Merkezi Olmayan Parolaların (Yerel Yönetici, BIOS, vs.) Yönetiminde “Güç Parolası” Yaklaşımı

Yerel yönetici, BIOS ve Disk Parolaları gibi merkezi olarak yönetilmesi zor olan parolalar için bilinen en yaygın güvenli yönetim şekli her sunucu ve istemciye ait parolanın bir listede tutulması ve bu listenin şifreli olarak saklanmasıdır. Her kullanıcı bilgisayarı için ayrı bir parola oluşturmak ve bu parolayı bir listede tutmak iş yükü gerektiren bir durumdur.

İdeal bir model olması nedeniyle bilişim altyapısını oluşturan öğelerin bir bütün halinde yönetilmesi, her kurumun uygulamak isteyebileceği bir modeldir. Ancak bu modelin pratikte tam anlamıyla hayat bulması, başta teknik kısıtların olması nedeniyle birçok açıdan zordur.

Kabul görmüş bir bilgi güvenliği pratiği olarak yerel yönetici hesaplarının adını değiştirmek güvenlik açısından olumlu bir çözümdür. Ancak her istemci ve sunucu için bunu yapmak ve kayıt altına almak pratikte zordur.

Söz konusu güvenlik olduğunda, güvenliğin uygulanabilirliği de sağlayacağı fayda kadar önemli bir konu olmaktadır. Daha uygulanabilir ve pratik çözümler ile hayata geçirilen güvenlik önlemleri, güvenlik kültürü olarak kendisini daha kolay benimsetebilir ve daha yaygın kullanılabilir.

Yerel yönetici hesapları, BIOS parolaları ve Disk şifreleme parolaları gibi her sistemde farklı olması beklenen öğelerin aynı parola ile korunuyor olması güvenlik açısından tehdit oluşturmaktadır. Yerel yönetici hesabının adı “administrator” ve parolası “Bj5!3%kU” olan bir sunucuyu ele geçiren saldırgan, bu sunucuda bulunan SAM veya SHADOW dosyasını kırmayı başarırsa diğer sistemlere de ulaşabilir. Değiştirilmemiş bir yerel yönetici hesabı adı bulundurması, Brute Force saldırılarına karşı zemin hazırlayabilir.

Bu tehditi bertaraf etmek ve uzun bir envanter listesi hazırlamaktan kaçınmak için parola ve kullanıcı hesaplarını üreten bir algoritma hazırlanabilir. Bunun için gerekli olan en önemli öğe, her sistem için sisteme özgü bir değer belirlemektir. Sunucular için bu değer IP adresleri olabilir. Sunucular statik IP yapılandırması ile hizmet verirler ve donanımları değişse bile IP adresleri çok nadir değiştirilir. Bu değer onları tanımlamak için kullanılabilir bir değerdir.

Söz konusu diğer sistemlere, kullanıcı bilgisayarlarına geldiğinde ise IP çözümü bu aşamada dinamik IP yapılandırmasının yaygın olarak kullanılması nedeniyle işe yaramayacaktır. Bu durumda fiziksel değerler kullanılabilir. Bu değerlerden biri istemcilere ait seri numarasıdır.

Örnek bir seri no:

Seri numaraları ve IP adresleri ile üretilecek parola ve kullanıcı adı değerleri için aşağıdaki gibi örnekler verilebilir. Bu örneklerde bilgisayar seri numarası olarak “KFD23”, sunucu IP adresi olarak “192.168.0.234” adresi kullanılacaktır. Ortak parola değeri “Bj5!3%kU” parolası seçilecek ve ikinci bir parola olarak “ikinci parola” adı altında “$oP8” değeri kullanılacaktır.

Yerel yönetici hesabı ve parolası üretilmesi:
Bu adımda bir sunucu için yerel yönetici hesap adı ve parolası yukarıdaki değerlerle şu şekilde oluşturulabilir:

Ortak parola değerinin tek başına bütün sistemlere kullanılması yerine değiştirilerek uygulanması adımları izlenecektir.

- İkinci parola IP adresi ile birleştirilir: **"***$oP8***192.168.0.234"**
- Oluşan değer MD5 algoritmasına sokulur → md5(*$oP8***192.168.0.234**) → **278f41**1edf83bc89a263de100280**86ae**
- Çıkan kriptografik özet (Hash) değerinin ilk 6 hanesi kullanıcı adı seçilir: **"**278f41**"**
- Çıkan kriptografik özet (Hash) değerinin son 4 hanesi güç parolası olarak seçilir: **"**86ae**"**
- Ortak parola değeri 8 hanelidir, 4'er hane olmak üzere ikiye bölünür: **"**Bj5!**" "**3%kU**"**
- Güç parolası olarak seçilen değer, ortak parolanın ortasına yerleştirilir: **"**Bj5!86ae3%kU**"**

Bu adımlardan sonra yerel yönetici hesabı için oluşturulan kullanıcı adı ve parola ikilisi aşağıdaki gibi olacaktır:

Kullanıcı adı: 278f41
Parola: Bj5!86ae3%kU

Burada kullanılan yöntemde detaylara inildiğinde yerel yönetici hesabı adının ve 12 haneden oluşan güçlü bir parolanın 2 adet sabit parola ve 1 adet değişken değerden oluştuğu görülecektir.

BIOS parolalarının üretilmesi:
Sunucularda yerel yönetici hesabı oluşturmanın aksine BIOS parolası oluşturmak daha az işlem gerektirecek bir aşama olacaktır.

- İkinci parola seri numarası ile birleştirilir: **"***$oP8***KFD23"**
- Oluşan değer MD5 algoritmasına sokulur → md5(*$oP8***KFD23**) → fff155afec3ca81bebbd242ff399**cda3**
- Çıkan kriptografik özet (Hash) değerinin son 4 hanesi BIOS parolası seçilir: **"**cda3**"**

Bu yöntemlerle oluşturulacak parolalar her sistemde aynı parolanın kullanılmasından daha fazla güvenlik sağlayacaktır. Buradaki işlemler aracı bir yazılım yardımıyla otomatik hale getirilebilir ve örneklerden bağımsız bir algoritma geliştirilerek uygulanabilir.

Yukarıda anlatılan yerel yönetici hesabı parolasının oluşturulması örneğinde temelde yapılan iş "güç parolası" adı altında bir değeri, güçlü karakter dizilerinden oluştuğu bilinen bir parolaya eklemektir. Bu işlem sırasında parolanın başı veya sonu yerine ortası seçilmiştir. Günümüzdeki Brute Force yazılımları başı ve sonu sabit olan parolalar için opsiyon sunarken birçoğu orta bir bölüm için opsiyon sunmamaktadır.

Kullanılan algoritmada MD5 yerine daha güçlü karakter dizilerinde çıktı veren kriptografik özet fonksiyonları da kullanılabilir. Böyle durumlarda son adımda kullanılan ve ortak parola adı altında seçilen değer kaldırılarak doğrudan güç parolası adı altında seçilen değeri kullanmak mümkün olabilir.

Kullanıcı bilgisayarlarında var olan parolaları değiştirmek veya olmayan parolaları aktif etmek kullanıcı sayısına oranla belli bir zaman alacaktır. Bu zaman dilimini ve iş yükünü azaltmak için tamir veya teknik nedenlerden dolayı kullanıcılardan gelen bilgisayarların güncellenerek kullanıcıya teslim edilmesi yöntemi uygulanabilir.

Gökhan Muharremoğlu
Bilgi Güvenliği Uzmanı
gokhan.muharremoglu@iosec.org