SİSTEM VE AĞ YÖNETİMİNDE PAROLA YÖNETİM ZORLUKLARI

Hüseyin Temuçin*, Kerem ERZURUMLU*

(*) Hacettepe Üniversitesi Bilgisayar Mühendisliği Bölümü, 06532, ANKARA

htemucin@cs.hacettepe.edu.tr, kerem@linux.org.tr

ÖZET

Bu belge ile, Sistem ve Ağ Yönetiminde parola yönetimi ve parola yönetimininde karşılaşılan problemler ele alınacaktır.
Bu bağlamda, belgede genel olarak parola yönetimi, parolaların sistem ve ağ yönetiminde ki kullanımları anlatılacak, daha sonra parola yönetim sistemleri kapsamında personel değişimleri ve kurum içi veya kurum dışı parola dağıtımı gibi durumlarda ortaya çıkan problemler incelenecektir.

Anahtar Kelimeler

Parola Yönetimi, Sistem ve Ağ Yönetimi, Parola Yönetim Problemleri, Merkezi Parola Yönetimi

SUMMARY

In this paper, password management problems of network and system management will be handled. In this concept, password management and its usage in systems and networks will be introduced in the paper. Then password management problems that occurs in such situations like personnel changing and internal or external password distribution will be investigated. In this paper the determination of password management problems will be done and these problems will be introduced.

Keywords

Password Management, System and Network Management, Problems of password management, Centralized Password Management

GİRİŞ

Bir kuruma ait sistem ve ağın, kurum içi ve/veya kurum dışındaki yetkisiz kişilerden ve yazılımlardan korunması için, donanımsal ve yazılımsal güvenlik önlemlerinin alınması gerekir. Sistem ve ağ yönetimlerinde; sisteme, sistem sunucularına, sistem içindeki veritabanı yönetim sistemlerine veya ağ içindeki bir yönetilebilir bir aktif aygıta bir kullanıcının kendisine atanmış yetkilerle giriş yapması ve bu bağlamda yetkisiz veya art niyetli kullanıcıların giriş yapmalarının engellenmesi kullanıcı yetkilendirmeleri olarak tanımlanır. Kurumlarda kullanıcı yetkilendirmeleri kullanıcılara ve kullanıcı gruplarına atanmış parolalar ile sağlanır. Farklı mimariye sahip işletim sistemlerine sahip sistemlerdeki farklı yetkilere sahip kullanıcıların parolaları, her mimarinin kendine özgü geliştirmiş olduğu parola yönetim yazılımları tarafından yönetilir.

Parola yönetim yazılımları, işletim sistemi tarafından, giriş işlemlerinde güvenliği sağlanması ve sistem içinde tanımlı parolaların güvenli bir biçimde saklanması için görevlendirilmiştir. Parola yönetim yazılımı,

- Sistem parolalarını periyodik olarak, yeni değerlerle değiştirmek.
- Sakladığı parola değerlerini korumak (şifreleme, tekrarlı saklama gibi).
- Bu parolaları, IT yöneticileri, hizmet uygulamaları ve diğer uygulamalara bağlanan uygulamalara açmak.

hizmetlerini verir [1].

Unix ve Linux ailesine ait işletim sistemlerinde, *root* kullanıcısı, Microsoft Windows ailesi işletim sistemlerinde ise *administrator* kullanıcısı, ayrıcalıklı ve sistem içinde tam yetkili, her türlü eylemi bir kısıtlama / sınırlama olmadan

gerçekleştirebilen bir kullanıcılardır ve bu tür kullanıcılar "Süper Kullanıcı" (*ing. Super User*) olarak anılır. Benzer bir şekilde, veritabanı sunucularında da tam yetkili, her türlü eylemi bir kısıtlama / sınırlama olmadan gerçekleştirebilen "Veritabanı Yöneticisi" (sysdba, sa gibi; *ing. Database Administrator*) kullanıcılar mevcuttur. Genel olarak, yukarıda özellikle bahsi geçen sistemler haricinde kalan işletim sistemleri, veritabanı sistemleri, uygulamalar ve ağ aygıtları bir süper kullanıcı girişi içerir. Bu girişi yapan kullanıcı yazılım yükleme, sistem veya aygıt ayarlarını değiştirmek, kullanıcıları yönetmek, güncellemeleri uygulamak gibi yetkilere sınırsız ve çoğu zaman denetimsiz olarak sahip olur[1].

PAROLA YÖNETİM ZORLUKLARI

Daha önce belirtildiği üzere sistemde, sistem içindeki sunuculara, veritabanı sistemlerinde ve ağ cihazlarında süper kullanıcı girişi yapan kullanıcı tam yetkilidir. Kurum içinde, sistem ve ağ yönetim rutinleri, hata ayıklama gerektiren aykırı durumlar, güncelleme ve sürüm yükseltme işlemleri birçok kullanıcının ve yazılım hizmetinin (BT yöneticileri, sistem yöneticileri vb.) bu yetkiyle sistemlere giriş yapma hakkına sahip olmasını gerektirir. Fakat, sistem devamlılığı için gereken bu yetkilendirme, birtakım parola yönetim zorluklarını da beraber getirir. Belgenin takip eden kesimlerinde, bu problemler başlıklar altında ele alınacaktır.

Sistem içinde tanımlı sistem yöneticileri, sistemin doğru ve devamlı bir şekilde çalışması için ağ, donanım bileşenleri, bu bileşenler üzerinde çalışan hizmet programları gibi yazılım, donanım bileşenlerinden ve sistem içinde tanımlı kullanıcıların yönetiminden sorumludurlar. Bu görevlerin yerine getirilmesi, sistem yöneticilerine süper kullanıcı yetkilerinin verilmesini gerektirir.

Sistem yöneticilerine iki farklı yöntem ile süper kullanıcı yetkisi verilmektedir. Bu yöntemlerden ilki süper kullanıcı parolasının yüm sistem yöneticileri arasında "paylaşılması"dır. Süper kullanıcı şifresini, sistem yönetimi yetkisine sahip tüm kullanıcılar bilir ve yönetim işlemleri sırasında bu kullanıcı adı/parola ikilisini kullanır.

Diğer yöntem ise Unix ailesi işletim sistemlerindeki "*sudo*", windows ailesi işletim sisteminde ise "*kullanıcı yetkilendirme*"sidir. Temel olarak bu yöntemde sistem yöneticilerinin tamamının kendilerine ait bir kullanıcı adı/parola ikilisi vardır. Bu ikililer tüm yönetimi yapılan sistemlerde tanımlanır ve süper kullanıcı bu kullanıcıların teker teker hangi işlemleri yapabileceğini her sisteme ayrı ayrı olmak üzere tanımlar. Bu şekilde süper kullanıcıların parolaları paylaşılmamış olup, sistem yönetim işlemleri devam edebilmektedir.

PERSONEL DEĞİŞİKLİKLERİ

Genel olarak kurumların Bilgi İşlem Merkezleri'nde sistem ve ağ yönetim işlemleri tek bir kişi tarafından değil, bir ekip tarafından gerçekleştirilmektedir. Bahsi geçen ekip çalışması başlangıçta kişiler arası görev dağılımı ve kurum devamlılığı açısından bir avantajdır. Fakat bu avantaj durumu, ekipten bir kişinin işten ayrılması, görevine son verilmesi veya başka gruba atanması gibi durumlarda çözümlenmesi gereken bir takım zorluklar ve zorunluluklar içeren probleme dönüşmektedir. Bahsi geçen kullanıcıların başka bir göreve atanması, yada daha da önemlisi kurumdan kendi isteği ya da kurum isteği ile ayrılması durumunda, sistemin güvenliği ve devamlılığı için bu kullanıcılardan süper kullanıcı yetkilerinin alınmasını zorunlu kılar.

Eğer süper kullanıcı yetkileri parola paylaşım esasında dağıtılmış ise, kullanıcıdan yetkilerin alınması süper kullanıcı parolasının kullanıcıyla paylaşımına son verilmesine, yani ilgili parolaların kullanılmakta olan tüm sunucu işletim sistemleri, veritabanı sistemleri, aktif ağ cihazlarında değiştirilmesine eşdeğer olacaktır. Benzer şekilde, ayrılan personelin sistemler üzerinde bir "*arka kapı*" bırakıp bırakmadığı kontrolü de yapılması gereken bir kontroldür. Süper kullanıcı parolasının root parolasının değiştirilmesinin yapılma amacı ayrılan kullanıcının süper kullanıcı girişini engellemek olduğu için, yeni atanan parolanın ayrılan kullanıcının bilemeyeceği, tahmin edemeyeceği bir parola olması gerekir. Bu bağlamda yeni oluşturulmuş olan parolanın dağıtılması ve sistem yöneticilerinin bu parolayı "ezberlemesi" ise başlı başına başka bir problemdir. Bu problem sistem yönetimi ekibine yeni kişiler katıldığında da yaşanmaktadır.

Eğer süper kullanıcı yetkileri kullanıcı yetkilendirme esasına göre yapıldı ise, kullanıcıdan yetkilerinin alınması, kullanılmakta olan tüm sunucu işletim sistemleri, veritabanı sistemleri, aktif ağ cihazlarında kullanıcının yetkilerinin alınması ve personel kullanıcı adının silinmesini gerektirecektir. Benzer şekilde sistem yönetimi ekibine yeni bir kişi katıldığında bu kullanıcı için tüm sistem ve cihazlarda kullanıcı adı/parolası atanması gerekmektedir.

Yukarıda bahsedilen durumlar her ne koşulda olursa olsun, bir personel değişikliği durumunda, kurum sistem ve ağında yönetilmekte olan tüm donanım ve yazılımlara müdahaleyi zorunlu kılar ve bu "toplu güncelleme" işlemi sırasında hata ile

unutulabilecek/atlanabilecek bir sistem hem güvenlik riski oluşturacak, hemde ilerleyen zamanlarda süper kullanıcı parolalarının karıştırılması gibi sonuçlar doğurabilecektir.

Dolayısı ile her kurumsal ve kurum içi personel değişikliklerinde yapılmasını gereken değişiklikler sistem yöneticilerine ve parola yönetim sistemine ciddi bir ek yük getirmektedir. Bu rutin işlemin bir çok kere tekrarlanması durumunda oluşabilecek olan unutma/atlama hataları yığmalı toplama şeklinde birikecek ve birgün (genellikle en kritik anda) kendini gösterecektir. Bu problem daha çok arıza gösteren sisteme parolası güncellenmediği için giriş yapamama şeklinde olacak ve sistem yöneticileri ilgili sistemin eski parolasını hatırlamaya çalışacaktır.

HATA BULMA ZORLUKLARI

Sistem, veritabanı sistemi ve ağ bileşenlerinde, her sistemde olduğu gibi, er ya da geç, donanımsal sıkıntılar yaşanmadığı durumlarda dahi, hataların ve aykırı durumların oluşacağı aşikardır. Sistem ve ağ bileşenlerinin yönetiminden ve oluşan sorunların giderilmesinden süper kullanıcı sorumlu olduğu için, son haliyle çalışan kararlı bir sistemde bir hata meydana geldiğinde, hata donanımsal olmadığı sürece, bu hatanın bir süper kullanıcı hatası olduğu açıktır. Bu hata süper kullanıcı yetkisine sahip yönetici tarafından kasten ya da kaza ile (yapılan bir işlemin yan etkisi gibi) yapılabilir. Fakat parola paylaşım yöntemi ile yetkinin dağıtıldığı durumlarda, yetkili kullanıcı grubunun bütün üyeleri sisteme aynı süper kullanıcı adı ve parolası ile giriş yaparlar. Bu bağlamda sistem, veritabanı veya ağ bileşenlerinden herhangi birinde istenilen dışında bir durum oluştuğunda, hatanın giderilmesi için geriye dönük çalışma yapılmak istenildiğinde, hataya sebep olan değişiklikleri hangi kullanıcının yaptığını bulmak zorlaşır. Çünkü sistem ve ağ raporlarında oturum geçmişlerinde her zaman aynı süper kullanıcı görünecektir. Yani değişikliği yapan hatalı kullancı olarak bir kullancıyı değil bir kullanıcı grubunu işaret edecektir.

Bu durum arzu edilmeyen bir durumdur ve son oturumu açıp değişkliği yapan kullanıcı bulmak için insan kaynaklı araştırmalar yapmaktan başka bir yol kalmaz.

DIŞ KAYNAK KULLANIMI DURUMU

Bilindiği üzere kurumlar işlerini yürütmek, raporlama işlemlerini gerçekleştirmek ve geçmiş kayıtlarını tutmak, birimler ve birimlerin hizmet sunucularıyla ve dış ağlarla iletişimlerini sağlamak gibi ihtiyaçlarını karşılamak için çeşitli yazılımsal, donanımsal ve ağ bileşenlere ihtiyaç duyarlar. Yazılımların “yaşayan varlıklar” olması dolayısı ile zaman içerisinde bakım ve yenileme hizmetlerine ihtiyaç duyması kaçınılmazdır. Benzer şekilde kurumun barındırmakta olduğu donanımsal cihazlar (sunucu sistemler ve ağ cihazları) da benzer şekilde rutin bakım işlemlerine ihtiyaç duyar.

Bu bileşenlerden, kuruma hizmet veren yazılımların yenilenmesi ihtiyacı durumunda, kurum kendi içinde barındırdığı yazılım geliştirme birimini kullanabilir. Fakat kurum içinde böyle bir birime ihtiyaç duyulmaması veya bu birimin istenilen yeni yazılım gereksinimlerini karşılayacak yazılımı geliştirecek kapasitede olmaması durumlarında, kurum istenilen yazılımı kurum dışından bir yazılım şirketine “dış kaynak kullanımı” (*ing. Out-Source*) yolu ile yaptırma yoluna gidecektir.

Benzer şekilde kurum elinde yeterli sayıda ya da yeterlilikte personel barındıramıyorsa, ağ ve sistem yönetimi işlemlerini de dış kaynak kullanımı yolu ile destek almayı tercih edebilir.

Kurum'un dış kaynak kullanması durumunda dış kaynağı sağlayan kişi ya da kurumların sistem, ağ ve veritabanı gibi yönetimi yapılmakta olan sistemlere süper kullanıcı yetkileri dahilinde erişebilmesi gerekmektedir. Bu durum birtakım problemleri beraberinde getirmekdir. Öncelikle sistemin en kritik kaynaklarına tam yetkiyle erişim hakkına sahip süper kullanıcı yetkisinin kurum dışı bir şirketle paylaşılması ve yazılım geliştirme sürecinde bu erişimlerin sürekli kontrolünü gerektirir. Yazılım geliştirme ve mevcut yazılımlar üzerinde güncelleme işlemlerinin yapıldığı sürecin sonunda ise süper kullanıcı parolalarının değiştirilmesini ve bu rutinin her yazılım geliştirme / günleme işlemlerinin sonunda gerçekleştirilmesi gerekir.

Yazılımı geliştiren kurumun, geliştirdiği yazılımı geliştirme ile birlikte söz konusu yazılımın yürütülmesinden de sorumlu olduğu durumda, süper kullanıcı parolasının yönetimi daha zor bir durum alır. Çünkü kurumun süper kullanıcı yetkilerini paylaştığı yazılım şirketinden süper kullanıcı yetkili kullanıcılardan herhangi birinin, örneğin veritabanında, yaptığı değişikliğin sebep olacağı aykırı durumda, bu şirket kullanıcıları da hata bulma durumunda sorgulanacak kullanıcı grubuna dahil olur. Bununla birlikte, yazılım şirketinde kurum için geliştirilen yazılım projesinin içinde bulunan ve kurumun yetkili kullanıcı parolarına sahip personellerinden birinin ayrılması durumunda, tıpkı kurum içi ayrılmalar durumunda olduğu gibi, kurum güvenliğini tehditlerden ötürü parola değişim prosedürünün uygulanması gerektirir. Dolayısıyla kuruma ait yazılım projesinde çalışan personelin de takibinin parola yönetimiyle yetkili birim tarafından yapılmalıdır.

UYGULAMA GÖMÜLÜ PAROLALAR

Kurumlar, geçmişten gelen alışkanlıklarını korumak ve rutin gerçekleşen bazı işlemler için (maaş bordrosu oluşturmak, yedek almak gibi) düzenli çalışan görevleri kullanmaktadır. Bu görevler ise çalışmaları sırasında sistemde bulunan veritabanı sunucuları gibi kaynaklara bir kullanıcı adı/parolası ile bağlanır.

Normal koşullar altında bu kullanıcı adı/parolası çiftinin hiç değişmemesi gerekmektedir. Fakat kurum içerisinde yaşanabilecek göç, yeniden planlama, güncelleme işlemleri sırasında bu kullanıcı adı/parolası çiftine "istenmeden" zarar verilebilir. Bu şekilde bir zarar oluşması durumunda düzenli çalışması gereken görevler işlerini doğru yapamaz ve iş gücü kaybına neden olurlar.

SONUÇ

Yukarıda bahsi geçen kavramlar bağlamında, süper kullanıcıların parolaların yönetimi, kurum büyüklüğünden, sunucu parkından ve aktif cihazlarından bağımsız olarak gereklidir. Bir kurum için kullanılması gereken merkezi süper kullanıcı parola yönetim yazılımından aşağıdaki özellikleri göstermesini beklemek bu bağlamda anlamlı olacaktır;

- İşletim sistemleri ile uyumlu,
- Ağ cihazları ile uyumlu,
- Veritabanı yönetim sistemleri ile uyumlu,
- Tüm süper kullanıcı parolalarını kendi üzerinde toplayacak,
- Bir sistem yöneticisi talep ettiğinde ilgili sistem için tek seferlik kullanım parolası oluşturacak,
- Oluşturduğu parolaların zaman tabanlı olarak işletibilecek,
- Parola oluşturma sürecini, kullanıcı ve sunucu başına modelleyerek, yönetici onaylı ve onaysız olarak yapabilecek,
- Parola oluşturma zamanlarını ve hangi kullanıcıya oluşturduğu bilgisini barındıracak,
- Düzenli olarak yönetmekte olduğu tüm sistemlerin süper kullanıcı parolalarını değiştirecek,
- Aykırı durumlar için mevcut parolaların bir çıktısını yanlızca yöneticiye verebilecek,
- Eğitilebilir olacak (yönetimini bilmediği cihazlar için eğitilebilecek ve o cihazları da yönetecek),
- Programanabilir arayüzü (API) olacak ve düzenli çalışan görevler içinde tek seferlik parola üretebilecek,
- Sistemlere bağlanabilmek için kendisinden alınan parolayı şart koşan,
- Bir sistem yöneticisinin hesabının pasif edilmesi durumunda yöneticinin tüm yetkilerini elinden alan,

Yukarıda bashi geçen özellikleri barındırmakta olan bir merkezi süper kullanıcı parola yönetim sisteminin sistem, ağ yöneticilerinin ve idari personellerin hayatını kolaylaştıracağı aşikardır.

KAYNAKLAR

1.http://en.wikipedia.org/wiki/Privileged_password_management

2. Password Management, Matt Bishop, Department of Mathematics and Computer Science, Dartmouth College

3. Password Management Best Practices, Hitachi ID Systems,

4. Bilgisayar İşletim Sistemleri, Ali Saatçi