Çok Faktörlü Kimlik Doğrulaması (MFA)

MFA, siber suçluların engellenmesine yardımcı oluyor

Siber suç eylemlerinin çoğunda, bilgisayar korsanlarının kurumsal ağınıza veya e-postanıza erişim sağlaması gerekir. Tek Faktörlü Oturum Açma (SFA) olarak da bilinen geleneksel kullanıcı oturum açma ve parola erişimini kullanan siber suçlular, şirketlerin BT sistemlerine kolaylıkla erişim sağlayabiliyor.

E-postanıza erişim sağlayan bir bilgisayar korsanı, sizin kimliğinize bürünerek sahte e-postalar gönderebiliyor veya ağınıza erişim sağladığında ortamınızla ilgili bilgi edinerek yetkilerini yükseltebiliyor, yedek dosyaları silebiliyor ve fidye yazılımlar kurabiliyor.

Bu tür bilgisayar korsanlığı faaliyetleri farklı şekillerde gerçekleşebilir:

- **Deneme yanılma saldırısı** veya parola kırma aracı ile yaygın kullanılan parolaların otomatik olarak denenmesi.
- **Kimlik bilgisi toplama** veya çoğu kişinin çeşitli hesaplarda aynı kullanıcı adı ve parola kombinasyonlarını kullandığı gerçeğinden faydalanma.
- **Kimlik avı** veya parola sıfırlama talepleri içeren sahte e-postalar göndererek çalışanın iş e-postası bilgilerini ele geçirme.

İstenmeyen kişileri sistemlerinizden uzak tutmanın en etkili yollarından biri, temelde ikinci bir kimlik doğrulama/savunma katmanı sunan Çok Faktörlü Kimlik Doğrulaması (MFA) olabilir.

MFA nedir?

MFA, şirket e-postasına veya diğer önemli şirket varlıklarına erişmeye çalışan kişilerin gerçekten belirttikleri kişiler olduğundan emin olmak için iki veya daha fazla kimlik doğrulama faktörü veya kimlik kanıtı gerektirir.

Örneğin, üç katmanlı kimlik doğrulaması şu şekilde olabilir:

1. 

Bildiğiniz bir şey
(genellikle parola veya doğrulama kodu)

2. 
Sahip olduğunuz bir şey
(güvenlik anahtarı veya telefon gibi kolayca kopyalanamayacak, güvenilir bir cihaz)

3. 
Taşıdığınız bir özellik
(biyometrik veriler)

> ***İki veya daha fazla kimlik doğrulama faktörünün bir arada kullanılması bilgisayar korsanları için ciddi bir zorluk teşkil eder ve bilgilerin ele geçirilme riskini önemli ölçüde azaltır.***

MFA neden önemlidir?

MFA, siber suçlular meşru kullanıcıların bilgilerini ele geçirse dahi, söz konusu kullanıcıların sahip olduğu şeyleri de ele geçirme olasılıklarının azaltılması fikrini temel alır. E-posta hesabını ele alacak olursak; kullanıcıların sahip olduğu şey, benzersiz ve kısa süreli geçerliliğe sahip bir kod üreten veya alan bir yazılım belirteci ya da cihazdır.

MFA'nın uygulanması

MFA kullanımı, kullanıcı kimliklerinin korunmasına ilişkin en hızlı ve en etkili yöntemlerden biri olabilir. Hepsi olmasa da popüler web servislerinin çoğu, varsayılan olarak devre dışı bulunan MFA işlevselliğini sunar.

Şirketinize en uygun MFA işlevini uygulamak için uzmanlardan tavsiye alabilirsiniz

Chubb. Insured.℠

UK8205-MD 05/22