarabilir. Bu önemli değişiklikler ve potansiyel risklerden bazıları şunlardır:

Yeni İşlevsellikler

Yeni veya zorunlu uygulama işlevselliği, bazı eski uygulama kontrollerini etkisiz hale getirebilirken, yeni kontroller henüz yapılandırılmamış olabilir.

Veri Geçişi

Yeni veri tabloları ve veritabanı yapılarına sahip olan S/4HANA'ya geçişte, taşınan verilerin yeterli test ve doğrulama süreçlerinden geçmesi gerekmektedir.

Gerçek Zamanlı Erişim

Verilere gerçek zamanlı erişim, organizasyonu; hassas verilere yetkisiz erişime açık hale getirir.

Sıkılaştırma

Birçok yeni arayüz yeterince sıkılaştırılmamış olabilir. Bu durum, güçlü bir arayüz kontrol ve izleme süreci gerektirir.

Üçüncü Taraf Erişimi

Üçüncü taraf güvenliği, yeni sistem mimarisi için değerlendirilmelidir. Organizasyonlar, hangi üçüncü taraf güvenlik önlemleri ve kontrollerini benimsemek istediklerini dikkate almalıdır.

Paylaşılan Sorumluluklar

SAP güvenliğine ilişkin her paydaşın görevlerini ve taahhütlerini anlamasını sağlamak için net sorumluluk çizgilerinin belirlenmesi, güvenlik çerçevesini güçlendirmek adına oldukça önemlidir.

Doğru Soruları Sorduğunuzdan Emin Olun

SAP Güvenlik Stratejisi
Tüm ilgili SAP Güvenlik yönlerini kapsayan bir SAP Güvenlik Stratejisi benimsediniz mi?

Sorumluluklar
SAP güvenliğinin farklı yönleri için sorumluluklar net bir şekilde tanımlanmış mı?

Güvenlik Standardı
SAP sistemlerini sıkılaştırmak için hangi güvenlik standardını kullanıyorsunuz?

SAP Güvenlik Araçları
Güvenliği izlemek için hangi SAP güvenlik araçlarını kullanıyorsunuz?

Roller ve Yetkilendirmeler
Kullanıcılar ve yöneticiler için roller ve yetkilendirmelerle ilgili bir konsept var mı?
Bu konsept uygulanmış mı?

SAP Ortam Bileşenleri
SAP sistemini barındıran ağ katmanı, işletim sistemleri ve veritabanları nasıl güvence altına alınıyor?

Yazılım güvenliği
Kaynak kodun güvenliğini nasıl sağlıyorsunuz? SAST, DAST ve SAP'ye özgü araçları kullanıyor musunuz?

Güvenlik Notları
SAP güvenlik notlarının (yamalarının) zamanında uygulanmasını nasıl sağlıyorsunuz?

Kontrol ve İzleme
Şüpheli aktiviteleri nasıl izliyorsunuz? Hangi izleme kullanım senaryoları uygulanmış durumda?

Nasıl Yardımcı Olabiliriz?

Hizmet Yaklaşımımız

KPMG olarak organizasyonların veri bütünlüğü ve gizliliğini korumak için SAP ortamlarının güvenliğinin sağlanmasının kritik öneminin bilincindeyiz. Yaklaşımımız, organizasyonunuzun riskleri azaltmasına ve siber savunmasını güçlendirmesine yardımcı olmak için çeşitli SAP güvenlik hizmetleri sunmaya odaklanıyor.

1. Altyapı Güvenliği

- SAP uygulama ve veritabanı sunucu güvenliği (sıkılaştırma, CIS benchmarkları)
- SAP router, diğer web uygulamaları vb. entegrasyon güvenliği (ör: OWASP Top 10)
- Ağ segmentasyonu ve trafik güvenliği (ör: kriptolama vs.)

2. Uygulama Güvenliği

- Kullanıcı yönetimi (kritik profil, rol, yetki) tasarımı
- Versiyon ve yama yönetimi
- Sistem logları yönetimi
- Kritik tabloları loglama ve erişim güvenliği (sistem tabloları, default ve custom programlar)
- Uyarlama ve geliştirme süreçleri güvenliği (standart ve standart dışı uyarlama, geliştirme ve müdahale yöntemleri)

3. Konfigürasyon & Veri Güvenliği

- Standart güvenlik parametreleri (SAP, ISACA vb. kılavuzları eşliğinde) ve yapılandırması
- SAP veri güvenliği Yönetimi
- SAP üzerinde işlenen veri envanteri değerlendirme, veri sınıflandırma ve güvenlik önlemleri eşleştirmesi (varsa)
- KVKK/GDPR için alınan önlemlerin değerlendirilmesi

4. GRC Teknoloji Etkinleştirme

- Kimlik doğrulama, yetkilendirme ve erişim yönetimi süreçlerinin teknoloji üzerinden yönetilmesi
- Otomasyon güvenliği
- GRC teknoloji etkinleştirme danışmanlığı

İletişim

Ümit Yalçın Şen
Siber Güvenlik
Hizmetleri Lideri,
Şirket Ortağı
umitsen@kpmg.com

Detaylı bilgi için:
KPMG Turkey
Clients & Markets
tr-fmmarkets@kpmg.com

Teklif Talep Formu:
https://kpmg.com/tr/tr/home/hizmetlerimiz/rfp-form.html

İstanbul
İş Kuleleri, Kule 3, Kat:1-9
Levent/ İstanbul/ Türkiye
34330
T: +90 212 316 60 00

Ankara
The Paragon İş Merkezi Kızılırmak Mah.
Ufuk Üniversitesi Cad. 1445 Sok. No:2
Kat:13 Çukurambar/ Ankara / Türkiye
06550
T: +90 312 491 7231

İzmir
Folkart Towers, Adalet Mah. Manas
Bulvarı No:39 B Blok Kat:35 Bayraklı/
İzmir / Türkiye
35210
T: +90 232 464 2045

Bursa
Odunluk Mahallesi, Liman
Caddesi, Efe Towers, No:11/B,
9-10 Nilüfer/Bursa / Türkiye
16225
T: +90 224 503 8000

Adana
Sunar Nuri Çomu İş Merkezi Sitesi A
Blok No: 18 İç Kapı No: 13 Seyhan /
Adana
T: +90 322 450 21 20

kpmg.com.tr

kpmgvergi.com

© 2025 KPMG Yönetim Danışmanlığı A.Ş., şirket üyelerinin sorumluluğu sundukları garantiyle sınırlı özel bir İngiliz şirketi olan KPMG International Limited ile ilişkili bağımsız şirketlerden oluşan KPMG küresel organizasyonuna üye bir Türk şirketidir. Tüm hakları saklıdır. Bu dokümanda yer alan bilgiler genel içeriklidir ve herhangi bir gerçek veya tüzel kişinin özel durumuna hitap etmemektedir. Doğru ve zamanında bilgi sağlamak için çalışmamıza rağmen, bilginin alındığı tarihte doğru olduğu veya gelecekte olmaya devam edeceği garantisi yoktur. Hiç kimse özel durumuna uygun bir uzman görüşü almaksızın, bu dokümanda yer alan bilgilere dayanarak hareket etmemelidir. KPMG adı ve KPMG logosu, bağımsız üye şirketlerden oluşan KPMG küresel organizasyonun lisansı altında tescilli ticari markalardır. KPMG International Limited ve ilişkili kuruluşları müşterilere herhangi bir hizmet sunmamaktadır. © 2025 KPMG Bağımsız Denetim ve Serbest Muhasebeci Mali Müşavirlik A.Ş., şirket üyelerinin sorumluluğu sundukları garantiyle sınırlı özel bir İngiliz şirketi olan KPMG International Limited ile ilişkili bağımsız şirketlerden oluşan KPMG küresel organizasyonuna üye bir Türk şirketidir. Tüm hakları saklıdır.