KUŞADASI BELEDİYE BAŞKANLIĞI
BİLGİ İŞLEM MÜDÜRLÜĞÜ
ÇOK FAKTÖRLÜ KİMLİK DOĞRULAMA TEKNİK ŞARTNAMESİ

- Sistem, yaygın olarak kullanılan Microsoft Active Directory, LDAP, RADIUS standartlarını desteklemelidir. Sistem birden fazla LDAP veya Active Directory hesapları veya sunucularıyla da sorunsuz şekilde çalışabilmelidir. Sistem, birden fazla kullanıcı veritabanıyla sorunsuz şekilde çalışabilmelidir.
- Ürün Active Directory üzerindeki security grupları görebilmeli ve seçilen grup içerisinde kullanıcıları ürün ara yüzünde gösterebilmelidir. Herhangi bir Security Grup içerisinde yer alan tüm Security Grupları ve içerisindeki kullanıcıları tanıma desteği olmalıdır.
- Ürün Active Directory üzerindeki kullanıcıları alırken kullanıcı hesabı üzerinden tüm Attribute'ları tanımalı ve Custom Attribute desteği olmalıdır.
- Ürün Active Directory üzerindeki seçilen grup da kaç adet kullanıcı olduğunu ve bunların kaç tanesinin kullanılabilir olduğunu ürün ara yüzünde göstermelidir. Ürün kabul etmediği kullanıcıları neden kabul etmediğine dair detaylı sebep gösteren rapor sunabilmeli ve çıktı alınabilmelidir.
- DC ile otomatik senkronizasyon zamanı belirlenebilmeli ve yönetici anlık senkronizasyon yapabilmelidir.
- Ürün için yönetici hesapları lokal oluşturulabileceği gibi active directory entegrasyonu ile DC hesapları ile de oluşturulabilmelidir.
- Ürün üzerinde lokal kullanıcı ve lokal gruplar oluşturulabilmelidir.
- Kullanıcı listesi detaylı bir şekilde yöneticiye gösterilmelidir. Mail adresi, Cep telefon bilgisi, Kullanıcı adı, SAM bilgisi, üye olduğu grup bilgisi vs.
- Kullanıcıların listelendiği sayfa da filtreleme olmalı, sayfa da ki tüm kullanıcı bilgileri içerisinde arama yapılabilmeli ve dışarı .CSV formatında aktarılabilmelidir.
- Ürün firmanın isteği doğrultusunda farklı SMS sağlayıcılar ile entegre olabilmelidir.
- İkinci kimlik doğrulama için SMS kullanılıyor ise SMS logları tutulmalıdır. Kullanıcıya SMS' in iletildiği, SMS ID ve kullanıcıya SMS' in ulaştığına dair rapor SMS sağlayıcıdan anlık ve otomatik olarak çekilebilmeli ve arayüz de gösterilebilmelidir.
- Herhangi SMS iletim sorunu yaşandığında sağlayıcının döndüğü değer loglarda görünmelidir.
- Kullanıcıya gönderilecek SMS içeriği düzenlenebilir olmalıdır.
- Kullanıcı bazlı test SMS' i atılabilmelidir.
- Sistem, tek kullanımlık şifre (one time password) ve kimlik doğrulama yanıtı (authentication response) yöntemlerini desteklemelidir.
- Ürün, iki faktörlü kimlik doğrulama metodu olarak SMS 'i destekleyebilmelidir.
- Ürün, iki faktörlü kimlik doğrulama metodu olarak Google authenticatior , Microsoft authenticatior ve benzeri en az bir adet authenticatior uygulamayı destekleyebilmelidir.
- Ürün, iki faktörlü kimlik doğrulama metodu olarak kendi mobil uygulamasına sahip olmalıdır. IOS ve Andorid platformlarında çalışabilmeli ve tek kullanımlık kod bilgisi gönderebilmelidir.
- Ürünün mobil uygulama onayı isteyerek (kullanıcı mobil uygulamaya gelen bildirim ile onayla ya da reddet seçeneğini kullanarak erişim belirleyebilmeli.) çok faktörlü kimlik doğrulama yapabilmelidir.
- Ürün tersine iki faktörlü kimlik doğrulama yapabilmelidir. Önce ikincil kodun doğrulu kontrol edilerek sonrasında asıl şifrenin kontrolü sağlanabilmelidir.

- Ürün aynı anda hep üsteki maddeye uygun çalışabilmeli hem de onayla reddet şeklinde bildirim son kullanıcıya sunulabilmelidir. Bu iki işlem için BT yöneticinin herhangi bir işlem yapmasına gerek kalmamalıdır.
- Sistem, açık standartları destekleyen VPN sonlandırıcı, güvenlik duvarı vb. ürünler ile entegre olabilmelidir.
- Ürün, grup bazlı kural yazma yeteneğine sahip olmalıdır.
- Ürün, IP ve network bazlı kural yazma yeteneğine sahip olmalıdır.
- Ürün, grup bazlı ikinci kimlik doğrulamayı devre dışı bırakabilmelidir.
- Oluşturulan kuralların öncelikleri belirlenebilmelidir.
- Ürün tüm standart Radius attribute 'lerini desteklemelidir.
- Ürün üretici bazlı Radius attribute (vendor spesific) desteklemelidir.
- Ürün grup bazlı Radius attribute atayabilmelidir.
- Ürün yaygın olan güvenlik cihazı markaları ile çalışabilmelidir. (İlerde Firewall markasının değişmesi durumunda yeni konumlandırılan ürün ile de entegre olabilmelidir.)
- Ürün loglarında kimlik doğrulama ile ilgili detaylı bilgiler bulunmalıdır.
- Ürün ara yüzünde lisans bilgileri yer almalıdır.
- Ürün sanal olarak ESX ve Hyper-V ortamında çalışabilmelidir.
- Ürün tek bir sanal sunucu üzerinde tüm özellikleri karşılayabilecek şekilde çalışabilmelidir.
- Ürün kuruma ait kullanıcı adı , şifre vb herhangi bir bilgi dışarı aktarmadan çalışabilmelidir.
- Ürün üzerinde dashboard ekranı olmalıdır. Bu ekran TOP X olarak başarılı ve başarısız kimlik doğrulama bilgilerini günlük olarak gösterebilmelidir. Günlük kullanılan SMS adeti görünmelidir.
- Ürün üzerinde rapor çekilebilmelidir. Belirlenen tarih arasında başarılı bir şekilde doğrulama yapan kullanıcılar, başarısız bir şekilde doğrulama yapan kullanıcılar, toplam harcanan SMS sayısı ve başarılı /başarısız oranını gösteren bilgiler rapor içerisinde yer almalıdır.

- Ürün Windows sunucularına uzak masaüstü bağlantılarında domain kullanıcı ve lokal kullanıcı hesapları ile giriş sağlarken çoklu kimlik doğrulama sağlamalıdır.
- Ürün merkezi olarak uzak masaüstü bağlantılarında çok faktörlü kimlik doğrulamayı devre dışı bırakabilmelidir.
- Windows sunucu üzerine kurulu olan ajan eğer ürünün merkezi yönetim sistemine erişemez ise talep doğrultusunda devre dışı bırakılabilmelidir.
- Windows sunucu üzerine kurulu olan ajan yedeklilik için birden fazla merkez ile konuşabilmelidir.
- Linux işletim sistemine sahip sunuculara giriş sağlarken çok faktörlü kimlik doğrulama yapılabilmelidir.
- Ürün Outlook Web Access (OWA) 'ya giriş sağlarken çoklu kimlik doğrulama sağlamalıdır.
- Ürün merkezi olarak Outlook Web Access (OWA) bağlantılarında çok faktörlü kimlik doğrulamayı devre dışı bırakabilmelidir.
- OWA üzerine kurulu olan ajan eğer ürünün merkezi yönetim sistemine erişemez ise talep doğrultusunda devre dışı bırakılabilmelidir.
- Ürün API desteği sağlamalıdır. API entegrasyonda üretici destek için ektra bir ücret talep etmemelidir. API entegrasyonu ile 3thrd party yazılımlar API'a uygun geliştirme yaparak çok faktörlü kimlik doğrulamayı destekleyebilmelidir.
- Ürün platformu ile ürün ajanları arasındaki iletişim ssl ve şifrelenmiş olmalıdır.
- Ürün ağ ve güvenlik cihazlarına giriş sağlarken çok faktörlü kimlik doğrulama yapabilmelidir.

- Ürün 1 yıllık ve 3 yıllık olarak teklif edilmelidir.
- Ürün kurulumu ve desteği teklife dahil edilmelidir.
- Ürün Yerli Malı belgesine sahip olmalıdır.
- Sistem, bulut tabanlı (Cloud based) olmamalıdır, sistemin tüm bileşenlerinin kurum altyapısında kurulu bulunması beklenmektedir.
- Sistem yedekli, kümelemeyi(clustering) veya high availability mekanizmalarından birini desteklemelidir.
- Ürün yedekli olarak teklif edilmelidir.
- Sistem, son kullanıcıların aynı istemci yazılımını kullanarak birden fazla uygulamaya giriş yapabilmesini sağlamalıdır.
- Sistem, sistem yöneticilerinin, son kullanıcıların hangi uygulamalara tek kullanımlık şifre ile giriş yapacaklarını kontrol edebilmelerini sağlamalıdır. Kurumun gereksinimleri doğrultusunda, kurallar ve istisnaların oluşturulabilmesi mümkün olmalıdır.
- Ürün veri tabanı dışardan erişime kapalı olmalıdır. Veri tabanına servis çalıştığı sürece servis dışında hiçbir unsur erişememelidir.

Ertuğrul TEMEL
Bilgi İşlem Md. V.