İŞLETİM SİSTEMLERİ GÜVENLİĞİ

Burak Bayoğlu, BTYÖN Danışmanlık

Bilgisayar sistemlerinin temel işletim altyapısını oluşturan işletim sistemleri, sistem üzerinde çalışan diğer uygulama ve servislere de güvenlik altyapısı sağladıkları için işletim sistemlerinin güvenliği bütün sistemin güvenliği için büyük rol oynamaktadır. İşletim sistemi açıklıkları ve zayıflıklarına karşı gerekli önlemler uygulamaya geçirilmediği sürece sistem oldukça fazla risk taşımaktadır ve büyük zararlara uğrayabilir.

İşletim sistemlerinde mevcut güvenlik mekanizmaları kullanılıyor olsa bile öncelikle sistem yöneticilerinde ve sistem kullanıcılarında güvenlik bilinci gelişmiş olmalıdır. Ayrıca kullanılacak işletim sisteminin iddia ettiği güvenlik garanti seviyesinin tarafsız bir test laboratuarı tarafından test edilip onaylanması, işletim sistemi güvenlik fonksiyonlarının güvenilirliği açısından çok önemlidir.

İnternet sayesinde bilgisayar sistemlerinin daha bağlaşık olmaları, zayıflık ve açıklıkların çok çabuk öğrenilip büyük zararlara sebep olabilecek saldırıların kolayca uygulanabilmesi, diğer servis ve uygulamalara çalışma altyapısı sağlaması gibi sebeplerden ötürü işletim sistemleri güvenliği bir bilgisayar sisteminin güvenliği sağlanırken ilk olarak düşünülmesi gereken konulardan birisidir. Bu makalede işletim sistemleri açıklıkları, tehditler, ideal olarak bulunması gereken ve pratik olarak uygulanan güvenlik tedbirleri açıklanmıştır.

İşletim Sistemlerinin Açıklıkları ve Tehditler

İşletim sistemlerinde bulunan güvenlik mekanizmalarını incelemeye başlamadan önce, bu güvenlik mekanizmalarında doğabilecek zayıflık ve açıklıklardan kaynaklanabilecek bazı tehditlerden bahsetmek gerekir. Bu bölümde bahsedilen tehditlerin, uygulanan bir güvenlik mekanizması mevcut olsa bile işletim sisteminin doğru konfigüre edilip yönetilmemesi durumunda olma olasılıkları yüksektir. Burada bahsedilen açıklık ve tehditler tabii ki muhtemel tüm durumları içermemektedir. Sadece olası zayıflıklardan örnekler verilmiştir.

Kimdir O?

Herhangi bir bilgisayar sistemini ele geçirmek isteyen bir saldırganın yapacağı ilk iş, kıracağı bilgisayar sistemi hakkında bilgi edinmektir. Örneğin bir güvenlik duvarını kırmak istiyorsa o güvenlik duvarının hangi yazılım olduğu, hangi işletim sistemi üzerinde koştuğu, sürüm numaraları vb. bilgiler bir bilgisayar korsanı için paha biçilmedir. Saldırgan hedef hakkında bilgi sahibi değilse, o hedef üzerinde özel güvenlik açıklıklarını deneyemeyecektir. Kapı çalma denilen yöntemlerle saldırgan sistem hakkında bilgi edinmeye çalışır. Bazı özel TCP paketlerine işletim sistemlerinin verdiği cevaplar farklı olabilir. Çünkü farklı tiplerdeki işletim sistemlerinde gömülü olan TCP/IP yığın yazılımları bazı yönleri ile farklıdır. Saldırgan bu tür TCP paketleri göndererek kurbanın işletim sistemini öğrenebilir. Kapı çalma saldırıları, genelde çok uzun vadede yapılan saldırılardır. Kurban bu tür bir saldırıyı anlayamadığı için karşı bir önlem alma ihtiyacı duymayabilir. İşletim sistemi ve üzerinde çalışan servis ve uygulamaların sürüm bilgilerinin genellikle açığa vurulduğu servis karşılama mesajları kullanıldığında bu tür bilgi toplama saldırılarında çok daha hızlı sonuç alınabilir. Karşılama mesajları genellikle değiştirilebilir. Yanlış sistem ve sürüm bilgileri gösterildiği zaman hem saldırgana değerli bilgi verilmemiş olur hem de saldırı zamanı geciktirilebilir.

Kullanıcı Şifrelerine Yönelik Saldırılar

Bir bilgisayar sistemindeki en önemli varlıklardan bir tanesi kullanıcı şifreleridir çünkü sistemde koruduğumuz daha önemli varlıklar mevcut olsa bile onlara erişim genelde söz konusu şifrelerin gizli olması halinde güvenli varsayılabilir. Her türlü gizli bilgilerimize, banka hesaplarımıza, elektronik postalarımıza şifreler yardımıyla ulaşır ve bu kıymetlerimizi şifreler yardımıyla korumaya çalışırız. Durum

böyle olunca, kötü niyetli bir kişi için şifreler en önemli hedef olmaktadır. Kötü niyetli kimseler, şifre kırma programları ile ya da ağdaki paketleri yakalayarak şifre elde etmeye çalışabilirler. Çok kullanıcılı işletim sistemlerinde kullanıcı şifreleri tek yönlü özet(hash) fonksiyonlarına sokulduktan sonra sistemde özet halinde saklanırlar. Kullanılan özet algoritmasının güvenilirliğine bağlı olarak bu bilgiyi ele geçiren bir saldırgan zor kullanma (brute force) metodu ile saklı şifreleri bulabilir. O halde kullanıcı şifre bilgilerinin saklandığı dosyanın kötü niyetli kişilerin eline geçmemesi için işletim sistemi ve sistem yöneticisi tarafından gerekli önlemlerin alınması gereklidir. Aynı durum kriptografik parametrelerin ve anahtarların saklandığı dosyalar için de geçerlidir.

Kullanıcı Hesaplarına İzinsiz Girilmesi ve Kullanıcı Hesaplarının Yetkisiz Kullanılması

Kullanıcı şifreleri tahmin edilebilecek kadar kolay olabilir, hatta bazı kimselerin iş bilgisayarlarına şifre atamaması ya da şifrelerini bir kağıda yazıp masaüstüne koymaları söz konusu olabilir. Böyle durumlarda hesaplarınız isteğiniz dışında bir başkası tarafından kullanılabilecek ve gizli bilgileriniz çalınabilecektir. Kullanıcı şifrelerinin tahmin edilmesi için saldırgan muhtemel şifreleri sistem kaynakları üzerinde deneyerek doğru şifreyi bulmaya çalışır. Üst üste belirli bir sınırın üzerinde yanlış şifre girildiğinde kullanıcı hesabını devre dışı bırakacak güvenlik mekanizması işletim sistemi kimlik doğrulama fonksiyonlarında mevcut değil ise otomatikleştirilmiş programlar sayesinde saldırgan çok sayıda şifreyi kısa sürede deneyebilir.

Güveni Kötüye Kullanma

İki bilgisayar arasında kurulan karşılıklı güven kötüye kullanılabilir. Örneğin, UNIX sistemlerinde rlogin komutu ile güven kapsamında olan başka bir bilgisayara şifresiz yetkili kullanıcı hakları ile bağlanılabilir. Böyle bir durum kötü niyetli bir kişi için bulunmaz bir fırsattır.

Servislere Yetkisiz Erişim

Bir saldırgan, hedeflediği sisteme giriş için mutlaka o sistemi değişik yöntemlerle ve araçlarla kırmak zorunda değildir. Kırmak istediği sistemin sağladığı ama saldırganın erişimine yetkisiz olduğu servisleri kullanarak da o sisteme normal kullanıcı gibi girebilir. Örneğin bilgisayara erişim yetkisi olmayan bir saldırganı düşünelim. Saldırganın bu bilgisayara girmesini sağlayacak kullanıcı ismi ve şifresi yoktur. Ama bilgisayarda bir FTP sunucusu koşuyorsa, saldırgan bu FTP servisinin açıklarını kullanarak ya da bildiği bir kullanıcının hesabıyla ya da anonim olarak belli bir oranda erişim sağlayabilir ve sistem hakkında bilgiler elde edip daha sonra tam erişim sağlayabilir.

Kaynaklara Yetkisiz Erişim

Kötü niyetli kişiler, bir sistemde bulunan kaynaklara yetkisiz ulaşmak isteyebilirler. Buna genelde iyi ayarlanmamış ve düşünülmemiş nesne izinleri ve sistemdeki açıklılar neden olur. Örneğin birçok kişinin kullandığı bir bilgisayarda, her kullanıcının kendine ait ev dizini bulunur. Bir kişi sisteme giriş yaptığı zaman, diğer kullanıcıların ev dizinlerindeki dosya ve klasörlere erişemez. Ancak kullanıcı tarafında yanlış ayarlanmış bir dosya ya da klasör izni, diğer kişilerin kendi dosya ve klasörlerini görmesine ve hatta değiştirmesine yol açabilir.

İmtiyaz Artırma

Kötü niyetli bir kişi bir sisteme erişim sağladıktan sonra, sisteme daha sonraki zamanlarda kolaylıkla girebilmesi için ya da daha sonra işlerini daha kolay yapması için kendi imtiyazlarını artırma yoluna gider. Böyle yaparak hem izinsiz girdikleri hesabı daha iyi kontrol altında tutarlar hem de ağda bulunan diğer bilgisayarlara bu şekilde yayılabilirler. İmtiyaz artırmaları, sistem yönetici hesaplarına girerek daha kolay

yapılır. Başka bir yolu da, normal kullanıcı hesaplarına yetkisiz girdikten sonra işletim sisteminin ya da yazılımların açıklıklarını kullanarak ayrıcalıklı haklar kazanmaktır.

Yetkisiz Faaliyeti Örtme

İşletim sistemlerinin ve yazılımların çoğunluğunun denetim (audit) özellikleri vardır. Denetim sonucu oluşan kayıtlar sistemdeki kayıt dosyalarına yazılırlar. Ama tüm sistemlerde görülen açıklıklar ve eksik kodlama, hesap denetimi programlarında da olabilir. Sisteme normal olmayan yollardan giriş yapan bir kişi kayıt dosyasını kullandığı özel programlarla işe yaramayan bilgilerle doldurabilir veya mevcut kayıtları değiştirebilir. Böylece yetkisiz faaliyetlerini örter.

Zararlı Programlar

Virüsler

Virüsler, bilgisayarlar ilk çıktığı zamanlardan bu yana devamlı gündemde olmuş zararlı yazılımlardır. Daha önceleri büyük oranda disketler yoluyla bulaşan virüsler internetin yaygınlaşmasıyla artık bilgisayarlarımızı daha fazla ve sıklıkla etkilemeye başlamıştır. Bununla da kalmayıp, en tehlikeli ve yayılması kolay olan ağ virüsleri (solucanlar) ortaya çıkmıştır. Örneğin, bir ağ virüsü, elektronik postaya iliştirilerek gönderilmekte, kurbanın adres kutusunda bulunan diğer elektronik posta adreslerine kendi kendini göndermekte ve kurbanın bilgisayarını kullanılamaz duruma getirmektedir. Virüsler için en iyi çözüm bir anti-virüs yazılımı kullanmak ve yazılımın güncellemelerini zamanında edinmektir. Ayrıca, elektronik posta ile gelen eklentilerin nereden geldiğini bilmiyorsak ve şüpheliysek hiç açılmadan silinmesi tavsiye edilir. Sistem giriş noktalarında ağ seviyesinde virüs koruma yazılımlarının bulunması oldukça faydalıdır.

Truva Atları

Truva atları, bir tür casus yazılımlardır. Truva atlarının bilgisayara bulaşması virüslerin bulaşmasına benzer, elektronik posta ile gelen bir eklentiyi açarak ya da internetten indirdiğimiz bir dosyayı açarak bir truva atını bilgisayarımıza bulaştırabiliriz. Ancak truva atları virüslerin yaptığı gibi sistem üzerinde görünür bir zararı olmayabilir. Truva atlarının bilgisayarda yaptığı iş, bir TCP ya da UDP portu açmaktır. Bu portlar 1023'den yukarı olan portlar olabileceği gibi, 23, 80 gibi tanınan portlar da olabilir. Truva atlarının iki ayağı vardır. Bunlar sunucu ve istemci olarak isimlendirilir. Sunucu, bilgisayara bulaşan ve bir port açan program parçasıdır. İstemci ise, saldırganın kullandığı parçadır. Kullanıcı, truva atlarının istemci ayağını kullanarak, sunucuya bağlanır ve etkilenmiş bilgisayarın birçok kaynağına erişebilir. Öyle ki uzaktaki bilgisayarın ekran görüntülerinin alınması, sabit diskini formatlanması vs. mümkündür. Truva atlarından en iyi korunma yöntemi, bir anti-virüs yazılımı kullanmak ve yazılımın güncellemelerini zamanında edinmektir. Ayrıca, elektronik posta ile gelen eklentilerin nereden geldiğini bilmiyorsak ve şüpheliysek hiç açılmadan silinmesi tavsiye edilir.

Diğer Yazılımlar

Virüsler ve truva atı kategorisine sokulmayacak başka zararlı programlar da mevcuttur. Bu programlar bilgisayarın işlemcisine çok fazla yük getirebilir, bu sebeple bilgisayarı kilitleyebilir, ya da bilgisayarın hafızasına bir sürü boş bilgi doldurup bilgisayarı kullanılamaz duruma getirebilir. Bu tip programlar ve kaynak kodları internette birçok sitede bulunabilir. C, C++, Java vb. dillerde yazılabilen bu programların kaynak kodları genelde kısa olur. Bu tip programları anti-virüs programları bulamayabilir. Bu tip programlar genelde büyük bir tehdit unsuru değildir. Çünkü yayılma özellikleri yoktur. Bilgisayarımızın kullanılmaz hale gelmesi de bir o kadar önemlidir.

Sosyal Mühendislik

Sosyal mühendislik, teknik olmayan bir saldırı türüdür ve kimi zaman teknik saldırılardan daha tehlikeli olabilir. Sosyal mühendislik değişik şekillerde yapılabilir. Örneğin bir kişi kendisini sistem yönetici gibi göstererek elektronik posta yollayabilir ya da şifresini almak istediği kişinin yanına gelip yardım etmek isteyebilir. Bütün bunlardaki amacı sisteme yetkisiz olarak girmek için gerekli bilgileri almaya çalışmaktır. Örneğin işletim sistemi versiyonu, kripto anahtarı, yazılım versiyonları, şifreler vb. bilgiler saldırganın hedefleri arasında olabilir.

Fiziksel Ortam Açıklıkları

Sistem odasında bulunan güvenlik duvarlarının, sunucuların ve sistem odasının fiziksel güvenliği göz ardı edilmeyecek bir noktadır. Bu odalar daima kilitli ya da manyetik kartlı olmalı ve güvenliğinden sorumlu insanların gözetiminde olmalıdır. Ayrıca bu odalar temiz tutulmalı, tozdan ve nemden korunmalıdır. Güvenliği tam olarak sağlanmamış bir sistem odasına yapılabilecek en basit ve etkili saldırı şöyle özetlenebilir. Sistem odasında bulunan bir veritabanı sunucu şifre ile korunmuş bile olsa, içeri girmeyi başaran yetkisiz bir kişi, bilgisayarı kapatıp elinde bulunan araçlarla sistemi tekrar açmak yoluyla bu sunucudaki bilgileri çalabilir ya da bilgisayarı kullanılamaz duruma getirebilir.

İşletim Sistemleri Güvenlik Mekanizmaları

Bu bölümde ürün ve markadan bağımsız olarak işletim sistemlerinde bulunması gereken teorik ve pratik güvenlik mekanizmaları açıklanmıştır. İşletim sisteminin güvenliğinin artırılması için, burada belirtilen önlemlerin yanında birçok ek önlem sıralanması da mümkündür. Güvenilir bir işletim sisteminde uygulamaya geçirilmiş olması gereken 4 ana prensip bulunmaktadır. Aşağıda açıklanan bu 4 ana prensip ideal olarak işletim sistemlerinde bulunmalıdır fakat her işletim sisteminde güvenlik dışındaki kullanılabilirlik, kullanıcı gerekleri, pazar payının korunması, maliyet gibi sebeplerden dolayı bu prensipler farklı şekilde yorumlanmış ve tam olarak uygulanmamış olabilir. Ana prensipleri yerine getirmek amacıyla pratik olarak günümüz çok kullanıcılı işletim sistemlerinde uygulamaya geçirilmiş güvenlik mekanizmaları da yine aşağıda açıklanmıştır.

Güvenilir İşletim Sistemi Prensipleri

Burada açıklanan 4 ana prensip, uygulamaya geçirildiğinde daha fazla başlık altında incelenebilir. Ayrıca uygulama seviyesinde alınabilecek bazı pratik güvenlik önlemlerini kapsamamaktadır. Pratik güvenlik önlemleri sonraki bölümlerde anlatılmıştır.

Bilgilerin Bölmelere Ayrılması

Sistemde saklanan bilgilere erişim, erişim niyetinde bulunan kullanıcının genel olarak sistem üzerindeki ayrıcalığından etkilenmeyecek şekilde kısıtlanabilmelidir. Bu sayede sistem yöneticisi dahil tüm kullanıcıların bir kaynağa ya da bilgiye ulaşırken eğer gerçekten erişim hakkı var ise erişebilmesi sağlanır ve erişimine izin verilmemiş bilgilere sahip olması engellenir. Ayrıca bir uygulamanın başka bir uygulamaya erişim sağlamak amacıyla sıçrama noktası olarak kullanması engellenir.

Rollerin Bölmelere Ayrılması

Sistem üzerindeki hiçbir kullanıcı, sistemde mümkün olan tüm işlemleri yapabilecek erişim haklarına sahip olmamalıdır. Bir sistem yönetim komut satırına erişim olsa bile tüm sistemin kontrolünün buradan yapılması mümkün olmamalıdır. Kullanıcı silinmesi, kullanıcı şifre değiştirilmesi, aygıt eklenmesi, sistemin yeniden başlatılması gibi kritik işlemler gerçekleştirilmeden önce en az iki kullanıcının onayının alınması,

saldırgan tarafından ele geçirilmiş bir kullanıcı hesabının kullanılmasıyla meydana gelebilecek zararları da azaltabilir. Bu mümkün değilse ilave onay mekanizmaları kullanılmalıdır.

En Az Erişim Hakkı

İşletim sistemleri prosesleri ve kullanıcılar, sadece ihtiyaç duydukları işlemleri yerine getirebilecek erişim haklarına sahip olmalıdırlar. Mesela bir e-posta sunucusu, sistem yöneticisi kullanıcı ile çalışıyor olsa bile web servisi dosyalarını değiştirememelidir. Benzer şekilde herhangi bir sistem kullanıcısı iş tanımında bulunan işlemler dışındaki işlemleri yapabilecek erişim haklarına sahip olmamalıdır.

Çekirdek Seviyesinde Yürütme

Güvenlik mekanizmaları, kullanıcı seviyesinde yapılacak herhangi bir müdahale ile etkilenemeyecek sistem seviyesinde uygulanmalıdır. Ayrıca kontrol edilmek istenen uygulamaya mümkün olan en yakın seviyeden güvenliğin zorlanması en garanti yoldur. İşletim sistemi çekirdeği seviyesinde güvenlik mekanizmalarının zorlanması, verilecek erişim kararlarına kullanıcıların müdahale edememesini ve uygulamaya doğrudan uygulanabilmesini mümkün kılar.

İşletim Sistemlerinde Uygulanan Güvenlik Mekanizmaları

Günümüz çok kullanıcılı işletim sistemlerinde genel olarak uygulanan güvenlik mekanizmaları tanıtılmıştır.

Kullanıcı Tanıma ve Kimlik Doğrulama

Kullanıcı Tanıma, herhangi bir sistem kaynağına erişim isteği yapılacağı zaman erişim niyetinde bulunan kullanıcının kendisini sisteme tanıtmak için kullandığı bir kullanıcı bilgisinin sisteme tanıtılmasıdır. Çoğu çok kullanıcılı işletim sisteminde kullanıcılar tarafından bilinen kullanıcı isimleri ve bu kullanıcı isimlerine karşılık düşen ve sistemde tek olan kullanıcı bilgisi numarası (SID) bulunmaktadır. Kullanıcı Tanıma bilgisi, Kimlik Doğrulama sırasında kullanılmaktadır.

Kimlik Doğrulama, Kullanıcı Tanıma safhasında öğrenilen kullanıcının gerçekten o kullanıcı olduğunun kabul edilmesinden önce yapılan kontrol işlemleridir. İşletim sistemlerinde kullanılan kimlik doğrulama metotlarının ayrıntılı olarak incelenmesi bu makalenin kapsamı dışında olmakla beraber mevcut kimlik doğrulama mekanizmalarına, Temel Kimlik Doğrulama (sadece kullanıcı tarafından bilindiği varsayılan şifrenin kontrol edilmesi), Kerberos gibi örnekler verilebilir.

Bir kullanıcıya sisteme erişim hakkı verilmeden önceki güvenlik giriş fonksiyonu olması dolayısıyla kimlik doğrulama işlemi büyük önem taşımaktadır. İşletim sistemi tarafından yapılan kimlik doğrulamaya güvenen birçok uygulama da aynı şekilde işletim sistemi kimlik doğrulama mekanizmasının sağladığı çerçevede güvenli sayılabilir. Kullanıcı şifrelerinin minimum uzunluğu, karmaşıklık gereksinimleri, değiştirme süresi gibi özellikleri, belirli sayıda yanlış şifre girilmesi durumunda kullanıcı hesabının bir süre için veya sistem yöneticisi onaylayana kadar devre dışı bırakılması gibi güvenlik politikalarının sistem genelinde zorlanabilmesi, kullanılan kimlik doğrulama işleminin güvenliğinin ve etkinliğinin artırılması için büyük önem taşımaktadır. Kullanıcı şifre bilgilerinin güvenli bir şekilde sistemde saklanması ve korunabilmesi de kimlik doğrulama mekanizmasının güvenilir olması için şarttır.

Güvenliği sadece kullanıcı şifresinin bilinmesi veya bazı kriptografik işlemlere bağlı olan kimlik doğrulama mekanizmaları, kritik kontrol gerektiren birçok sistemde yeterli olmayacaktır. Bu ihtiyaçtan dolayı "Güçlü Kimlik Doğrulama" kavramı gelişmiştir. Güçlü Kimlik Doğrulama mekanizmalarında aşağıda belirtilen üç ana prensipten en az iki tanesinin kimlik doğrulama mekanizması içerisinde kullanılması gerekmektedir.

1. Bildiğiniz bir şey (Şifre, PIN vb.)

2. Sahip olduğunuz bir şey (Akıllı Kart, Manyetik Kart, Anahtar vb.)

3. Fiziksel karakteristiğinizi yansıtan biyometrik bir özellik (Parmak İzi, Avuç içi izi, Retina İzi, Ses, İmza vb.)

Yetkilendirme

Yetkilendirme Mekanizması, bir sistemdeki kullanıcıların niyet ettikleri işlemleri gerçekleştirebilmesi için gerekli erişim haklarının verilmesini sağlar. Yetkilendirme işlemi güvenilir bir Kimlik Doğrulama mekanizmasına ihtiyaç duyar. Örnek olarak UNIX işletim sisteminde yetkilendirme iki kullanıcı sınıfına ayrılmıştır. Root kullanıcılar(sistem yöneticileri) sistemde hemen hemen tüm işleri yerine getirebilecek yetkilere sahip iken normal kullanıcılar sistemdeki program ve bilgilere daha kısıtlı bir erişim sağlayacak şekilde yetkilendirilmişlerdir.

Erişim Kontrolü

Bir öznenin (aktif bir kullanıcı veya proses) sistem üzerinde bir nesneye (dosya gibi pasif varlıklar) erişiminin kontrolü, sistemde erişim kontrol kurallarının belirlenip uygulanmasıyla mümkündür. Erişim kontrolü yapılmadan önce Yetkilendirme mekanizmalarında olduğu gibi güvenilir bir Kimlik Doğrulama mekanizmasının bulunması ve erişim isteğini yapan kullanıcının kimliğinin doğrulanmış olması gerekmektedir. Erişim Kontrolü Sistemleri, sistem ihtiyaçlarına bağlı olarak üç ana modelden biri baz alınarak gerçeklenebilir.

Zorunlu Kimlik Doğrulama

Bir öznenin herhangi bir sistem nesnesine erişimi sırasında karar verilirken göz önünde bulundurulan karakteristikler, nesnenin sınıfı ve hassasiyet seviyesi ile erişim isteğinde bulunan öznenin güvenlik kleransıdır. Eğer bir öznenin sahip olduğu güvenlik kleransı erişmek istediği nesnenin güvenlik etiketi için yeterli ise erişim başarılı olur. Aksi takdirde erişim engellenir. Ayrıca kimi sistemlerde kullanıcının güvenlik kleransı nesneye erişim için yeterli olsa bile "Bilmesi Gereken" prensibince erişim engellenebilir.

İsteğe Bağlı Kimlik Doğrulama

İsteğe bağlı kimlik doğrulama mekanizmalarında, bir nesne üzerinde hangi öznelerin hangi erişim haklarına sahip oldukları belirtilir. Erişim Kontrol Listeleri isteğe bağlı kimlik doğrulama bilgilerini taşır. Erişim kontrol listeleri bir nesneye özel olarak düzenlenebilir ve o nesneye üzerinde hangi öznelerin (aktif kullanıcı veya prosesler) gerçekleştirebilecekleri işlemleri tanımlar.

İsteğe Bağlı Olmayan Kimlik Doğrulama

İsteğe bağlı olmayan kimlik doğrulama mekanizmalarında merkezi bir otorite sistem gereksinimleri ve organizasyonel politikalara bağlı kalarak sistem nesneleri üzerinde belirlenmiş öznelere erişim hakları tanımlar. İsteğe bağlı kimlik doğrulama mekanizmalarından farkı ise, nesnelere erişim hakları düzenlenirken tek tek kullanıcılar yerine belirli bir görevi yerine getiren veya belirli bir rolü üstlenen kullanıcı profiline erişim hakkı verilmesidir. Bu sayede sık sık kullanıcıların değiştiği bir sistemde erişim kontrol listelerinin tekrardan düzenlenmesi gereği ortadan kalkmaktadır.

Denetim/Yönetilebilirlik

Çoğu işletim sisteminde uygulamaya geçirilmiş olan denetleme mekanizması, sistem kullanıcılarının sistem üzerinde yaptıkları işlemlerin kayıtlarını tutar. Kayıt dosyalarının boyutlarının hızlı şekilde büyümesi ve kayıt tutma işleminden dolayı performansın olumsuz yönde etkilenmesi dolayısıyla denetleme politikaları iyi belirlenmelidir. Sadece ilgili işlemlerin güvenlik kayıtları tutulmalı ve güvenlik kayıtları düzenli olarak incelenmelidir. İşletim sistemleri denetleme kayıtlarının değerlendirilmesi ve filtrelenebilmesi için genel olarak üçüncü parti yazılımlara ihtiyaç duyulmaktadır.

Nesnelerin Tekrar Kullanımı

Güvenli bir işletim sisteminin, yeni oluşturulmuş bir sistem nesnesinin (bellek, taşıyıcı bellek, dosya vb.) daha önceki kullanımından kalan bilgiler taşımadığını garanti etmesi gerekmektedir. Nesnelerin tekrar kullanımı, kullanıcılara tahsis edilecek yeni nesnelerin tahsis edilmeden önce temizlenmesi veya üzerinden bilgi edinilmeyecek şekilde ilklendirilmesini gerektirir.

Saldırılara Dayanıklılık

Tüm güvenlik önlemleri alınmış olsa dahi bir işletim sistemi, açıklıklarından veya zayıflıklarından kaynaklanabilecek saldırılara karşı dayanıklı olacak şekilde tasarlanıp derlenmiş olmalıdır.

Saldırı Tespit

İşletim sistemi üzerinde bulunan kritik bilgi ve sistemlerin devamlı olarak izlenmesi ve yetkili ya da yetkisiz kullanıcılar tarafından gerçekleştirilen normal dışı aktivitelerin tespit edilmesi amacıyla saldırı tespit mekanizmasının bulunması gerekmektedir. Saldırı tespit algılayıcıları sistem üzerindeki olayları takip edebileceği gibi ağ trafiğin dinleyip ağ üzerindeki zararlı aktiviteleri tespit etmek amacıyla da kullanılabilir.

Sistem Sıkılaştırma

İşletim sistemleri genellikle son kullanım ortamı için gerekli olmayan servis ve fonksiyonlar çalışır halde kurulurlar. Sistem sıkılaştırılması, işletim sistemi üzerindeki gereksiz servislerin durdurulup devre dışı bırakılması, işletim sisteminin minimum özellikler ile konfigüre edilmesi, kullanıcıların ve uygulamaların sadece çekirdek görevin yerine getirilebilmesine yetecek şekilde düzenlenmesi gibi işlemleri içerir. Ayrıca hizmet verilen servisler dışındaki servislerin portlarının kapatılması ve sistem/güvenlik kritik tüm yamaların uygulanması gerekmektedir. Hiçbir işletim sistemi ilk çıktığı haliyle güvenli kalamaz. İşletim sistemi geliştiricileri ve kullanıcılar tarafından bulunan zayıflık ve açıklıkların kapatılabilmesi için yamalar çıkarılır. Bu yamalar kullanılarak kapatılan açıklıklar kimi durumlarda oldukça ciddi zararlara sebep olabilecek açıklıklar olabilirler. Bu sebepten dolayı sistem yamaları düzenli şekilde takip edilmeli ve test ortamında denendikten sonra en hızlı şekilde sistem güncellenmelidir.

Güvenlik Garanti Seviyesi

Yukarıdaki bölümlerde anlatılanlar genel olarak işletim sistemlerinde alınabilecek güvenlik mekanizmalarıydı. Bu güvenlik mekanizmalarının gerçekten de işletim sistemi geliştiricileri tarafından iddia edildiği şekilde çalıştığının ispatlanması da kullanıcı ihtiyaçlarının karşılanacağının garanti edilmesi açısından oldukça önemlidir. Güvenlik garanti seviyesinin belirlenebilmesi için iki farklı metot izlenebilir. Bunlardan birincisi, işletim sistemi geliştiricisinin gerekli gördüğü testleri uygulaması ve sonuçlarının yayınlamasıdır. İkinci çözüm ise, tarafsız bir test laboratuarının işletim sisteminin testlerini yaparak güvenlik garanti seviyesini belirlemesidir. Güvenilir ve objektif olması açısından tarafsız bir test laboratuarının güvenlik garanti seviyesi için önceden belirlenmiş ve kabul edilmiş kriterleri göz önünde

bulundurarak testleri yapması daha kabul edilebilir bir durumdur. Bu ihtiyacı karşılamak üzere Amerika Birleşik Devletleri TCSEC isimli standardı, Avrupa Birliği ise ITSEC isimli standardı yayınlamıştır. Fakat günümüzde bu standartlardan daha geniş kapsamlı olarak hazırlanmış ve aynı amaca uygun olarak uluslararası kullanılması amaçlanan Common Criteria - ISO 15408 (Ortak Kriterler) standardı mevcuttur.

Ortak Kriterler'e uygun olarak değerlendirmesi yapılacak ürünün güvenlik hedefi dokümanında (ST-Security Target) belirtilen güvenlik fonksiyonlarının yerine getirilip getirilmediği ve gerekli dokümantasyonun hazırlanıp hazırlanmadığı kontrol edilir. Güvenlik hedefi dokümanları, değerlendirilecek ürün profiline uygun Koruma Profili (PP-Protection Profile) baz alınarak hazırlanır. Ortak Kriterler değerlendirmelerinin nasıl yapıldığı bu makalenin amaç ve kapsamı dışında kalacak kadar detay içermektedir. Bir ürün için alınabilecek Ortak Kriterler sertifikası, değerlendirmeyi gerçekleştiren laboratuarın en yüksek sertifikasyon makamı (CB-Certification Body) onayına sahiptir ve Ortak Kriterler standardını kabul etmiş diğer ülkeler bu sertifikayı kabul ederler. Ortak Kriterler Güvenlik Garanti Seviyeleri (EAL - Evaluation Assurance Level) 1 ile 7 arasında numaralandırılır ve her EAL değerinin gerektirdiği minimum güvenlik gereksinimleri ISO 15408 standartlarında ayrıntılı şekilde açıklanmıştır. Günümüze kadar işletim sistemleri için en yüksek EAL5+ güvence seviyesinde Ortak Kriterler değerlendirmesi gerçekleşmiştir. Bugüne kadar Ortak Kriterler sertifikası alan işletim sistemleri ve güvenlik garanti seviyeleri hakkında en güncel bilgi **http://www.commoncriteriaportal.org/products_OS.html#OS** linkinden edinilebilir.

Sonuç

Bilgisayar İşletim Sistemleri güvenliğinin sağlanması, işletim sistemi bünyesindeki güvenlik mekanizmalarının kullanılmasının yanında sistem sıkılaştırmasının amaca uygun şekilde yapılması, yama yönetiminin yapılması, sistem yöneticisi ve sistem kullanıcılarında güvenlik bilincinin gelişmiş olması, güvenlik mekanizmalarını destekleyecek üçüncü parti yazılımların etkin olarak kullanılması ve sistem genelinde güvenlik politikalarının belirlenip ciddi şekilde uygulanması gibi gerekliliklerin yerine getirilmesiyle mümkündür. Tüm bu gerekler yerine getirilmiş olsa dahi hiçbir işletim sistemi %100 güvenli hale getirilemez ve %100 güvenliğin sağlanmış olduğu iddia edilemez. Önemli olan mevcutta bilinen risklerin sistem gereklerine ve maliyet kısıtlarına uygun şekilde en aza indirilmesi ve sistem risklerinin sürekli olarak izlenerek güvenlik seviyesinin korunmasıdır.

Referanslar

[1] Bilge Karabacak, "Kerberos", IT Security Magazine, Eylül 2002

[2] HP-UX Security White Paper, 2001

[3] Vijai Gandikota, "Securing Operating Systems", 6 Mayıs 2002

[4] Ronald L. Krutz, "The CISSP Prep Guide", 2003

[5] PitBull .comPack White Paper, 2001

[6] ISO 15408 - Common Criteria Standart

[7] US DoD 5200.28-STD, TCSEC Standart