Sertiva

PCI DSS 4.0.1 — 31 Mart 2025'te zorunlu olan gereksinimler

v4.0 ile gelen 64 yeni gereksinimin 51'i ileri tarihliydi ve 31 Mart 2025'te yürürlüğe girdi. Bu liste, uygulamada en çok iş çıkaran ve denetimde en sık takılınan maddeleri işaretleyerek ilerlemeniz için hazırlandı.

24 MADDE SÜRÜM 4.0.1 AĞUSTOS 2026 SERTİVA.CO

Nasıl kullanılır. Her maddeyi üç soruyla değerlendirin: kontrol **var mı**, **yıl boyunca** çalıştığını gösterebiliyor musunuz, ve **sahibi** kim? Denetimde sorulan şey kontrolün bugün çalıştığı değil, dönem boyunca çalıştığıdır. Bu liste tam bir uygunluk değerlendirmesi yerine geçmez; kapsamınıza özel maddeler için denetçinizle çalışın.

Ödeme sayfası güvenliği

Tarayıcı tarafında kart verisi çalan saldırılara karşı.

- [ ] 6.4.3 Ödeme sayfasındaki her script yetkilendirildi, bütünlüğü güvence altına alındı ve gerekçesiyle envantere yazıldı.
- [ ] 11.6.1 Sayfa içeriğindeki ve HTTP başlıklarındaki yetkisiz değişikliği tespit edip uyarı üreten mekanizma çalışıyor (en az haftalık).

Kimlik doğrulama ve hesap yönetimi

En çok bulgu çıkan alan.

- [ ] 8.4.2 Kart veri ortamına konsol dışı tüm erişimlerde çok faktörlü doğrulama uygulanıyor.
- [ ] 8.3.6 Parola uzunluğu en az 12 karakter (sistem desteklemiyorsa 8) olarak zorlanıyor.
- [ ] 8.6.1 Etkileşimli oturum açabilen uygulama/sistem hesapları için ek koşullar tanımlı.
- [ ] 8.6.2 Hiçbir parola koda, betiğe ya da yapılandırma dosyasına gömülü değil.
- [ ] 8.6.3 Uygulama ve sistem hesaplarının parolaları periyodik olarak değiştiriliyor.
- [ ] 7.2.4 Kullanıcı hesapları en az altı ayda bir gözden geçiriliyor ve kayda alınıyor.
- [ ] 7.2.5 Uygulama ve sistem hesapları da periyodik incelemeye tabi.

Zafiyet yönetimi ve test

Tarama yapmak yetmiyor; nasıl yapıldığı da denetleniyor.

- [ ] 11.3.1.1 Yüksek/kritik olmayan zafiyetler risk analizine göre ele alınıyor.
- [ ] 11.3.1.2 İç zafiyet taramaları kimlik doğrulamalı olarak yapılıyor.
- [ ] 6.4.2 Halka açık web uygulamalarında WAF ya da eşdeğer otomatik çözüm var.

☐	6.3.2	Özel yazılım ve üçüncü taraf bileşenlerin envanteri tutuluyor.
☐	5.2.3.1	Kapsamdaki sistemlerin kötü amaçlı yazılıma yatkınlığı periyodik değerlendiriliyor.
☐	5.3.3	Çıkarılabilir medya için kötü amaçlı yazılım taraması yapılıyor.
☐	5.4.1	Kimlik avına karşı otomatik koruma mekanizması devrede.

Veri koruma ve şifreleme

☐	3.5.1.2	Disk düzeyi şifreleme, çıkarılabilir medya dışında tek başına yeterli sayılmıyor.
☐	4.2.1	Kart numarası taşıyan sertifikalar geçerli; süresi dolmuş ya da iptal edilmiş sertifika yok.
☐	4.2.1.1	Güvenilen anahtar ve sertifikaların envanteri tutuluyor.

Risk analizi ve program yönetimi

En çok atlanan grup — özellikle 12.3.1.

☐	12.3.1	Frekansı esnek bırakılan HER gereksinim için hedefli risk analizi (TRA) yazıldı: varlık, tehdit, gerekçe, frekans.
☐	12.3.3	Kullanılan şifreleme takımları ve protokoller yıllık gözden geçiriliyor.
☐	12.3.4	Kullanılan teknolojiler yıllık gözden geçiriliyor; ömrünü tamamlamış bileşen yok.
☐	12.6.2	Güvenlik farkındalık programı yıllık gözden geçiriliyor (kimlik avı ve kabul edilebilir kullanım dahil).
☐	12.10.7	Kart numarasının olmaması gereken bir yerde bulunması senaryosu olay müdahale planında yer alıyor.