## Erişim kontrol modelleri

Saldırılara karşı savunma yollarından biri, çeşitli bilgi parçalarına kimin erişebileceğini belirlemenin titiz yollarını sağlayarak bunları önlemektir. Tüm modeller, erişim kontrol özelliklerini tanımlayan veri yöneticileri, veri sahipleri veya sistem yöneticilerinin olduğunu varsayar. Erişim, söz konusu bilgilere erişme ve/veya bunları değiştirme ihtiyacı olan kişilerle sınırlandırılmalıdır. Yani, en az ayrıcalık ilkesini uygulamalıdırlar.

Erişim Kontrol Matrisleri (ACM)

İzinleri tanımlayan bir tablodur. Bu tablonun her satırı, eylemler gerçekleştirebilen bir kullanıcı, grup veya sistem olan bir özne ile ilişkilendirilmiştir. Tablonun her sütunu, erişim haklarını tanımlamak istediğimiz bir dosya, dizin, belge, aygıt, kaynak veya başka herhangi bir varlık olan bir nesne ile ilişkilendirilmiştir. Tablonun her hücresi, özne ve nesnenin ilişkili kombinasyonu için erişim haklarıyla doldurulur. Erişim hakları, okuma, yazma, kopyalama, yürütme, silme gibi eylemleri içerebilir. Boş bir hücre, hiçbir erişim hakkının verilmediği anlamına gelir.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | / vb / şifre | / kullanıcı /bin/ | /u/Roberto/ | /yönetici/ |
| Kök | Oku, yaz | Oku, yaz, yürüt | Oku, yaz, yürüt | Oku, yaz, yürüt |
| Mike | Okumak | Oku, yönetici |  |  |
| Roberto | Okumak | Oku, yönetici | Oku, yaz, yürüt |  |
| Yedekleme | Okumak | Oku, yönetici | Oku, yönetici | Oku, yönetici |

Erişim Kontrol Listeleri (Access Control List, ACL)

Bunlar, her nesne için kimin (öznenin) nesneye hangi erişime sahip olduğunu gösteren listeler halinde düzenlenmiş ACM sütunlarıdır.

Yetenek Listeleri (Capability List, CL)

Bunlar, her bir özne için hangi nesnelerin ve hangi modda kullanılmasına izin verildiğini gösteren ACM satırlarıdır

Rol Tabanlı Erişim Kontrolü (Role-Based Access Control, RBAC)

Yöneticiler rolleri tanımlar, onlar için erişim kontrol haklarını belirler ve ardından rollere öznelere/rollere atar. Roller, organizasyon yapısını temsil edecek şekilde hiyerarşik olarak düzenlenebilir.

Zorunlu Erişim Kontrolü (Mandatory Access Control, MAC) , Bell – La Padula modeli (BLP)

BLP modeli askeri çok seviyeli güvenlik paradigmasından türetilmiştir (Çok gizli, Gizli, Gizli, Sınıflandırılmamış)

Her belgenin 4 güvenlik seviyesinden 1'i, her kullanıcının da 4 güvenlik seviyesinden 1'i "güvenlik izni" bulunmaktadır.

Belirli bir düzeydeki belgeye yalnızca aynı veya daha yüksek yetki düzeyine sahip kullanıcılar erişebilir, "okuma yok" kuralı.

Bir kullanıcı sadece kendi veya daha üst güvenlik seviyesindeki dokümanlara, “yazma yok” kuralına, '\*' özelliğine göre yazabilir.