Yönetsel Arayüzler

Amaç

- Yönetsel işlevlerin kullanıcı faaliyetlerinden uygun şekilde ayrılmasını
- Kullanıcıların yönetici işlevselliğini kullanamaması ya da erişememesini
- Yönetici işlevselliğine yönelik gerekli denetim ve izlemenin temin edilmesini sağlamak.

Etkilenen Ortamlar

Hepsi.

İlgili COBIT Konuları

PO4

- 4.08 Veri ve Sistem iyeliği – ayrı işlemsel ve güvenlik yönetimi gerektirir
- 4.10 Görev ayrımı

Doğru Uygulamalar

Yönetsel arayüzler, yasal olarak düzenlenen Kılavuz kapsamındaki kontrollerden biridir – Sarbanes Oxley, yönetsel işlevlerin normal işlevlerden ayrılmasını gerektirmektedir çünkü bu dolandırıcılığa karşı kullanılan temel bir kontrol aracıdır. ABD yasalarına uyması gerekmeyen organizasyonlar için, ISO 17799 da görev ayrımı olduğunu ifade eder. SOX veya ISO 17799 gereklerine uyum sağlamamaktan kaynaklanan riski dikkate alıp almamak tasarımcıların kararına kalmıştır.

- Uygulamaları tasarlarken, yönetsel işlevsellik çerçevesini belirleyin ve uygun erişim kontrolleri ile denetim sisteminin var olduğundan emin olun.
- Süreçleri dikkate alın – bazen yapılması gereken tek şey kullanıcıların basit bir erişimsizlikten dolayı bir özelliği kullanmalarına nasıl engel olunduğunu anlamaktır
- Yardım masası erişimi her zaman ara alandır – müşterilere destek olmak için erişime gerek duyarlar, ancak yönetici değildirler.
- Sınırlı yönetim kapasitesi, ayrılmış uygulama ya da erişim çevresinde yardım masası / moderatör / müşteri destek işlevini dikkatli bir şekilde tasarlayın.

Bu, birincil uygulamaya kullanıcı olarak kayıt olan yöneticilere izin verilmediği anlamına gelmemekle birlikte yöneticiler bu şekilde kayıt olduklarında normal kullanıcı durumunda olacaklardır. Büyük bir e-ticaret sitesinin sistem yöneticisinin siteyi kullanarak bir şeyler satması ve satın alması örnek gösterilebilir.

Yöneticiler kullanıcı değildirler

Yöneticilerin normal kullanıcılardan ayrılması gerekmektedir.

Savunmasız ve saldırıya açık olduğunuzu nasıl anlayacaksınız

- Uygulamaya yönetici olarak kayıt olun.
- Yönetici normal işlemler gerçekleştirebiliyor mu ya da normal uygulamayı görebiliyor mu?
- Yönetim işleminin URL'sini biliyorlarsa, kullanıcılar yönetsel çalışmalar ya da işlemler gerçekleştirebiliyor mu?
- Yönetsel arayüz aynı veritabanını ya da aracı yazılım erişimini kullanıyor mu? (örneğin, veritabanı hesapları ya da güvenilir iç yollar)
- Yüksek değer sisteminde, kullanıcılar yönetsel arayüzü içeren sisteme erişebiliyorlar mı?

Eğer sorulara cevabınız evet ise, sistem potansiyel olarak saldırıya açıktır.

Nasıl korunacaksınız

- Bütün sistemlerin, yönetici ve kullanıcı erişimi için ayrı uygulamaları olmalıdır.
- Yüksek değerli sistemler, yönetim ağlarına erişim olmadan bütün İnternet ortamında, erişime açık olmayabilen sunucuları ayırmak için bu sistemleri ayırmalıdır. Ciddi bir şekilde kimlik denetimi yapılmış VPN kullanımı aracılığıyla ya da güvenilir ağ işlemleri merkezinden gerçekleştirilebilir.

Yüksek değer sistemleri için kimlik denetimi

Yönetsel arayüzler, yapıları gereği bütün sistemin sağlıklı işlemesi için tehlike arz etmektedir. Yönetsel özellikler doğrudan SQL soruları, veritabanını yükleme ya da destekleme, güvenilir bir üçüncü taraf sistemininin durumunu doğrudan sorgulamayı kapsayabilir.

Savunmasız ve saldırıya açık olduğunuzu nasıl anlayacaksınız

Yüksek değerli bir sistem, arayüze kayıt olmak için sağlam bir kimlik denetimi ya da şifrelenmiş kanallar kullanmıyorsa, söz konusu sistem gizlice dinleme, araya girme saldırısı ve tekrar gönderme saldırısı gibi saldırılara açık ve korumasız olabilir.

Nasıl korunacaksınız

Yüksek değerli sistemler için;

- Yönetsel erişim için güçlendirilmiş ayrı bir yönetim ağı kullanın.
- Kayıt olmak için güvenilir kimlik denetimi kullanın, yönetsel parola hırsızlığı ve oturum sürme saldırılarını engellemek için büyük ya da tehlikeli işlemleri tekrar kimlik denetiminden geçirin.
- Oturumun gizliliğini ve bütünlüğünü korumak için SSL şifreli web sayfaları gibi şifreleme kullanın.

Daha ayrıntılı bilgi için lütfen aşağıdaki kaynakları inceleyiniz

- Yönetici ve kullanıcıların neden ayrılması gerektiği ile ilgili mükemmel bir örnek: http://www.securityfocus.com/bid/10861/discuss

  Dökümanın Aslı : OWASP GUIDE 2.0.1

  Çeviri **:** Çiğdem Akanyıldız - acigdema@yahoo.com