TÜBİTAK BİLGEM YTE

DİJİTAL KABİLİYET REHBERLERİ

AKTİF DİZİN REHBERİ

BİLGİ TEKNOLOJİLERİ HİZMETLERİ

Eylül 2020

DEĞİŞİKLİK TARİHÇESİ

Rev. No	Yayın Tarihi	Yayın Nedeni	Hazırlayan(lar)
Sürüm 1	Ağustos 2019	İlk sürüm	TÜBİTAK BİLGEM YTE
Sürüm 1.1	Ekim 2019	Revizyon	TÜBİTAK BİLGEM YTE
Sürüm 1.2	Eylül 2020	Revizyon	TÜBİTAK BİLGEM YTE

İÇİNDEKİLER

TABLOLAR

ŞEKİLLER

YÖNETİCİ ÖZETİ

Dijital Devlet (d-Devlet) alanında ülkemiz koşulları ile kamu kurumlarının ihtiyaçlarını göz önünde bulunduran ve uluslararası çalışmaları dikkate alan, kurumsal dijital kabiliyetlerini bütüncül bir yapı üzerinden değerlendirmeyi sağlayan **Dijital Olgunluk Değerlendirme Modeli**'nin geliştirilmesi ve bu **Model** ile uyumlu **Rehberlerin** hazırlanması ile dijital kurumsal kapasitenin artırılmasına ihtiyaç bulunmaktadır. Bu ihtiyaç doğrultusunda TÜBİTAK-BİLGEM-YTE tarafından iç destekli olarak **Dijital Olgunluk Modeli ve Rehberlik** (DİJİTAL-OMR) Projesi 2016 yılında başlatılmıştır. Proje kapsamında d-Devlet çalışmalarında sistemli ve bütüncül bakış açısı getirilerek kamu kurumlarının dijital yetkinliklerinin geliştirilmesi ve yürüttükleri proje ve faaliyetlerinin etkililik, etkinlik ve bilgi güvenliği niteliklerinin artırılması ile dijital kamu hizmetlerinin kalite ve performansının iyileştirilmesi sağlanacaktır.

Modeli ve **Rehberlerin** hazırlanmasına yönelik ulusal politika hedefleri, ülkemizde geliştirilen ve uygulamaya alınan Bilgi Teknolojileri (BT) rehber ve olgunluk modelleri ile 5 uluslararası kuruluş, 12 danışmanlık firması, 6 ülke tarafından geliştirilen standart, rehber ve çerçeve modelleri, uygulama örnekleri ve ilgili akademik çalışma örnekleri incelenmiştir. Farklı dijital kabiliyet alanlarında 34 bilişim uzmanından tecrübe aktarımı sağlanmıştır. Merkezi Yönetim ile yapılan anket üzerinden ilgili kapsama giren konular özelinde anket sonuçları analiz edilmiştir. Elde edilen tespitler doğrultusunda, **Dijital Olgunluk Değerlendirme Modeli**'nin taslağı oluşturulmuş ve seçilen kamu kurumlarında pilot uygulama yapılmıştır. Pilot uygulama sırasında alınan geri bildirimler doğrultusunda **Model** nihai hale getirilmiştir. **Model** ile Stratejik Yönetim, Organizasyon, Yazılım Hizmetleri, Yazılım Yaşam Döngüsü, BT Hizmetleri, İşletim ve Bakım, d-Hizmetler başlıklarında yedi yetkinlik belirlenmiştir. Bu yetkinlikler altında gruplandırılmış dijital kabiliyetler bazında seviyelendirilmiş 2834 soru belirlenmiştir.

Model'in 8 kurumda uygulaması yapılarak Dijital Olgunluk Seviyeleri belirlenmiş ve dijital kabiliyetler bazında tespit değerlendirmeleri gerekçelendirilerek Dijital Olgunluk Seviyesini geliştirmeye yönelik kısa, orta ve uzun vadede çözüm önerileri sunulmuştur.

Dijital Olgunluk Değerlendirme Modeli kapsamında yer alan yetkinlikler ve söz konusu yetkinlikler kapsamında yer alan dijital kabiliyetler dikkate alınarak yol gösterici olarak kullanılmak üzere **Rehberler** hazırlanmaktadır. Kurumsal kaynakların büyük bir kısmının işletim ve bakım proje ve faaliyetlerine ayrılmış olduğu tespitinden hareketle, ilk olarak **İşletim ve Bakım Rehberi** hazırlanmış ve 2017 yılında yayımlanmıştır. **Rehber**'de, işletim ve bakım yetkinliği altında toplanan kabiliyetler bazında tespit edilen seviyelendirilmiş

sorular ile kurumların mevcut olgunluğuna yönelik referans, rol, işleyiş, iş akışı ve çıktılar ile ilgili bilgiler sunulmaktadır. Aynı yıl **Model** ile belirlenen tüm dijital kabiliyetler için, yatırım planlanırken dikkate alınması gereken unsurlar ve alternatifleri ile ilgili bilgi ve yönlendirmeleri içeren 32 adet **Dijital Kabiliyet Rehberi** hazırlanmıştır. Söz konusu rehberlerin yetkinlikler altında ve tüm yaşam döngüsü dikkate alınarak genişletilmesine yönelik rehber hazırlama çalışmaları devam etmekte olup bu kapsamda 2018 yılında yılında **BT Hizmetleri** yetkinliği altında yer alan **Veri Merkezi Rehberi**, 2019 yılında aynı yetkinlik altında **Kablosuz Ağların İşletimi Rehberi**, **Kablosuz Ağların Yönetimi Rehberi**, **Aktif Dizin Rehberi**, **Sunucu Yönetimi Rehberi ve İstemci Yönetimi Rehberi** yayımlanmıştır. 2020 yılı içerisinde bunlara ek olarak **Uzaktan Çalışma Rehberi**, **VOIP Rehberi** ve **Alan Adı (Domain) Sistem Yönetimi Rehberi** yayınlanmıştır.

Dijital Devlet ekosistemi paydaşlarının değerlendirmesine yönelik tüm **Rehberlerin** **www.dijitalakademi.gov.tr** platformu ile açık erişimi sağlanmakta ve **Rehberlerin** kullanımının yaygınlaşması amacıyla eğitim programları, toplantılar ve çalıştaylar düzenlenmesi ile **Rehberlik Mekanizmaları** hayata geçirilmektedir. Bu sayede d-Devlet ekosisteminde görev alan bilişim uzmanlarının yetkinliklerinin artırılması hedeflenmektedir. Yanı sıra **Dijital Olgunluk Değerlendirme Modeli** ile uyumlu olarak 2017 yılında Türkiye'ye özgü **Dijital Yetkinlik Değerlendirme Modeli** geliştirilmiş ve **Model** ile kamu kurumlarında çalışan bilişim uzmanlarının yetkinlik değerlendirmesi yapılarak güçlü ve zayıf yönlerinin belirlenmesi ve eğitim ve mesleki gelişim açısından iyileştirmeye açık alanların tanımlanması amaçlanmıştır. 38 bilişim profesyonel rolü ile bu rollerdeki çalışanların sahip olması hedeflenen 56 yetkinlik ve yetkinlik için 5 kademeli seviye tanımlanmış olup, roller, yetkinlik alanları ve yetkinlik seviyeleri arasındaki ilişkiler belirlenmiştir. 6 kurumda yaklaşık 550 uzman için yetkinlik değerlendirmeleri yapılmış ve kurumların dijital kapasitelerinin geliştirilmesi için öneriler geliştirilmiştir.

On Birinci Kalkınma Planı'nda ve 2019 Yılı Yıllık Programı'nda belirlenen kurumsal olgunluk ve insan kaynağı yetkinlik modelleri geliştirilmesi ihtiyacının karşılanmasında Dijital Devlet ekosistemine katkı sağlayacağını öngördüğümüz Türkiye'ye özgü geliştirilen ilk **Dijital Olgunluk ve Yetkinlik Değerlendirme Modelleri** ile **Dijital Kabiliyet Rehberleri'nin** içeriğine yönelik olarak **epid.yte@tubitak.gov.tr** ve **www.dijitalakademi.gov.tr** adresleri aracılığıyla ileteceğiniz değerlendirmelerinizle ilgili çalışmaların tüm ekosistemin bilgi ve tecrübesiyle iyileştirilmesini temenni ederiz.

1 GİRİŞ

Aktif Dizin Rehberi 5 bölümden oluşmaktadır:

1. Bölüm'de, dokümanın kapsamı, kullanılan terimler ve yararlanılan kaynaklar,
2. Bölüm'de, Proje'nin amacı ve kapsamı,
3. Bölüm'de Dijital Olgunluk ve Yetkinlik Değerlendirme Modelleri ile ilgili bilgiler,
4. Bölüm'de, Aktif Dizin Rehberi'nin gerekçesi, yapısı, kapsamı ve ilgili çalışmalar,
5. Bölüm'de, Aktif Dizin Rehberi kapsamında tanımlanan kabiliyetlere ilişkin yönlendirici bilgiler

sunulmaktadır.

1.1 TERİMLER VE KISALTMALAR

Terim / Kısaltma	Tanım
Account Operators	Etki alanındaki kullanıcıları ve grupları oluşturmak ve yönetmek için tanımlanmış varsayılan gruptur.
AD	[Active Directory] Ağdaki nesneler ile ilgili bilgileri depolayan hiyerarşik yapıdır.
AdminSDHolder	Etki alanındaki korumalı hesaplar ve gruplar için şablon izinleri sağlayan konteynırdır.
ADSI	[Active Directory Service Interfaces] Farklı network sağlayıcılarından dizin servisleri özelliklerine erişilebilmesini mümkün kılan bir arayüzüdür.
Ağaç	[Tree] Ortak bir şema ve yapılandırmayı paylaşan, bitişik bir ad alanı oluşturan ve birkaç etki alanından oluşan yapıdır.
Ayrıcalıklı Hesap	[Privileged Account] Standart hesaplardan farklı olarak güçlü haklar, ayrıcalıklar ve izinlerin verildiği hesaplardır.
Backup Operators	Etki alanı denetleyicileri üzerinde yedekleme ve yedekten geri dönüş işlemlerini gerçekleştirebilen varsayılan gruptur.
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
Bilgi Güvenliği	Bilginin gizlilik, bütünlük ve erişilebilirlik niteliklerinin korunmasıdır.
BT	Bilişim teknolojileri

Terim / Kısaltma	Tanım
BT	Bilgi Teknolojileri
CredSSP	[Credential Security Support Provider Protocol] Bir uygulamanın, kullanıcının kimlik bilgilerini istemciden hedef sunucuya iletmesine izin veren bir protokoldür.
d-Devlet	Dijital Devlet
DFL	[Domain Functional Level] DC'lerin domain bazında işletim sistemi seviyesidir.
DNS	[Domain Name System] TCP/IP ağlarda kullanılan isim çözümleme protokolüdür.
Domain	Etki Alanı. Aynı dizin veritabanını paylaşan objeler bütünüdür.
Domain Admin	Etki alanı yönetişi
Dört Göz İlkesi	Yapılan bir işin iki kişi ile gerçekleştirilmesi gerektiğini belirtilen ilkedir.
Erişilebilirlik	Hizmetin veya hizmeti oluşturan bileşenin ihtiyaç duyulduğunda istenilen fonksiyonu gerçekleştirebilme durumudur.
ESE	[Extensible Storage Engine] Bilgileri mantıksal sırayla depolayan bir veritabanı motorudur.
FFL	[Forest Functional Level] Forest'da mevcut tüm Domain'lerin içindeki DC'lerin forest bazında işletim sistemi seviyesidir.
Geri Dönüşüm Kutusu	[AD Recycle Bin] Silinen AD nesnelerini kurtarmayı sağlayan dizin özelliğidir.
Global Catalog	Ormandaki her nesnenin kısmı bir kopyasının barındırılmasını mümkün kılan etki alanı denetleyicisi rolüdür.
GPO	[Group Policy Object] Etki alanındaki bilgisayar ve kullanıcı nesneleri ile uygulamaların merkezi olarak yönetimini ve yapılandırılmasını sağlayan özelliktir.

Terim / Kısaltma	Tanım
Group Managed Service Account	Uygulamaların ihtiyaç duydukları servis hesaplarının grup tabanlı olarak merkezi ve güvenli bir şekilde yönetilmesini sağlayan özelliktir.
Güven İlişkisi	[Domain Trust] Farklı iki etki alanı arasında bilgi ve kaynak paylaşımı amacıyla kurulan mantıksal ilişkidir.
Güvenli Dinamik Güncelleme	[Secure Dynamic Update] DNS kayıtları için güncellemelerin, DNS protokolü aracılığı ile yetkili DNS sunucusuna gönderildiği mekanizmadır.
Hizmet	Kullanıcını ihtiyaçlarını karşılayarak bir fayda yaratma biçimidir. (Örnek: Kullanıcıların iletişim ihtiyaçları için sunulan e-posta hizmeti, kurum içi yazışmaların oluşturulması ve yönetilmesi için sunulan doküman yönetim hizmeti, vb.)
Kabiliyet	Bir işin kalite, bilgi güvenliği, performans vb. gereksinimlerinin karşılanma durumudur.
Kullanıcı	Hizmeti kullanan kişilerdir. Kurum içi BT hizmeti kullanıcıları olabileceği gibi, kurumun elektronik ortamda sunduğu kamu hizmetlerinin son kullanıcıları (vatandaş, özel sektör, diğer kurumlar vb.) da olabilir.
LDAP	[Lightweight Directory Access Protocol] Dizin hizmetindeki bilgilerin sorgulanmalarını ve güncellenmelerini sağlayan endüstri standardı bir protokoldür.
NTLM	[New Technology LAN Manager] Kullanıcılara kimlik doğrulama, bütünlük ve gizlilik sağlama amaçlı Microsoft güvenlik protokolüdür.
Olgunluk	Önceden tanımlanmış bir durumu sağlama halidir.
Olgunluk Modeli	Başlangıç durumundan, önceden tanımlanmış yetkinlik alanlarındaki olgunluk durumuna kadar, öngörülen, arzu edilen ya da tercih edilen yol doğrultusunda, sıralı düzeyler ya da aşamalar içeren modeldir. İlgili alanda referans modele göre

Terim / Kısaltma	Tanım
	mevcut durumun değerlendirilmesi ve referans modele göre iyileştirme alanlarının belirlenmesi için kullanılır.
Orman	[Forest] Bitişik bir ad alanı oluşturmayan, bir veya daha fazla etki alanı ağacı kümesidir.
OU	[Organization Unit] Kullanıcı, grup, bilgisayarlar ve diğer objelerin barındırılmasını sağlayan alt bölümdür.
Problem	Bir veya birden fazla arızaya/kesintiye ilişkin kök neden olarak tanımlanan durumdur.
Red Forest	Etki alanı ortamının tam kontrolü ile yüksek riskli iş istasyonu varlıkları arasında bir dizi tampon bölge kullanarak kimlik sistemlerini korumayı hedefleyen kademeli modeldir.
Risk	Bir faaliyetin içerdiği belirsizlik ve zarar olasılığıdır.
Schema	Bir AD ormanında oluşturulabilecek her nesne sınıfının resmi tanımlarını içeren dizin bölümüdür.
SID	[Security Identifier] Active Directory ortamında bilgisayarlara, kullanıcılara veya gruplara atanan eşşiz bir sayıdır.
Site	Etki Alanı Denetleyicileri arasında bilgileri verimli bir şekilde çoğaltmak için kullanılan IP alt ağlarının fiziksel gruplamalarıdır.
SSO	[Single Sign On] Kullanıcının bir oturum açma kimlik bilgisi ile birden çok uygulamaya erişmesine olanak sağlayan kimlik doğrulama işlemidir.
STK	Sivil Toplum Kuruluşu
Şifreleme	Bir veriyi matematiksel işlemler kullanarak şifreli duruma getirme
TGS	[Ticket Granting Service] İstemcilerin, aynı etki alanı içerisindeki bir servise erişmek istediklerinde, erişim iznini sağlayan servistir.
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

Terim / Kısaltma	Tanım
Yetkinlik	Kabiliyet ya da kabiliyet gruplarının bir yaşam döngüsü ve amaç bazında gruplanmış şeklidir.
YTE	Yazılım Teknolojileri Araştırma Enstitüsü

1.2 REFERANSLAR

Ref 1. NSA (2018), Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), Amerika Birleşik Devletleri

Ref 2. IT Grundschutz 1.Yayım (2018): Bilgi Teknolojileri Güvenliği Enstitüsü (BSI), Almanya.

Ref 3. ISO (2013). ISO/IEC 27001 - Information security management.

Ref 4. ISO (2013). ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security controls

2 DİJİTAL OLGUNLUK MODELİ VE REHBERLİĞİ PROJESİ

Dijital Olgunluk Modeli ve Rehberlik (DİJİTAL-OMR) Projesi, 2016 yılında TÜBİTAK-BİLGEM-YTE tarafından yürütülen iç destekli bir projedir. Projenin amacı, Dijital Devlet (d-Devlet) alanında gelinen düzeyde ülkemiz koşulları ile kamu kurumlarının ihtiyaçlarını göz önünde bulunduran ve uluslararası çalışmaları dikkate alan kurumsal **Dijital Olgunluk Değerlendirme Modeli'nin** geliştirilmesi ve bu yönde kurumsal kapasitenin artırılması için **Model** ile **Rehberlerin** hazırlanmasıdır.

Bu proje ile 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'nda doğrudan rehberlik mekanizmalarına yönelik tanımlanan aşağıdaki eylemlere de katkı sağlanacaktır:

- "*E1.1.4-e-Devlet Ekosistemi Rehberlerinin Hazırlanması ve Güncellenmesi*" eylemi, e-Devlet ekosisteminin etkin bir şekilde çalışabilmesi ve sürdürülebilirliği için birlikte çalışabilirlik, kamu kurum / kuruluşlarının internet siteleri ve mobil uygulamaları ile kamu kurum / kuruluşlarının resmi sosyal medya hesaplarının kullanımı ve yönetimine dair rehberler başta olmak üzere mevcut rehberlerin güncellenmesi ve ihtiyaç duyulan yeni rehberlerin hazırlanmasına yönelik bir eylemdir.
- *"E1.1.6-Ulusal e-Devlet Olgunluk Seviyesi Ölçümleme Mekanizmasının Oluşturulması"* eylemi, yaşamsal olaylar bütünlüğünde kamu hizmetlerinin e-Devlet olgunluk düzeyi, Kurum seviyesinde e-Devlet olgunluk düzeyi ve Ulusal e-Devlet olgunluk düzeyi kapsamında e-Devlet olgunluk ve olgunluk ölçümleme modellerinin tanımlanması, tanımlanan bu modeller kullanılarak ulusal düzeyde e-Devlet olgunluk düzeyi ölçümleme çalışmaları ile birlikte, seçilen e-Devlet hizmetleri ve kamu kurumları için e-Devlet olgunluk düzeyi ölçümleme çalışmalarının yürütülmesine yönelik bir eylemdir.

Proje kapsamında yapılacak faaliyetler, kurumsal düzeydeki dijital dönüşümü ve 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'ndaki eylemler ile hayata geçirilmesi öngörülen ulusal düzeydeki olgunluk değerlendirme modelini destekleyecektir. Bir başka ifadeyle, Proje kapsamında üretilecek **Model** ve **Rehberler** ile kurumların teknoloji odaklı güncel dönüşüm ihtiyaçlarına cevap verebilmek adına kurumsal düzeyden başlayan ve ulusal düzeye çıkan ölçümleme çalışmalarına katkı sağlanacaktır. Dolayısıyla mikro seviyede kurum düzeyindeki kurumsal etkinliği artırma odağı ile şekillendirilen proje çıktıları, makro seviyede ulusal olgunluk düzeyine çekilebilecek bir alt yapı oluşturacaktır. Bu alt yapı sayesinde 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'nda yer alan eylemlerin uygulanabilirliği artırılacaktır.

Dijital Olgunluk Değerlendirme Modeli ile;

- Kamu kurumlarının bilişim proje ve faaliyetlerine sistemli ve bütüncül bakış açısının geliştirilmesi desteklenecektir.
- Kamu kurumları ve sundukları hizmetlerin dijital olgunlukları hakkında bir değerlendirme yapabilmek ve seviye tespit edebilmek mümkün olacaktır.
- Kurumların içinde bulunduğu dijitalleşme sürecinde değişimlere ve yeniliklere uyumu desteklenecektir.

Model kapsamında hazırlanacak **Rehberler** ve **Rehberlik** mekanizması ile;

- Bilişim projeleri ve faaliyetlerinin daha verimli, etkin ve güvenli planlanması, yürütülmesi ve tamamlanması sağlanarak başarı oranının artırılmasına katkı sağlanacaktır.
- Bilişim proje ve faaliyetlerinin verimliliği artırılarak ilgili hizmetlerin kalite ve performansı iyileştirilecektir.
- Bilişim uzmanlarının dijital kabiliyetleri artırılacaktır.
- TÜBİTAK tarafından yürütülen Kamu BT projeleri ile edinilen bilgi ve tecrübenin, özel sektör ve STK ile açık paylaşımı sağlanacak ve ilgili paydaşlar ile karşılıklı bilgi ve tecrübe alışverişi gerçekleştirilecektir.

3 DİJİTAL OLGUNLUK VE YETKİNLİK DEĞERLENDİRME MODELLERİ

Dijital Olgunluk Değerlendirme Modeli, bir organizasyonun önceden tanımlanmış yetkinlik alanlarındaki yetkinlik durumundan hedeflenen ya da gerekli görülen seviyeye kadar, dijital dönüşüm ve/veya dijital hizmet kabiliyetlerindeki seviyelerin değerlendirilmesini ve iyileştirilmesini sağlayan kademeli referans modeldir.

Dijital teknolojilerin yenilikçi fırsatlarıyla iş süreçlerine uyarlanması ve dijital teknolojiler doğrultusunda yeni katma değerli hizmet ve süreçler oluşturulması kurumsal düzeyde dijital dönüşümün en öncelikli amacı olmaktadır. Dünyada özellikle son 10 yıldır dijitalleşmenin ve ülkelerin farklılaşan koşullarına göre geliştirilen birçok dijital olgunluk değerlendirme modeli olmasına karşın, Türkiye'de kamu kurumlarında "e-Kurum" "e-Devlet" ve "dijital" gibi kavramların hiçbirine yönelik olgunluk referans modelinin olmadığı görülmüştür.

Günümüz koşulları değerlendirildiğinde "dijital" kavramı doğrultusunda hazırlanacak ve kurumların dijital dönüşümlerini analiz edip referanslar doğrultusunda yönlendirecek bir modelin ve model uygulama yaşam döngüsünün olması önemli bir ihtiyaçtır. Ancak bilişim ya da bilgi güvenliği standart ve rehberlerine benzer şekilde uluslararası kabul gören bir kurumsal dönüşüm standardı mevcut değildir.

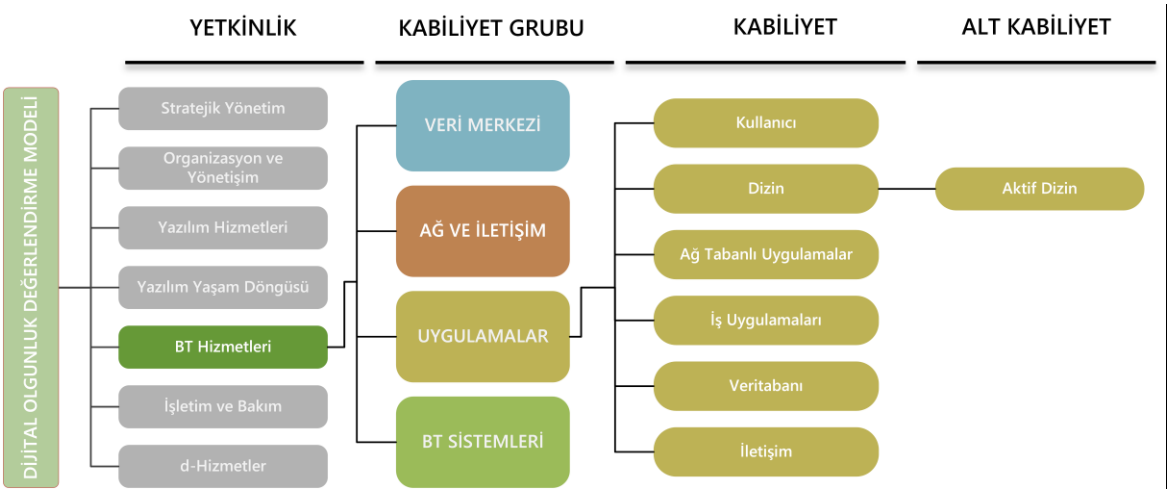
Bununla birlikte, kurumların teknoloji odaklı güncel dönüşüm ihtiyaçlarına cevap verebilmek üzere danışmanlık firmaları ve teknoloji firmaları tarafından oluşturulmuş birçok ticari dijital dönüşüm modeli söz konudur. Bu modellerin çoğunluğu özel sektöre yönelik olarak özel sektör bakış açısıyla hazırlanmaktadır. Ancak ortak alanlar olmakla birlikte kamu kurumlarının ihtiyaçları özel sektör ihtiyaçlarından ayrışmaktadır. Üstelik kamu yönetim anlayışı ve birikimi göz önüne alındığında, ülkemiz diğer ülkeler ile de ayrışmaktadır. Teknoloji odaklı dönüşüm çabası içerisinde olan tüm organizasyonlar için ortak gereksinimler söz konusu iken mevcut koşulları doğrultusunda her organizasyon tipinin kendi içerisinde özelleşmiş ihtiyaçları da olabilmektedir. Bu doğrultuda, kamu kurumlarında dijital dönüşüme yön verilmesi ve uygulamanın başarı ile hayata geçirilebilmesi için öncelikli olarak, kamu kurumlarına yönelik **Dijital Olgunluk Değerlendirme Modeli** oluşturulmuş ve **Modelin** ülke koşullarına uygun yapıya sahip olması sağlanmıştır. Oluşturulan **Model**, aynı zamanda ülkenin mevcut dijital dönüşüm politikalarıyla uyumludur ve uluslararası tecrübeleri dikkate almaktadır.

Model ile bir organizasyonun dijital kabiliyetlerini değerlendirerek, tespit edilen mevcut kabiliyet seviyelerinin iyileşmesi için yol haritası sağlanmaktadır. Böylece, kurumların dijital

dönüşümlerinin yapısal, standart, tutarlı, etkin ve verimli bir şekilde yapılmasına katkı sağlanmaktadır.

Dijital Olgunluk Değerlendirme Modeli gereksinim ağacı 3 basamak olarak oluşturulmuştur:

- Yetkinlik
- Kabiliyet Grubu
- Kabiliyet
    - Alt Kabiliyet



Şekil 1. Dijital Olgunluk Değerlendirme Modeli Gereksinim Seviyeleri

Dijital Olgunluk Değerlendirme Modeli 7 yetkinlik altında tanımlanmış 35 kabiliyet grubu ve bu kabiliyet grupları altında gruplandırılmış çeşitli kabiliyetlerden oluşmaktadır:

- **Yetkinlik**, kendi aralarında ilişki söz konusu olan kabiliyet gruplarından oluşmaktadır. Her bir yetkinlik kendi içerisinde bir bütündür ve organizasyonlarda dijital dönüşüm için müstakil olarak ele alınabilir. Belirlenecek tespitler ve değerlendirmeler doğrultusunda organizasyonun her bir yetkinlik için yetkinlik seviyesi ortaya konmaktadır.
- Birbirlerine yakın olan kabiliyetler **kabiliyet grupları** altında toplanmıştır. Her bir yetkinlik altında tanımlanmış kabiliyet grupları arasında ilişki mevcuttur. Bu ilişki genel olarak bir döngü ya da pratikler üzerinden tarif edilmektedir.
- **Kabiliyetler**, organizasyonun iş ve işlemlerini gerçekleştirebilmek için gerek duyduğu/duyacağı en küçük bileşenlerdir. Kabiliyetler uluslararası normlara ve ulusal gereksinimlere uygun olarak belirlenmiştir.
- **Alt Kabiliyetler,** kabiliyetlerin; amaç, hedef kitle ve operasyonel sorumluluk alanlarına göre özelleşmiş alt bileşenleridir.

- **Seviye**, kurumun varlıklarının, uygulamalarının ve süreçlerinin gerekli çıktıları güvenilir ve sürdürülebilir bir şekilde üreterek olgun bir yapıya ulaşması amacıyla yapılandırılmış düzeylerdir.

Dijital dönüşümü hedefleyen kurumların ihtiyaç duyacağı yetkinlik alanları **Dijital Olgunluk Değerlendirme Modeli** kapsamında aşağıdaki gibi tanımlanmıştır:

Şekil 2. Dijital Olgunluk Değerlendirme Modeli - Genel Görünüm

1. Yetkinlik: STRATEJİK YÖNETİM

Dijital dönüşüm ve dijital hizmet yönetimi kapsamında orta ve uzun vadeli amaçları, temel ilke ve politikaları, hedef ve öncelikleri ve bunlara ulaşmak için izlenecek yol ve yöntemleri içeren strateji belgelerinin; kapsamına ilişkin faaliyetleri amaç, yöntem ve içerik olarak düzenleyen ve gerçekleştirme esaslarının bütününü içeren politika belgelerinin hazırlanmasını, izlenmesini ve güncellenmesini kapsar. Bu strateji ve politikalar doğrultusunda, kurumsal mimari yapısının kurulması, ihtiyaçların tanımlanması, çözümlerin planlanması ve bütçenin yönetilmesi amaçlanmaktadır. Bu yetkinlik, dijital strateji yönetimi, politika yönetimi, kurumsal mimari yönetimi, dijital dönüşüm yönetimi ve bütçe yönetimi kabiliyet gruplarını içermektedir.

2. Yetkinlik: ORGANİZASYON VE YÖNETİŞİM

Dijital dönüşüm çalışmalarının (portföy, program vb.) yönetişim mekanizmasından sorumlusu ekip / kişilerin mevcudiyeti, yönetişim mekanizmasının işlerliği, rol, yetenek ve

yetkinliklerinin yönetilmesini kapsar. Bu yetkinlik, organizasyon, dijital kültür, dijital kapasite geliştirme ve dijital yönetişim kabiliyet gruplarını içermektedir.

3. Yetkinlik: YAZILIM HİZMETLERİ

Kurum ihtiyaçlarına göre bir yazılımın yaşam döngüsü için yapılan yazılım fizibilitesi, geliştirilmesi, bakımı ve modernizasyonu, hazır paket yazılımların tedariki ile veri üretimi ve sayısallaştırma hizmetlerini kapsar. Bu yetkinlik, yazılım fizibilite, yazılım geliştirme, yazılım modernizasyonu, yazılım tedarik, yazılım bakımı, veri üretimi ve sayısallaştırma kabiliyet gruplarını içermektedir.

4. Yetkinlik: YAZILIM YAŞAM DÖNGÜSÜ

Yazılım projesinin planlamasından başlayarak teslimatına kadar geçirmiş olduğu bütün aşamaları ve bu aşamalardan oluşan döngüyü kapsar. Bu yetkinlik, gereksinim mühendisliği, teknik çözüm, doğrulama ve geçerleme, konfigürasyon yönetimi ve kalite güvence kabiliyet gruplarını içermektedir.

5. Yetkinlik: BT HİZMETLERİ

Kurumun sahip olduğu teknolojiler ile mevcut donanım ve altyapıların yönetilmesini kapsar. Bu yetkinlik, ağ ve iletişim, veri merkezi, uygulamalar ve BT sistemleri kabiliyet gruplarını içermektedir.

6. Yetkinlik: İŞLETİM VE BAKIM

Kurumsal BT hizmetlerinin planlanması ve yönetişimi, yeni planlanan / değişen BT hizmetlerinin devreye alınması ve kontrolü, BT hizmetlerinin yönetimi, sunulması ve desteği ile BT Hizmet kalitesinin sürekli iyileştirilmesi için gerekli kabiliyetleri kapsar. Bu yetkinlik, planlama, geçiş ve kontrol, sunum ile izleme ve değerlendirme kabiliyet gruplarını içerir.

7. Yetkinlik: D-HİZMETLER

Kurumun sahip olduğu idari uygulamaların yönetimini, kurum dijital tanıtım kanalları (internet sitesi, sosyal medya hesapları vb.) ve dijital olarak sunulan kamu hizmetlerinin tasarımını ve iyileştirilmesini içeren tüm adımları kapsar. Bu yetkinlik, kurumsal uygulamaların kullanımı, kurumsal bilgi yönetimi, d-hizmet yönetişimi, d-hizmet tasarımı, d-hizmet sunumu, d-hizmet iyileştirme, d-hizmet inovasyonu kabiliyet gruplarını içerir.

Kabiliyet grubu altındaki hangi kabiliyetlerin organizasyon için gerekli olduğu ve mevcut durumu dijital olgunluk değerlendirmesi kapsamında belirlenebilmektedir. Bu sayede, bazı kabiliyetler ya da kabiliyet grupları değerlendirme dışında bırakılabilmektedir. Benzer şekilde, kurumsal faaliyetlerin çeşitliliğine göre bazı kabiliyet ya da kabiliyet grupları diğerlerinden daha öncelikli olabilmektedir. Nihai kurumsal dijital olgunluk değerlendirmesi, kurumun faaliyet alanı, iş ve işlemlerini dikkate alarak kuruma uygun olarak özelleştirilebilmektedir. Bu sayede, dijital dönüşüm çalışmaları özelleşmiş ihtiyaçlara göre yönlendirilebilmektedir.

Kurumsal Dijital Olgunluk Seviyesi 4 ana gruba ayrılmıştır:

- Seviye 0 (Eksik): kabiliyet yoktur.
- Seviye 1 (Uygulanan): kabiliyetin temel pratikleri uygulanmaktadır.
- Seviye 2 (Kurumsallaşmış): kabiliyetler tanımlı, olup pratikleri, standart ve tutarlı bir şekilde uygulanmaktadır.
- Seviye 3 (Optimize Edilen): kabiliyet seviyeleri ölçülmekte olup, gerçek ve potansiyel problemlerin kaynağı analiz edilerek sürekli iyileşen kabiliyetler vardır.

Her kabiliyet seviyesinin altında tanımlanan sorular, doküman inceleme, ilgili personelle görüşmeler, yerinde gözlemleme, katılımcı gözlemi, fiziksel bulgular gibi çeşitli veri toplama yöntemleri kullanılarak yanıtlanmaktadır. Elde edilen yanıtların konu uzmanlarının değerlendirmeleri ile kabiliyetin seviyesi tespit edilmektedir.

Dijital Olgunluk değerlendirmesi kapsamında kurumun büyüklüğüne göre değişen ortalama 16 haftalık bir süreçte, ilgili alan uzmanlarından oluşan 10-15 kişilik **Değerlendirme Ekibi** tarafından değerlendirme yapılmaktadır. Kurum çalışanlarıyla **Dijital Olgunluk Öz Değerlendirme Anketi** yolu ile bilgi toplanmakta, kurum uzmanları ile 3-4 tam gün değerlendirme mülakatları yapılmakta, bilgi, belge ve dokümanlar incelenmekte ve değerlendirme sonrası kurumun mevcut **Dijital Olgunluk Seviyesi** belirlenmektedir. Dijital Olgunluk Seviyesinin bir üst seviyeye çıkması amacı ile değerlendirme sonucu elde edilen tespitler gerçekleşme etkisi ve gerçekleşme süresi üzerinden sınıflandırılarak kısa, orta ve uzun vadeli öneriler ilgili uzman görüşleri dijital kabiliyet rehberleri ile desteklenecek şekilde raporlanmaktadır.

Dijital Olgunluk Değerlendirme Modeli ile;

- Dijital Devlet çalışmalarında sistemli ve bütüncül bakış açısının geliştirilmesi,
- Kamu kurumların dijital kapasitelerinin yapısal, standart ve tutarlı bir şekilde değerlendirilmesi,

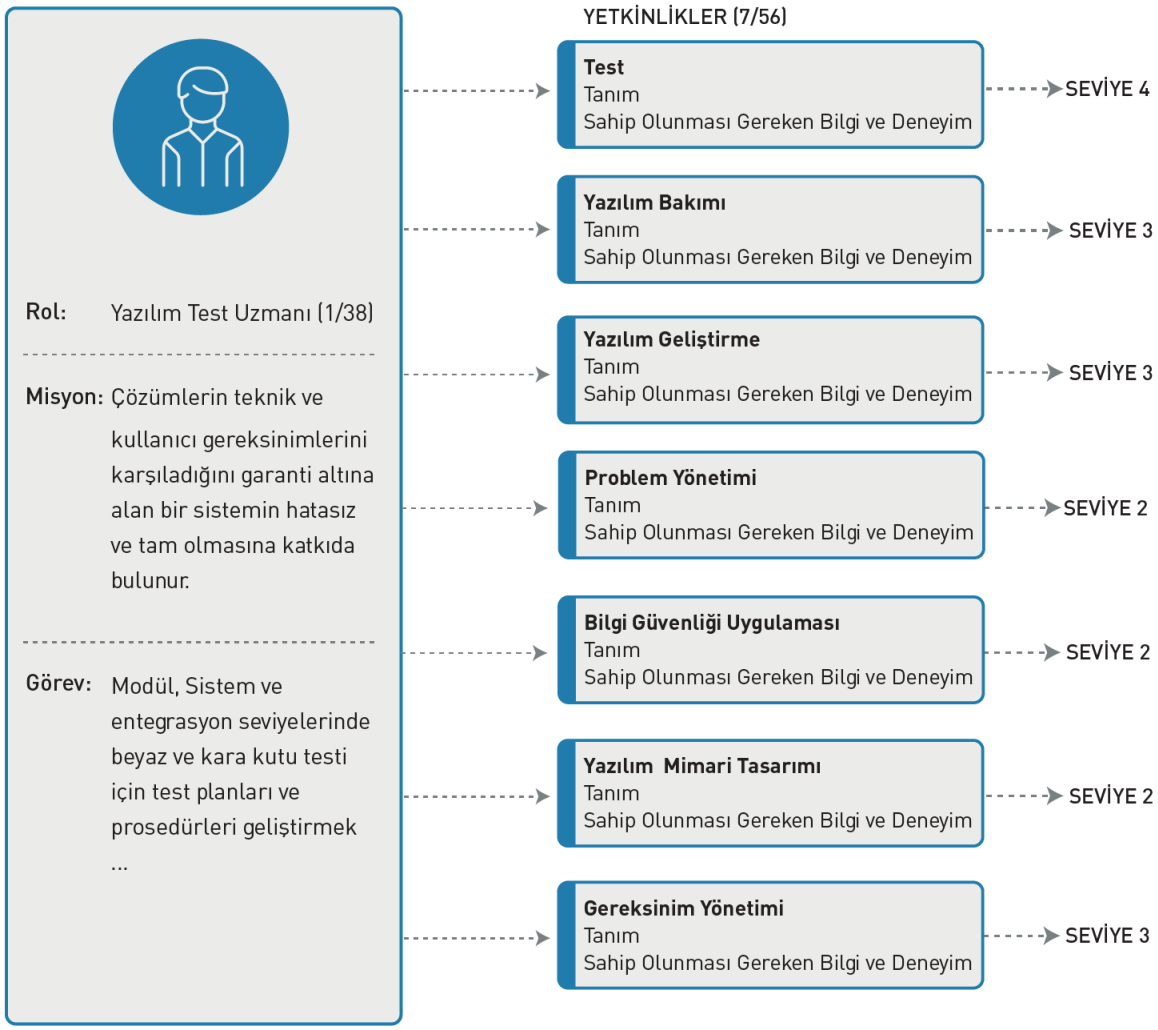
- Kamu kurumların dijital kapasitelerinin etkin ve verimli bir şekilde arttırılması için rehberlik edecek yol haritasının belirlenmesi,
- Dijital kamu hizmetlerinin kalite ve performansının iyileştirilmesi, çalışan ve vatandaş memnuniyetinin arttırılması

sağlanmaktadır.

Kurum dijital olgunluğunun yetkin insan kaynağı ile iyileştirilmesine yönelik **Dijital Olgunluk Değerlendirme Modeli'nde** yer alan kabiliyetler baz alınarak TÜBİTAK-BİLGEM-YTE tarafından **Dijital Yetkinlik Değerlendirme Modeli** geliştirilmiştir. Model ile kamu kurumlarında çalışan bilişim uzmanlarının yetkinlik değerlendirmesi yapılarak güçlü ve zayıf yönleri belirlenmekte, eğitim ve mesleki gelişim açısından iyileştirmeye açık alanların tanımlanması amaçlanmaktadır. "SFIA - Skills Framework for the Information Age" ve "European e-Competence Framework" modelleri analiz edilerek Türkiye'ye özgü ihtiyaçlar dikkate alınarak **Dijital Yetkinlik Değerlendirme Modeli** geliştirilmiştir. Dijital Yetkinlik Değerlendirme Modeli'nde;

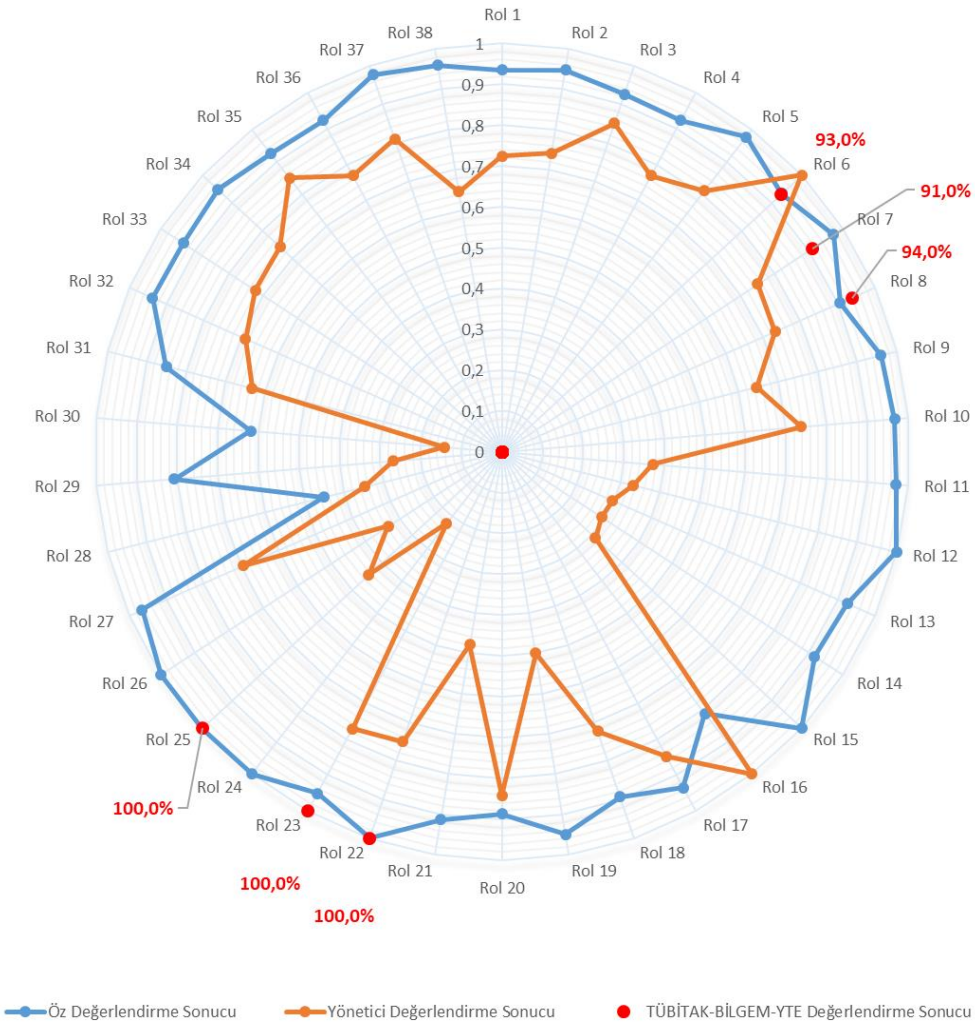
- BT Yönetimi,
- İhtiyaç Tanımlama ve Çözüm Planlama,
- Bilişim Sistemleri Yönetimi,
- Yazılım Teknolojileri Yönetimi

alanlarında Türkiye'deki organizasyon yapılarına özgü 38 bilişim profesyonel rolü tanımlanmıştır: Ayrıca, bu rollerdeki çalışanların sahip olması hedeflenen 56 yetkinlik ve yetkinlik için 5 kademeli seviye tanımlanmış olup, roller; yetkinlik alanları ve yetkinlik seviyeleri arasındaki ilişkiler belirlenmiştir. Bunun için bir örnek aşağıdaki gibidir:



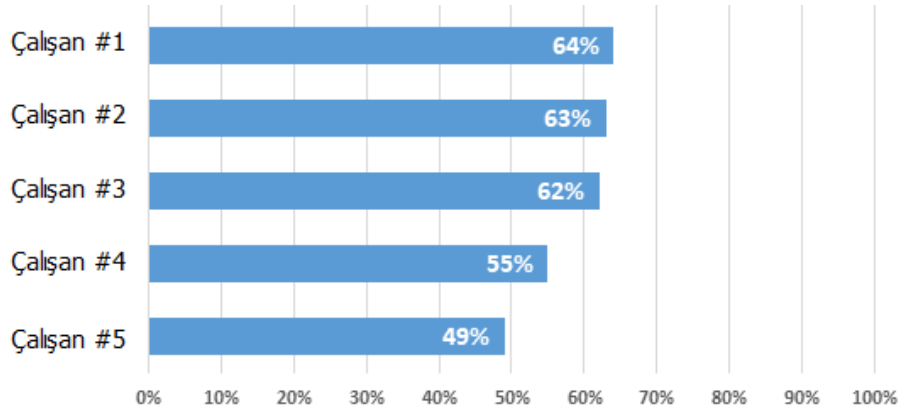
Şekil 3. Örnek Rol-Yetkinlik-Yetkinlik Seviyesi Eşlemesi

Dijital yetkinlik değerlendirmesi kapsamında kurumdaki bilişim uzmanı sayısına bağlı olarak değişen bir sürede, ilgili alan uzmanlarından oluşan 10-15 kişilik **Değerlendirme Ekibi** tarafından değerlendirme yapılmaktadır. Kurum çalışanlarının **Dijital Yetkinlik Öz Değerlendirme Anketi** yolu ile kendilerini değerlendirmesinin yanında, çalışanın bağlı olduğu bir üst yöneticisi tarafından **Yönetici Çalışan Değerlendirme Anketi** yoluyla yöneticisinin çalışanı değerlendirmesi sağlanmaktadır. Çalışan sayısına bağlı olarak değişen sürede çalışanlar ile değerlendirme mülakatları gerçekleştirilmektedir. Çalışan öz değerlendirme ve yönetici değerlendirmesi ile YTE değerlendirme sonucu üzerinden 38 rol bazında uygunluğu raporlanmaktadır:



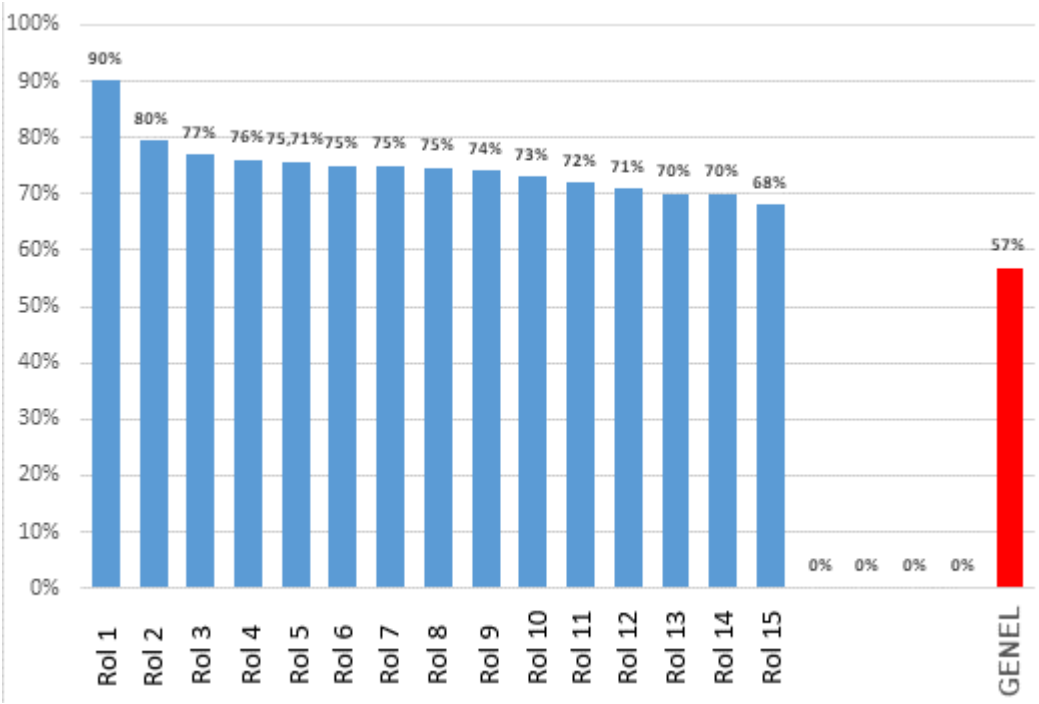
Şekil 4. Çalışan Dijital Yetkinlik Değerlendirmesi

Rol bazlı çalışan karşılaştırması yapılarak insan kaynağı kapasitesi değerlendirilmektedir:



Şekil 5. Rol Bazında Dijital Yetkinlik Değerlendirmesi

Bunun yanı sıra kurumdaki roller bazında değerlendirme raporlanmaktadır ve **Kurum Dijital Yetkinlik Haritası** çıkarılmaktadır:



Şekil 6. Kurum Dijital Yetkinlik Haritası

Kurumun büyüklüğü ve bağlı olduğu sektöre göre benzer kategoriye giren dünyadaki en iyi örnekler ile bilişim istihdam dağılımının karşılaştırması yapılarak kurumun istihdam planına rehberlik sağlanmaktadır.

Dijital Yetkinlik Değerlendirme Modeli ile;

- Yetkin bilişim insan kaynağı kapasitesinin arttırılması,
- Bilişim insan kaynağı yetkinliğinin ve kapasitesinin yapısal, standart ve tutarlı bir şekilde değerlendirilmesi,
- Bilişim uzmanlarının kariyer planı için gerekli yetkinlikleri ve gereken yetkinlik seviyelerini içeren yol haritasının belirlenmesi,
- Bilişim insan kaynağının etkin bir şekilde yönetilmesi

sağlanmaktadır.

4 BT HİZMETLERİ YETKİNLİĞİ

BT Hizmetleri Rehberleri, BT sistemleri için standartlaştırılmış koruma gereksinimlerini ve bu gereksinimleri karşılamak için gerekli uygulama faaliyetlerini açıklar. Bu rehberlerin amacı, kamu kurumlarına BT hizmetleri alanında yol göstermek; "Ağ ve İletişim", "Veri Merkezi", "BT Sistemleri" ve "Uygulamalar" kabiliyetleri bazında tespit edilen seviyelendirilmiş sorular ile kurumların mevcut olgunluğuna ve bu olgunluğu geliştirmeye yönelik bilgiler sunmaktır. Böylece, bu kabiliyet için öncelikli yapılması veya kontrol edilmesi gereken noktalar ve bundan sonra uygulanması gereken faaliyetler sıralı bir şekilde verilmektedir. Bu sayede, bir yol haritası da sunulmaktadır. Bu anlamda bu rehber, kurumun olgunluk seviyesini artırmaya yönelik sürekli kullanılabilecek bir rehber olma özelliği taşımaktadır.

Her konu, temel bileşen (açıklamalar, riskler ve gereksinimler) ve buna ek olarak uygulama rehberlerinden (gereksinimlerin nasıl karşılanacağına dair talimatlar) oluşur.

Bu rehberler, korunma gereksinimlerini basit ve ekonomik bir şekilde oluşturmayı mümkün kılmaktadır. Geleneksel risk analizi yöntemi ilk olarak tehditleri tanımlar ve bunların meydana gelme olasılıkları ile değerlendirir, ardından uygun güvenlik önlemlerini seçer ve sonra kalan riski değerlendirir. Bu adımlar, BT hizmetlerinin her temel bileşen rehberi içerisinde zaten yapılmıştır. Rehberler içerisindeki standartlaştırılmış güvenlik gereksinimleri, BT çalışanları tarafından kendi kurumsal koşullarına uyan koruma önlemlerine kolay bir şekilde dönüştürülebilir. Rehberlerde uygulanan analiz yöntemi, temel bileşenlerde önerilen güvenlik gereksinimleri ile mevcut durumun karşılaştırılmasını mümkün kılmaktadır.

BT hizmetleri rehberlerinde belirtilen gereksinimleri, yeterli düzeyde korunma amaçlı uygulanmalıdır. Bu gereksinimler; 1. seviye koruma, 2. seviye koruma ve 3. seviye koruma olarak ayrılmıştır. 1. seviye gereksinimler, sistemlerin korunması için gerekli asgari/temel ihtiyaçları içerir. Başlangıç olarak kullanıcılar, en önemli gereksinimleri öncelikli karşılamak için kendilerini 1. seviye gereksinimlere göre sınırlandırabilirler. Ancak, yeterli korunma yalnız 2. seviye gereksinimlerin uygulanmasıyla sağlanacaktır. 3. seviye koruma gereksinimleri için örnek olarak, uygulamada kendini kanıtlamış ve kurumun daha fazla korunma gereksinimi durumunda, kendini nasıl emniyet altına alabildiğini göstermektedir.

Yüksek gereksinimler, ele alınması gereken 3. seviye güvenlik eksikliklerini gösterir. Yüksek gereksinim hedefleri, bir taraftan sistemlerin en iyi şekilde korunması sağlar diğer tarafta uygulamada ve bakımda önemli ölçüde maliyetleri artıracaktır. Bundan dolayı yüksek koruma gereksinimleri hedefleniyorsa, maliyet ve etkililik yönleri dikkate alınarak bireysel bir risk analizi yapılmalıdır. Bu rehberlerde yer alan 1. ve 2. seviye gereksinimlerin

uygulanması ve bu yöndeki ihtiyaçların giderilmesi, kurumun veya organizasyonun hedefleri doğrultusunda yeterlidir.

Temel bileşen rehberlerine ek olarak oluşturulan uygulama rehberleri, hedeflenen gereksinimlerin en iyi şekilde nasıl uygulanabileceğine dair ek bilgiler içerir. Bu rehberlerde yer alan 1. ve 2. seviye gereksinimlerin yerine getirilmesi, ISO 27001 sertifikasının alınması sürecine katkı sağlayacaktır.

4.1 YÖNTEM

BT Hizmetleri yetkinliğinde hazırlanan **Aktif Dizin Rehberi** çalışmaları sırasında, uluslararası boyutta hazırlanmış ve bu alanda kabul görmüş çeşitli standartlar ve çerçevelerden faydalanılmıştır.

Faydalanılan kaynaklar şunlardır:

- Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) [Ref 1], Amerika Birleşik Devletleri.
- Bilgi Teknolojileri Güvenliği Enstitüsü (BSI) [Ref 2], Almanya.
- ISO 27001 [Ref 3]: Bilgi Güvenliği Yönetimi Sistemi gereksinimlerini tanımlayan uluslararası denetlenebilir standarttır.
- ISO 27002 [Ref 4]: Bilgi Güvenliği Yönetim Sistemine ait iyi uygulama örneklerini içeren dokümandır.

Özellikle **Rehberde** detaylandırılacak alt kabiliyetlerin belirlenmesi için IT-Grundschutz BSI, ISO 27001 ve ISO 27002 temel alınmıştır. Türkiye'nin yapısına uygun uluslararası model ve standartlar örnek alınarak ilgili temel başlıklar oluşturulmuş ve kabiliyetler üzerinden **Rehberin** yapısı belirlenmiştir.

4.2 REHBER YAPISI

Her kabiliyet, temel bileşen (açıklamalar, riskler ve gereksinimler) ve buna ek olarak uygulama rehberlerinden (gereksinimlerin nasıl karşılanacağına dair talimatlar) oluşur.

TEMEL BİLEŞEN YAPISI

Temel bileşenler, ilgili konunun prosedürlerini ve açıklamalarını içermekte, risklere ve bileşenin korunmasını sağlamaya yönelik özel gereksinimlere kısa bir genel bakış sunmaktadır. Ayrıca BT bileşenleri, aynı fihrist/dizin yapısında düzenlenmiştir. Temel bileşen yapısı aşağıdaki gibi oluşturulmuştur:

- **Bölüm 1 – Açıklama:** Bileşenin konusu açıklanmaktadır.
    - **1.1 Tanım**: Bileşenin kısa tanımıdır.

- **1.2 Hedef**: Bu bileşenin uygulanmasıyla ne tür güvenlik kazanımlarının sağlanacağı hedefler verilmektedir.
- **1.3 Kapsam Dışı**: Bileşende ele alınmayan kapsamın yanı sıra hangi bileşenin konusu olduğu gibi bilgiler yer alır.

- **Bölüm 2 – Risk Kaynakları**
  - Temel bileşene ait özet riskler anlatılmaktadır. Bunlar, sistemlerin kullanımında önlem alınmadığı takdirde ortaya çıkabilecek güvenlik sorunlarının bir resmini çizer. Olası risklerin açıklanması, kullanıcının konu hakkındaki bilinç düzeyini artırır.
- **Bölüm 3 – Gereksinimler**
  - **3.1 1. Seviye Gereksinimler:** Kurumlar öncelikli olarak bu başlık altında yer alan maddeleri zorunlu olarak değerlendirmelidir .
  - **3.2 2. Seviye Gereksinimler:** İhtiyaçlar doğrultusunda bu standart gereksinimlerin yerine getirilmesi tavsiye edilir.
  - **3.3 3. Seviye Gereksinimler:** Yüksek gereksinim maddeleri bu alt başlıkta sunulmaktadır.
- **Bölüm 4 – Detaylı Bilgi için Kaynaklar**
  - Rehberlerde kullanılan ve referans alınan kaynakları içermektedir.

BT Hizmetleri rehberleri içerdikleri konular itibari ile birbirleri arasındaki ilişkinin kurulması için bir referanslama metodu kullanılmıştır. Bu amaçla her gereksinim maddesi numaralandırılmıştır. Örneğin, BT Hizmetleri rehberlerinde yer alan UYG.2.2.G1 kod tanımı aşağıdaki şekildedir:

Tablo 1. Örnek Kod Tanımı

"Uygulama" kabiliyet grubu için kullanılan kısaltma	**"Dizin" kabiliyeti için atanan numara**	**"Aktif Dizin" alt kabiliyeti için atanan numara**	**1. Gereksinim maddesi**
UYG	2	2	G1

Gereksinim maddelerinin detaylı açıklamalarının yer aldığı uygulama rehberlerinde ise yalnız "G" harfi yerine "U" harfi kullanılmıştır. Örneğin, UYG.2.2.G1 gereksinim maddesinin karşılığı UYG.2.2.U1 olarak geçmektedir.

Ayrıca madde başlıklarında, köşeli parantez içinde madde konusundan ana sorumlu/önerilen kişiler verilmektedir. Bu şekilde, kurum içerisinde hangi role sahip kişilerin ilgili maddenin uygulamasından sorumlu olduğu açıklanır. Kurumdaki konuyla ilgili uygun kişiler, bu roller yardımıyla tespit edilebilir.

UYGULAMA REHBER YAPISI

BT hizmetlerinin temel bileşenleri için ayrıntılı uygulama talimatları (öneriler ve tecrübe edilmiş pratikler) bu rehberlerde detaylandırılmıştır. Bunlar, gereksinimlerin nasıl uygulanabileceğini ve uygun korunma önlemlerini ayrıntılı olarak açıklar. Korunma konseptleri için bu tür önlemler bir temel olarak kullanılabilir, ancak ilgili kurumun hedef ve koşullarına uyarlanmalıdır.

- **Bölüm 1 – Açıklama:** Bileşenin konusu açıklanmaktadır.
    - **1.1 Tanım:** Bileşenin detaylı tanımıdır.
    - **1.2 Yaşam Döngüsü:** Uygulama rehberleri “Planlama ve Tasarım”, “Tedarik”, “Uygulama”, “Operasyon”, “Elden Çıkarma” ve “Acil Durum Hazırlık” gibi aşamalardan oluşan yaşam döngüsüne yönelik önlemlerin genel resmini içerir.
- **Bölüm 2 – Uygulamalar:**
    - **2.1 1.Seviye Uygulamalar:** Kurumlar öncelikli olarak bu başlık altında yer alan maddeleri zorunlu olarak değerlendirmelidir.
    - **2.2 2.Seviye Uygulamalar:** İhtiyaçlar doğrultusunda bu standart gereksinimleri yerine getirilmesi tavsiye edilir.
    - **2.3 3.Seviye Uygulamalar:** Yüksek gereksinim maddeleri bu alt başlıkta sunulmaktadır.
- **Bölüm 3 – Detaylı Bilgi için Kaynaklar**
    - Rehberlerde kullanılan ve referans alınan kaynakları içermektedir.

Uygulama rehberlerinde yer alan gereksinimlere ait hazırlanan kontrol soruları **EK-A**’da verilmektedir.

4.3 KABİLİYET GRUPLARI

BT Hizmetleri yetkinliğinde ele alınan kabiliyet gruplarının açıklaması ve altlarındaki kabiliyetler şu şekildedir:

Şekil 7. BT Hizmetleri Yetkinliği Kabiliyet Grupları

- **Veri Merkezi;** Veri merkezi kapsamında, kritik BT bileşenlerini içeren kurumun yapısal-teknik koşullarının yanında, altyapı güvenliği ile ilgili yönlerini de irdeler. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
  - Genel Bina
    - Veri merkezi içerisinde bulunan binalar için, genel bina önlemleri en az bir kere uygulanmalıdır.
  - Veri Merkezi ve/veya Sistem Odası
    - Veri merkezi ve/veya sistem odası modülü, kurumun kritik odaları için uygulanmalıdır.
    - Kurum/organizasyon erişilebilirlik hedeflerine veya organizasyon boyutuna göre bu tür alanlar, rehber içeriğinde kritiklik düzeyine göre özelleştirilerek verilmiştir.
  - Elektrik Kablolama
    - Veri merkezini ve kritik bileşenleri besleyen güç kaynaklarının hedeflenen erişilebilirlik prensipleri doğrultusunda en az bir kere uygulanması gereklidir.
  - BT Kablolama
    - Kural olarak bu modül veri merkezinin içerisinde yer alan bina veya yerleşke için en az bir kere uygulanmalıdır. Ayrıca veri merkezi için de kullanılabilir.
- **Ağ ve İletişim;** Ağ ve iletişim hizmetlerinin planlanması ve güvenli bir şekilde yönetilmesi için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
  - Ağ
    - Ağ Mimarisi ve Tasarımı ile Ağ İşletimi konularındaki kabiliyetleri içermektedir.
  - Kablosuz Ağlar
    - Kablosuz Ağların Kullanımı ve İşletimi konularındaki kabiliyetleri

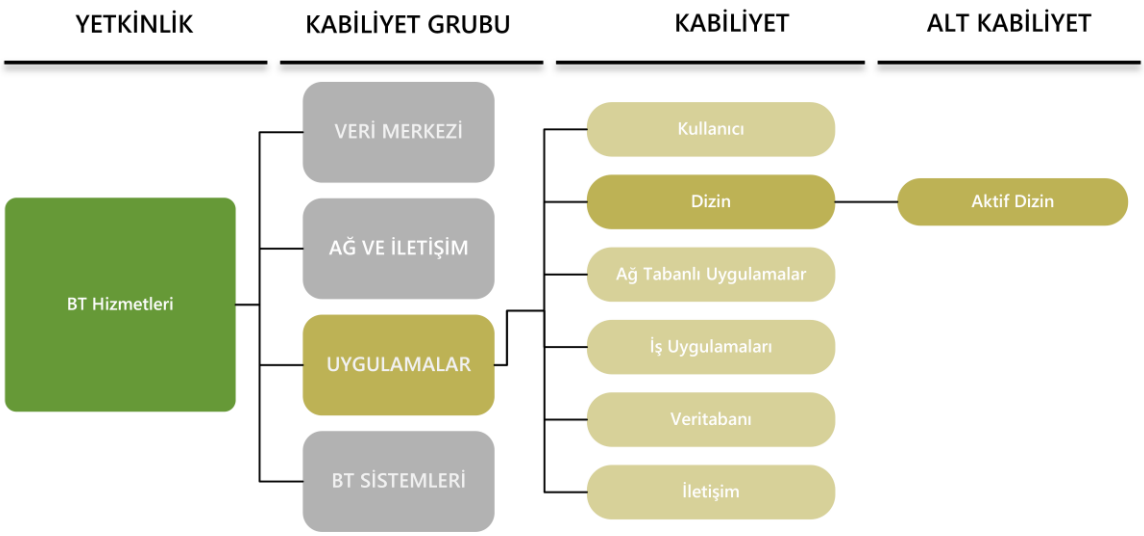
içermektedir.

- Ağ Bileşenleri
  - Yönlendirici ve Ağ Anahtarlama Cihazı, Güvenlik Duvarı, VPN ve IDS/IPS konularındaki kabiliyetleri içermektedir.
- Telekomünikasyon
  - PBX, VOIP, Fax ve Video Konferans konularındaki kabiliyetleri içermektedir.

- **Uygulamalar;** BT hizmetlerinde kullanılan çeşitli uygulamaların planlanması ve güvenli bir şekilde yönetilmesi için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan temel kabiliyetler:
  - Kullanıcı
    - Bu kabiliyet, tüm kurum veya organizasyonda kullanılan ofis uygulamalarını, web tarayıcılarını ve/veya mobil uygulamalarını içerir.
  - Dizin
    - Kurum veya organizasyonda kullanılan dizin hizmetine (Active Directory, OpenLDAP vs.) özel kabiliyetleri kapsar.
  - Ağ Tabanlı Uygulamalar
    - BT sistemlerinde kullanılan web hizmetleri (ör. İntranet veya internet), web sunucusu, dosya paylaşımı, DNS hizmetleri gibi kabiliyetleri kapsar.
  - İş Uygulamaları
    - Kurum veya organizasyon genelinde, kurumsal kaynakların yönetimi için iş birimleri tarafından kullanılan uygulamalara özel kabiliyetleri içerir.
  - Veritabanı
    - Belli bir amaca yönelik düzenli, büyük miktarda veriyi depolayabilen, bu verilerin hızlı bir şekilde yönetilip değiştirilebilmesine ve raporlanmasına imkan sağlayan ilişkisel veya ilişkisel olmayan veritabanı uygulamalarına dair kabiliyetleri içerir.
  - İletişim Uygulamaları
    - Organizasyon genelinde, çalışanların iletişim amaçlı kullandıkları uygulamalara dair kabiliyetleri kapsar.

- **BT Sistemleri;** BT hizmetlerinde kullanılan sistemlerin planlanması ve güvenli bir şekilde yönetilmesi için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan temel kabiliyetler; sunucu, sanallaştırma, istemci, mobil cihazlar ve çevresel cihazlardır.

5 KABİLİYETLER



Şekil 8. Kabiliyetler

UYG: UYGULAMALAR

UYG.2.2.G AKTİF DİZİN

TEMEL BİLEŞEN REHBERİ

UYG.2.2.G AKTİF DİZİN TEMEL BİLEŞEN

1 AÇIKLAMA

1.1 TANIM

Active Directory (rehber içeriğinde “AD” olarak kullanılacaktır), Microsoft Firması tarafından geliştirilen ve ilk olarak Windows 2000 Server işletim sistemi ile tanıtılan bir dizin hizmetidir. Microsoft Windows 2000 Server işletim sisteminin AD yetenekleri temel alınmakla birlikte, Windows Server ailesinin her yeni sürümünde AD hizmetine, ilave özellikler eklenmiştir.

AD, ağırlıklı olarak Microsoft bileşenleriyle çalışan BT ağlarında kullanılır. AD, bir BT ağında yer alan kullanıcı veya bilgisayar gibi nesneler hakkındaki bilgileri depolar ve bu bilgilerin sistem yöneticileri tarafından kullanılabilmesine, düzenlenebilmesine ve izlenebilmesine olanak sağlar. Nesne tabanlı bir dizin hizmeti sunan AD, gerçek ağ ortamını oluşturan nesnelerin ve bu nesnelerin birbirleriyle olan ilişkilerinin yönetilebilmesini mümkün kılar. Ayrıca AD, ilgili ağ için merkezi kontrol ve izleme olanağı sağlar. Böyle bir dizin hizmeti kullanımı, özellikle de BT ağında yer alan istemci sayısının fazla olduğu ve merkezi olmayan bir yönetim şeklinin benimsendiği durumda yaşanabilecek zorlukları azaltma açısından faydalı olur. Dizin hizmetinin kullanılmadığı bir ortamda, yerel olarak yapılandırılan ayarların (ör. güvenlik gereksinimlerine dair ayarlar) güvenilirliği, garanti edilememektedir. Parola yönetimi, hesap oluşturma ve erişim hakları gibi yönetimsel görevler, dizin hizmeti kullanılarak daha verimli bir şekilde gerçekleştirilebilir.

1.2 HEDEF

Bu rehber, AD hizmetinin güvenli bir şekilde kullanılmasını sağlamayı amaçlamaktadır.

1.3 KAPSAM DIŞI

Bu rehber, AD'ye özgü tehdit ve önlemleri içerir. Bununla birlikte, AD'nin işletimi ve yönetimi için kullanılan sunucu ve istemcilerin işletim sistemleri ile temel ağ altyapısının güvenliğini sağlamaya yönelik gereksinimleri bu rehberin konusu değildir. Veri yedekleme ve yama yönetimi gibi işlemler ise, yalnızca AD alanındaki özelliklerinin dikkate alındığı şekli ile kapsama dâhil edilmiştir.

2 RİSK KAYNAKLARI

Aşağıdaki özel tehdit ve güvenlik açıkları, UYG.2.2 AD modülü açısından özel bir öneme sahiptir:

2.1 GÜVENLİK SINIRLARININ YETERSİZ ŞEKİLDE PLANLANMASI

AD, içerisinde barındıracağı tüm etki alanlarını kapsayan bir ağaç yapısı oluşturur. Bir ağaç yapısı; ortak bir mantıksal yapı, global katalog, şema ve otomatik geçişken güven ilişkileri paylaşan bir veya daha fazla etki alanı nesnesi içerebilir. Böylece ağaç yapısı, bilginin AD içerisinde varsayılan olarak iletildiği güvenlik sınırını temsil eder. Eğer bu sınırlar, bilinçli ve yapılandırılmış bir mimaride planlanmaz ise bilgi istenmeyen şekilde dışarı sızabilir ve bu durum, kurumun güvenlik yapısında zafiyet oluşturur. Bu nedenle, altyapının bazı bölümlerine farklı güvenlik politikaları uygulama gereksinimi var ise, AD mimarisinde birden fazla ağaç yapısı tasarlamak gerekebilir. Ancak bu yapı, kurulum ve yönetim süreçlerine karmaşıklık ekleyeceği için yönetimi zorlaştırabilir.

2.2 GÜVEN İLİŞKİSİNİN BİRDEN ÇOK OLMASI VEYA YETERİNCE SIKILAŞTIRILMAMA DURUMU

Eğer ağaç yapıları ve etki alanları arasında yer alan güven ilişkileri; hala gerekli olup olmadıkları, doğru tipte tanımlanıp tanımlanmadıkları (ör. gerçekten iki yönlü güven ilişkisi ihtiyacının olup olmadığı) ve güvenlik kontrollerinin yeterli olup olmadığını garanti etmek için düzenli bir şekilde gözden geçirilmez ise, yetki sorunları oluşur ve bu durum istenmeyen bir bilgi akışına sebep olabilir. Özellikle, varsayılan aktif SID (Güvenlik Tanımlayıcısı) filtrelemesi devre dışı bırakılmış ise; karmaşık ve/veya kolayca saptanamayan güvenlik açıkları oluşabilir.

Aynı durum, ağaç yapıları arasındaki seçici kimlik doğrulama yöntemini kullanan güven ilişkileri için de geçerlidir.

2.3 GÜVENLİK ÖZELLİKLERİNİN YETERSİZLİĞİ

Her yeni nesil Windows Sunucu işletim sistemi, AD'ye ek güvenlik özellikleri ve geliştirmeler getirmektedir. Ayrıca, varsayılan ayarlar genellikle her yeni sürümde daha da güvenli hale getirilmektedir. Bu özelliklerden bazıları sadece yeni sürüme geçildiğinde, bazıları ise sadece etki alanı/ağaç yapısı seviyesi yükseltildiğinde kullanılabilir. (Birincil) etki alanı denetleyicisi rolüne sahip olan sunucunun işletim sisteminin güncel olmaması veya etki alanı seviyesinin düşük kalmış olması, güncel güvenlik özelliklerinin kullanılmasına engel olur ve güvenli olmayan varsayılan ayarların kullanım riskini artırır. Güvenli bir şekilde yapılandırılmamış bir etki alanı, içerdiği bilgileri tehlikeye atar ve üçüncü partiler tarafından gerçekleştirilebilecek saldırıların başarı olasılığını artırır.

2.4 ETKİ ALANI DENETLEYİCİSİ SUNUCULARINDA DİĞER ROL VE HİZMETLERİN ÇALIŞMASI

Etki alanı denetleyicisi rolüne sahip olan sunuculara, AD servislerinden farklı servislerin ve rollerin yüklenmesi, (servis etki alanı için gerekli olan DNS servisi dahi olsa) yanlış yapılandırılma olasılığını yükseltir, üçüncü partilere karşı saldırı yüzeyini genişletir ve ek güvenlik zafiyetlerine sebep olabilir. Bu durum, bilinçli veya bilinçsizce istismar edilebilir (ör. yetkisiz bir şekilde bilginin kopyalanması veya değiştirilmesi).

2.5 ETKİ ALANI YÖNETİCİLERİ (DOMAİN ADMİNS) GRUBUNUN KÖTÜ AMAÇLI KULLANILMASI

AD, çok az sayıda yönetici tarafından yönetilmelidir. Ancak çoğu zaman, gerçek ihtiyaçtan daha fazla etki alanı yöneticisi (*Domain Admin*) hesabı bulundurulur. Bu hesaplar; tüm etki alanı denetleyicileri, istemciler, grup ilkeleri, vb. nesneler üzerinde tam yetkiye sahiptirler. Bu hesaplardan herhangi birinin ele geçirilmesi saldırganların işini kolaylaştıracaktır. Genellikle etki alanı yöneticileri grubu, AD'nin yönetimine doğrudan dâhil olmayan hizmet hesaplarını ve diğer grupları da içerir.

2.6 YETKİLENDİRİLMİŞ HAKLARIN İZLENMESİNİN VE DOKÜMANTE EDİLMESİNİN YETERSİZLİĞİ

Bireysel kullanıcıların ve grupların yetkilendirme sürecinin sistematik bir şekilde planlanmaması ve uygulanmaması durumunda, delegasyon kontrolden çıkabilir. Hedeflenenden daha fazla yetkinin devredilmesi, üçüncü şahıslar tarafından kötüye kullanılabilir. Grupların ve yetkilerin düzenli bir şekilde denetlenmemesi, bu yetkilerin zaman içerisinde tehdit oluşturmasına yol açabilir. Standart grupların kullanımı ve bu gruplara ait hakların bireysel olarak tanımlanan gruplara direkt olarak devredilmesi (örneğin, çağrı merkezi operatörlerine varsayılan etki alanı grubu olan “Account Operators” grubu yetkilerinin delegasyonu), genellikle ihtiyaç duyulandan daha fazla yetkinin tanımlanan gruba verilmesine neden olur.

2.7 GÜVENLİ OLMAYAN KİMLİK DOĞRULAMA

LM (LAN Manager) ve NTLM (NT LAN Manager) v1 gibi güncel olmayan kimlik doğrulama mekanizmaları, günümüzde güvensiz kabul edilir ve belirli koşullar altında saldırganlar tarafından kolayca istismar edilebilir. Saldırgan bu zafiyetten faydalanarak; kullanıcı parolalarını bilmeden, tahmin etmeden veya bir şekilde kırmadan, etki alanında yetki elde edebilir ve bu yetkiyi kötüye kullanarak etki alanının tamamında veya bir kısmında istenmeyecek olaylara yol açabilir.

2.8 AD YÖNETİCİLERİNİN GÜVENLİK SEVİYESİ DÜŞÜK OLAN SİSTEMLERDE OTURUM AÇMASI

Zararlı kodun, istemciler veya sunucular gibi farklı sistemlerde bulunabileceği varsayımı ile önlem alınmalıdır. Zararlı kod kullanarak ilk erişimi sağlayan bir saldırgan, kötüye kullanabileceği diğer kimlik bilgilerini arayabilir. Ayrıcalıklı hesapların, güvenlik seviyesi düşük, farklı BT sistemlerine giriş yapması durumunda (özellikle kimlik bilgilerinin önbelleğe alındığı bir ortamda) saldırgan, kimlik bilgilerini elde etmek ve ek ayrıcalıklar kazanmak için bir fırsata sahip olacaktır.

2.9 AYRICALIKLI GRUP ÜYELİKLERİNİN DENETİM EKSİKLİĞİ

Çoğu kurumda, yönetimsel haklara sahip olan hesapların sayısı gün geçtikçe artmaktadır ve bu durum nadiren düzenlenmekte ya da hiç düzenlenmemektedir. Bu tür bir uygulama, en az ayrıcalık ilkesini ihlal eder; saldırganların ek yetkilere sahip olmaları ve bunları kötüye kullanmaları için daha fazla fırsat oluşturur.

2.10 AYRICALIKLI YETKİLERE SAHİP OLAN VEYA SIKILAŞTIRILMAMIŞ SERVİS HESAPLARI

Uygulama yazılımı tedarikçileri, ürünlerinin test işlemlerini basitleştirmek ve dağıtımını kolaylaştırmak için (daha az yetkinin çoğunlukla yeterli olacağı durumlarda dahi), genellikle servis hesaplarında etki alanı yöneticisi (domain admin) yetkilerini talep ederler. Servis hesabına verilecek ek yetkiler, saldırganlar tarafından etki alanını ele geçirme amacıyla kullanılabilir. Servis hesabı kimlik bilgileri, LSASS'ın korunan depolama alanında tutulduğu için, saldırgan bu bilgileri ele geçirebilir. Örneğin, güvenlik seviyesi düşük bir BT sisteminde kullanılan tek bir hizmet hesabı, tüm etki alanını tehlikeye atabilir.

Bu durum özellikle, servis hesabı için zayıf bir parola kullanıldığında ortaya çıkmaktadır. Bir saldırgan, Kerberos kimlik doğrulaması kullanımında, servis hesabının parolasının işlendiği TGS (Ticket Granting Service) isteğinde bulunabilir ve bu istek sonrası kendisine gönderilen cevap paketini kullanarak, kaba kuvvet saldırısı yöntemi ile parolayı ele geçirebilir.

2.11 AYNI YEREL YÖNETİCİ PAROLASININ BİRÇOK FARKLI SİSTEMDE KULLANILMASI

Yerel hesaplar kullanılarak, etki alanı ile iletişimi olmayan bir sistemde oturum açılabilir. Yerel hesap kimlik bilgilerinin, birden fazla sistemde aynı biçimde (aynı kullanıcı adı ve parola ile) tanımlanmış olması durumunda, bir saldırgan, herhangi bir sistemde ele geçirdiği ayrıcalıklı yetkilere sahip olan kimlik bilgilerini, başka sistemleri istismar etme amacı ile kullanabilir.

2.12 KULLANILMAYAN HESAPLARIN AD'DEN KALDIRILMASI

Saldırganlar, amaçlarına yönelik olarak, aktif olarak kullanılmayan, ancak hala AD içerisinde yer alan hesapları kullanmayı tercih ederler. Çünkü bu hesapların bir sahibi bulunmadığı ve kullanımları genellikle denetlenmediği için istismar edilmeleri durumu uzun süre fark edilmeyebilir.

3 GEREKSİNİMLER

UYG.2.2 AD rehberinin özel gereksinimleri aşağıda listelenmiştir. Temel olarak BT Operasyon Ekibi, gereklilikleri karşılamaktan sorumludur. Bilgi Güvenliği Birimi her zaman stratejik kararlarda yer almalıdır. Buna ek olarak, Bilgi Güvenliği Birimi tüm ihtiyaçların belirlenen güvenlik politikasına uygun olarak karşılanmasını ve doğrulanmasını sağlamaktan sorumludur. Ayrıca, gereksinimlerin uygulanmasında ilave sorumlulukları olan başka roller de olabilir. Bunlar daha sonra ilgili gereksinimlerin başlığında köşeli parantez içinde açıkça listelenecektir.

Rehber içerisinde gereksinimler, üç ana başlık altında toplanmıştır. Kurumların öncelikli olarak "1.Seviye Gereksinimler" başlığı altında yer alan maddeleri zorunlu olarak değerlendirmeleri, sonra ihtiyaçları doğrultusunda "2.Seviye Gereksinimler" ve "3. Seviye Gereksinimler" başlıklarını ele almaları önerilmektedir

Tablo 2. Active Directory Rol Listesi

Temel Bileşen Sorumlusu/Sahibi	BT Operasyon Ekibi
Diğer Sorumlular	Bina Hizmetleri, BT Yöneticisi, BT Mimari

3.1 1.SEVİYE GEREKSİNİMLER

AD için aşağıda listelenen gereksinimler öncelikli olarak uygulanmalıdır.

UYG.2.2.G1 AD'nin planlanması [Sorumlu Teknik Uzman]

Planlamada, mümkün olan en yüksek etki alanı seviyesi seçilmelidir. Tasarıma etki eden gerekçeler dokümante edilmelidir. Talep ve ihtiyaç tabanlı bir AD yetkilendirme modeli tasarlanmalıdır. Yönetimsel delegasyonlar, kısıtlı ve ihtiyaca yönelik izinler verilerek sağlanmalıdır. Planlanan AD yapısı (şema değişikliklerini de içeren hali ile), izlenebilir bir şekilde dokümante edilmelidir.

UYG.2.2.G2 AD yönetiminin planlanması [Sorumlu Teknik Uzman]

Rol tabanlı bir yetkilendirme modeli oluşturulmalıdır. Tüm yönetimsel görevlerin ve yetkilerin uygun şekilde dokümante edilmesi tavsiye edilir.

Geniş etki alanlarında yönetimsel kullanıcılar, AD'nin servis yönetimi veya veri yönetimi görevlerini gerçekleştirecek şekilde ayrıştırılmalıdır. Ayrıca, AD'deki yönetimsel görevlerin benimsenen yetkilendirme modeline göre farklı görevler ile çakışmadan dağıtılması gerekmektedir.

UYG.2.2.G3 Grup ilkelerinin planlanması

Grup ilkeleri için öncelikle bir strateji oluşturulmalı ve planlama yapılmalıdır. Grup ilkeleri planlanırken olabildiğince örtüşmelerinden kaçınılmalıdır. Grup ilkesi stratejisi dokümantasyonunda, istisna kurallar açıkça belirtilmelidir. Oluşturulan tüm GPO'lar (Group Policy Object) kısıtlayıcı erişim hakları ile korunmalı ve GPO'lardaki parametreler güvenli ayarlara sahip olmalıdır.

UYG.2.2.G4 AD yönetimi eğitimi

AD'yi yönetecek kişiler, AD'deki faaliyet alanlarını ve tüm güvenlik özelliklerini bilmelidirler. AD'nin kurulumu öncesinde; AD kurulumu, yapılandırılması ve işletimi için gerekli eğitimlerin ilgili kişiler tarafından alınması gerekmektedir.

UYG.2.2.G5 AD'nin sıkılaştırılması

Varsayılan hesaplar (Built-in Accounts), karmaşık parolalara sahip olmalı ve sadece acil durum hesapları olarak kullanılmalıdır. Ayrıcalıklı hesaplar, "Protected Users" grubunun üyeleri olmalıdır. Servis hesapları, "(Group) Managed Service Accounts" şeklinde kullanılmalıdır.

Tüm etki alanı denetleyicileri için, işletim sistemi düzeyinde kısıtlayıcı erişim hakları atanmalıdır. AD Geri Yükleme Modu güçlü bir parola ile korunmalıdır. Bu moddaki çalışmalar, dört göz ilkesi (iki kişi tarafından kontrol edilmesi) ile uyumlu olarak yapılmalıdır.

Periyodik olarak etki alanı denetleyicisinin bir imajı oluşturmalıdır. "Everyone" grubunun izinleri sınırlı olmalıdır. Etki alanı denetleyicileri, yetkisiz yeniden başlatmalara karşı korunmalıdır.

Etki alanı ve etki alanı denetleyicisi grup politikaları; güvenli parola ve hesap kilitleme ilkeleri, Kerberos kimlik doğrulama ayarları, kullanıcı hakları ve denetimi hususlarını içermelidir. Etki alanı denetleyicisinin güvenlik günlüğü için uygun bir boyut ayarlanmalıdır. Diğer alanlara yapılan dış bağlantılar için kullanıcı yetkilendirme verileri filtrelenmeli ve anonimleştirilmelidir.

UYG.2.2.G6 AD'nin operasyonel güvenliğini sağlamak

AD'deki tüm güven ilişkileri düzenli olarak değerlendirilmelidir.

Servis yöneticisi hesapları, yalnızca gerekli haklara sahip olmalıdır. Bu haklar periyodik olarak gözden geçirilmelidir. "Domain Admins" grubu (ve üyeleri) yalnızca kurulum ve felaket durum senaryolarında kullanılacak şekilde bir planlama yapılmalıdır. Rutin yönetim işleri açısından kullanılacak hesaplar "Domain Admins" grubuna üye yapılmamalıdır

(sadece varsayılan “Administrator” hesabı için belli koşullarda istisna yaratılabilir). Kullanılmayan hesaplar AD'de devre dışı bırakılmalı ve uygun zaman sonrasında silinmelidir.

Gerekli tüm AD parametreleri, güncel ve izlenebilir olmalıdır.

UYG.2.2.G7 AD için güvenli yönetim yöntemlerinin uygulanması [Sorumlu Teknik Uzman]

AD işletimi için kullanılacak yönetici hesapları, rutin günlük işler için kullanılmamalıdır. Sunucu yöneticisi hesapları, istemcilerde; etki alanı yöneticisi hesapları, istemcilerde veya sunucularda kullanılmamalıdır.

Her hesap, bir çalışana açıkça atanmalıdır.

AD servis yöneticilerinin ve veri yöneticilerinin hesap sayısı, gerekli asgari hesap sayısına indirilmelidir. Hesaplar öncelikli olarak korunmalıdır.

“Administrator” varsayılan hesabı yeniden adlandırılmalı ve “Administrator” adlı ayrıcalıklı olmayan bir hesap oluşturulmalıdır. İşletim ve yönetim ile ilgili olmayan her türlü çalışma için, ayrıcalıklı olmayan kullanıcı hesapları kullanılmalıdır.

Servis yöneticisi hesaplarının yönetiminin, yalnızca servis yöneticisi grubunun üyeleri tarafından yapılması sağlanmalıdır. "Account Operators" grubu boş olmalıdır.

AD yöneticileri, yalnızca şema değişiklikleri süresince “Schema Admins” grubuna geçici olarak atanmalıdırlar. Kök etki alanının yönetiminde "Enterprise Admins” ve “Domain Admins” grupları için dört göz ilkesi kullanılmalıdır.

AD'nin yönetimi için kullanılacak istemciler uygun şekilde korunmalıdır. Etki alanı denetleyicilerinin uzaktan yönetimi için trafik mutlaka şifrelenmelidir.

“Administrators” veya “Domain Admins” gruplarının her bir etki alanına ait etki alanı kök nesnesinin sahipleri arasında yer aldığından emin olunmalıdır.

Nesne özniteliklerini okuma izinlerini denetlemek için ”domain local” grupların kullanımından kaçınılmalıdır.

“AD Recycle Bin” aktif hale getirilmelidir.

Büyük kurumlarda, bir kurumsal kimlik yönetimi çözümü aracılığı ile tüm kullanıcı yetkilerinin, gerekli ihtiyaca yönelik olarak tanımlanması sağlanmalıdır.

3.2 2.SEVİYE GEREKSİNİMLER

1.seviye uygulamalar sonrasında, AD altyapılarını daha iyi bir seviyeye getirmeyi düşünen kurum ve organizasyonlar, aşağıdaki uygulama maddelerini dikkate alarak, iyileştirme/geliştirme faaliyetlerini planlayabilirler.

UYG.2.2.G8 Windows ortamında güvenli kanal yapılandırması

Windows ortamında verilerin güvenli şekilde iletilebilmesi için kullanılan iletişim kanalı, güvenlik gereksinimleri ve yerel koşullara göre yapılandırılmalıdır. İlgili tüm grup politikası parametreleri dikkate alınmalıdır.

UYG.2.2.G9 AD kullanımında kimlik doğrulamanın korunması

AD ortamında, Kerberos kimlik doğrulama protokolü kullanılmalıdır. Uyumluluk gereksinimleri nedeniyle NTLMv2 kullanılıyorsa, Kerberos'a geçiş yapılması mutlaka planlanmalıdır. Ayrıca, LM kimlik doğrulaması devre dışı bırakılmalı ve SMB trafiği imzalanmalıdır. Etki alanı denetleyicilerine anonim erişim de engellenmelidir.

UYG.2.2.G10 AD ortamında DNS'nin güvenli işletimi

Yetkisiz sistemlerden yapılacak DNS istemci sorgularının engellenmesi için tümleşik DNS bölgeleri (Integrated DNS zone) veya DNS kayıtları için güvenli dinamik güncelleme (secure dynamic update) yöntemi kullanılmalıdır. DNS sunucusunun yapılandırma verilerine yalnızca yönetim hesaplarının erişmesine izin verilmelidir. DNS sunucularındaki DNS önbelleği, yetkisiz değişikliklere karşı korunmalıdır. Etki alanı denetleyicilerinin DNS hizmetine erişimi gerekli ölçüde sınırlandırılmalıdır. DNS istekleriyle ilgili ağ etkinlikleri izlenmelidir. AD'deki DNS verilerine erişim, erişim kontrol listeleri kullanılarak sadece yöneticilerle sınırlandırılmalıdır.

İkincil DNS bölgelerinden kaçınılmalıdır. En azından, DNS bölgesi bilgilerinin tutulduğu dosya (DNS zone file) yetkisiz erişime karşı korunmalıdır.

DNS iletişimini güvenli hale getirmek için IPsec kullanılıyorsa, ağda ilgili trafik izlenmelidir.

UYG.2.2.G11 AD altyapısını izleme

AD altyapısı, günlük kayıtları temel alınarak izlenmelidir. AD'nin güvenlik gereksinimlerine uyumluluk açısından, izleme sonuçları düzenli olarak değerlendirilmelidir. Etki alanı denetleyicilerinin erişilebilirlikleri ve kaynak kullanım durumları; etki alanı düzeyinde ve AD'de ağaç yapısındaki değişiklikler izlenmeli, kayıt altına alınmalı ve değerlendirilmelidir.

UYG.2.2.G12 Etki alanı denetleyicilerinin yedeklerinin alınması

Kurumda, etki alanı denetleyicisinin yedeğinin alınması ve yedekten geri yüklenmesine dair bir politika bulunmalıdır. Kullanılan yedekleme yazılımı, etki alanı denetleyicilerinin yedeğini alabilme yeteneklerine sahip olmalıdır. Yedekleme işlemi için, servis yöneticisi haklarına sahip ayrı bir yedekleme servis hesabı oluşturulmalıdır. "Backup Operators" grubunun üye sayısı gerekli minimum seviyede tutulmalı, özellikle "AdminSDHolder" nesnesine erişim izinleri hususunda hassas davranılmalıdır.

Etki alanı denetleyicilerinin verileri düzenli aralıklarla yedeklenmelidir. Yedekleme sırasında, uzun süredir kullanılmayan nesnelerin yedeklemeye dâhil edilmemesi sağlanmalıdır.

Yedekleme verisini barındıran medya, uygun bir yerde, uygun bir biçimde muhafaza edilmelidir. Etki alanı denetleyicisi yedeklerine ilişkin geri dönüş testleri, alınan yedeklerin sağlıklı olarak çalıştığının kanıtlanması açısından, düzenli aralıklarla kontrol edilmelidir.

3.3 3.SEVİYE GEREKSİNİMLER

1. ve 2. seviye uygulamalar sonrasında, AD için artan koruma koşullarında dikkate alınması gereken uygulamalar aşağıda yer almaktadır. Kurumların kendi ihtiyaçları doğrultusunda, risk analizi çerçevesinde uygun uygulamalardan faydalanmaları önerilir. Uygulama kapsamında öncelikli koruma sağlanan prensip parantez içinde bulunan harfler ile belirtilmektedir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

UYG.2.2.G13 İki faktörlü kimlik doğrulama (GBE)

AD yönetiminde kullanılan ayrıcalıklı hesaplar iki faktörlü kimlik doğrulama ile korunmalıdır.

UYG.2.2.G14 Ayrıcalıklı yönetici sistemleri (GBE)

AD yönetimi, üzerinde sadece AD yönetimi faaliyetlerinin gerçekleştirilebileceği, bu amaca yönelik olarak tahsis edilmiş sistemler üzerinden gerçekleştirilmelidir. Bu sistemler, güvenlik gereksinimleri açısından özellikle sıkılaştırılmalıdır.

UYG.2.2.G15 Yönetim ve canlı ortamın ayrıştırılması (GBE)

Etki alanı denetleyicileri ve etki alanı yönetimi için tahsis edilmiş sistemlerin, tasarlanacak olan izole bir ağaç yapısı içerisinde konumlandırılması ("Red Forest" mimarisi) ve canlı ortam ağaç yapısından yönetim için oluşturulacak ağaç yapısına doğru tek yönlü bir güven ilişkisinin tahsis edilmesi önerilir.

4 DETAYLI BİLGİ İÇİN KAYNAKLAR

AD ile ilgili detaylı konulara, aşağıdaki referans ve kaynaklardan ulaşılabilir:

- AD Hizmeti
  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services
- AD Federasyon Hizmetleri
  https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services
- AD'nin Güvenliğini Sağlama
  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
- AD'de Ayrıcalıklı hesaplar ve gruplar
  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b--privileged-accounts-and-groups-in-active-directory
- AD'de ayrıcalıklı erişimin güvenli hale getirilmesi
  https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access
- AD Geri Dönüşüm Kutusu'nu Yapılandırma
  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/introduction-to-active-directory-administrative-center-enhancements--level-100-
- AD Antivirüs taramasına dair öneriler
  https://support.microsoft.com/en-us/help/822158/virus-scanning-recommendations-for-enterprise-computers-that-are-runni
- APP.2.2 BSI-IT Grundschutz Active Directory
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_2_2_Active_Directory.html

UYG: UYGULAMALAR

UYG.2.2.U AKTİF DİZİN

UYGULAMA REHBERİ

UYG.2.2.U AKTİF DİZİN UYGULAMA

1 AÇIKLAMA

1.1 TANIM

Active Directory, Microsoft tarafından özellikle Windows sunucu ve istemci bilgisayar sistemleri için tasarlanmış olan; içerisinde kullanıcı, bilgisayar, yazıcı, gruplar gibi nesnelere ilişkin bilgileri tutan bir dizin hizmetidir. Teorik olarak Active Directory, hiyerarşik ve ağaç yapısı şeklinde nesne temelli bir veri tabanıdır. İçyapısı, temel aldığı X.500 dizin hizmeti standardına dayanmaktadır. Ancak, X.500 uyumlu bir dizin hizmeti değildir. Active Directory genellikle "AD" şeklinde kısaltılır.

1.2 YAŞAM DÖNGÜSÜ

Planlama ve Tasarım

Kurum bünyesinde yer alan teknik personelin, Active Directory konusunda yeterince bilgi sahibi olmaması durumunda, Active Directory'nin temel yapısı ve terminolojisine hâkim olunabilmesi için gerekli eğitimlerin düzenlenmesi önerilir (bkz. “UYG.2.2.U4 Active Directory yönetimi eğitimi”).

Active Directory kurulumu öncesi, mümkün olan en iyi tasarımı yapabilmek amacıyla, kurumun organizasyon yapısını detaylı analiz etmek gerekir. “UYG.2.2.U1 Active Directory’nin planlanması” maddesi, planlama aşamasında izlenecek yöntemler hakkında bilgiler içerir.

“UYG.2.2.U2 Active Directory yönetiminin planlanması” maddesi, bir etki alanı yönetiminin temel yapısını ele alır ve her bir yönetim rolünü, faaliyetler ve uygulama alanlar ile ilişkilendirir. Bu madde ayrıca, Active Directory organizasyon yapısı ve yönetim amaçlı kullanılan hesaplara ait yetkilerin özelleştirilmesi konularına da açıklık getirir.

“UYG.2.2.U3 Grup ilkelerinin planlanması” maddesi, Active Directory aracılığıyla yönetilebilen Windows işletim sistemleri için grup ilkelerine dair bilgiler sunar.

Tedarik

Bu rehberde tedarik sürecine ilişkin detaylara yer verilmemiştir. Tedarik sırasında, bazı güvenlik özelliklerinin yalnızca yeni AD sürümlerinin, dolayısıyla yeni sürüm Windows Sunucu işletim sistemlerinin, kullanılması ile uygulanabilir olduğu ve bu durumun, satın alma kararlarını etkileyebileceğine dikkat edilmelidir (bkz. UYG.2.2.U1 Active Directory’nin planlanması).

Uygulama

Tek tip bir güvenlik standardı oluşturmak için, “UYG.2.2.U7 Active Directory için güvenli yönetim yöntemlerinin uygulanması” maddesi gözden geçirilmelidir. Ayrıca, dizin hizmetini yönetmekle sorumlu olan kişiler, kendilerine atanan görevi yerine getirebilmeleri için “UYG.2.2.U4 Active Directory yönetimi eğitimi” maddesinde detaylandırılan, eğitimleri almalıdırlar.

Bir kurumun etki alanı denetleyicileri, tüm ağ ortamı için merkezi öneme sahip olmalarından dolayı, yeterince sıkılaştırılmalıdır (bkz. UYG.2.2.U5 Active Directory’nin sıkılaştırılması). Bu sıkılaştırma işlemi özellikle, etki alanı denetleyicileri, sunucular ve istemciler arasında güvenli iletişim kanallarının oluşturulması (bkz. UYG.2.2.U8 Windows ortamında güvenli kanal yapılandırması) ve kimlik doğrulamanın korunması (bkz. UYG.2.2.U9 Active Directory kullanımında kimlik doğrulamanın korunması) hususundaki uygulamaları içerir.

Active Directory bütünlüğünü, DNS bileşenlerini de güvenli hale getirerek, sağlamak için, “UYG.2.2.U10 Active Directory ortamında DNS'nin güvenli işletimi” maddesi dikkate alınmalıdır.

İşletim

İçerdiği bilginin güncel tutulabilmesi amacı ile üzerinde çalıştığı işletim sistemine ek olarak, Active Directory’nin de hassas bir şekilde yönetilmesi gerekir (bkz. UYG.2.2.U6 Active Directory’nin operasyonel güvenliğini sağlamak).

Active Directory yönetimi esnasında ortaya çıkan sorunları zamanında fark ederek çözümleyebilmek amacıyla, “UYG.2.2.U11 Active Directory altyapısı izleme” maddesi dikkate alınmalıdır. Bu uygulama maddesi, sadece tanımlanmış eşik değerleri aşan durumlarda geri bildirim alınmasını değil, aynı zamanda sistem değişikliklerinin kayıt altına alınmasını da sağlar.

Kullanım Dışı Bırakma

Bu rehberde Active Directory hizmetinin kullanım dışı bırakılmasına dair detaylar ele alınmamıştır.

Acil Durum Hazırlık Planı

Active Directory için acil durum planlama hususları, “UYG.2.2.U12 Etki alanı denetleyicilerinin yedeğinin alınması” maddesinde ele alınmaktadır.

2 UYGULAMALAR

Aşağıda yer alan maddeler, Active Directory hizmetine özel önlem maddeleridir.

2.1 1. SEVİYE UYGULAMALAR

UYG.2.2.U1 Active Directory'nin planlanması [Sorumlu Teknik Uzman]

Active Directory mimarisinin güvenli bir şekilde işletimi için gerekli ön koşul, öncesinde geniş çaplı bir planlamanın gerçekleştirilmesidir. Active Directory için planlama, birden çok adım içerecek şekilde oluşturulabilir. Öncelikle, etki alanı yapısı için genel bir mimari oluşturulur ve buna bağlı alt kırılımlar belirlenir. Planlama, güvenlikle ilişkili hususlar ile birlikte normal operasyonel hususları da kapsamalıdır. Active Directory'nin temel yapısı ile ilgili bilgiler, "UYG.2.2.U4 Active Directory yönetimi eğitimi" maddesinde detaylandırılmaktadır.

Active Directory planlamasının bir parçası olarak:

- Gerekli güvenlik özelliklerinin uygulanabilmesi için Active Directory etki alanında ihtiyaç duyulan fonksiyonel sürüm,
- Active Directory'nin mantıksal yapısı (orman, etki alanı, DNS, vb.) ve site mimarisi,
- Etki alanı denetleyicisi kapasitesi,
- Kullanıcıların ve bilgisayarların, konumlandırılacakları etki alanları

dikkate alınmalıdır.

Her etki alanı için, aşağıdaki konular da detaylandırılmalıdır:

- Active Directory yapısında hangi OU nesnelerinin yer alacağı, nasıl bir hiyerarşide hizmet edecekleri ve içlerinde hangi nesnelerin yer alması gerektiği,
- Hangi güvenlik gruplarına ihtiyaç duyulacağı ve grupların hangi OU'lar altında barındırılacakları,
- Hangi yönetim modelinin uygulanacağı (merkezi / merkezi olmayan yönetim),
- Yönetimsel görevlerin devredilip devredilmeyeceği ve devredilecek ise kime devredileceği,
- Farklı bilgisayar ve kullanıcı gruplarına hangi güvenlik ayarlarının uygulanması gerektiği,
- Hangi GPO ayarlarına ihtiyaç duyulacağı ve GPO'ların nasıl ilişkilendirileceği (bkz. UYG.2.2.U3 Grup İlkelerinin Planlanması),

- Active Directory güven ilişkilerinin hangilerinin varsayılan olarak oluşturulduğu ve hangi ek güven ilişkilerinin oluşturulması gerektiği,
- Active Directory yönetim ara yüzlerine (ADSI, LDAP vb.) hangi kullanıcılar tarafından erişilebileceği,
- "Global Catalog" rolünde hangi nesne bilgilerinin barındırılacağı,

Planlanan Active Directory yapısı, kurum gereksinimlerine ve güvenlik standartlarına uygun olmalı, ayrıca dokümante edilmelidir. Bu yaklaşım, istikrarlı ve tutarlı bir yönetim şeklinin tesis edilmesine (dolayısıyla sistem güvenliğine) önemli ölçüde katkıda bulunur. Şema değişikliklerinin hangi sebeplerle gerçekleştirildiğinin kayıt altına alınması özellikle tavsiye edilir.

İşletim Sistemi Veya Etki Alanı Seviyesine Göre Active Directory Güvenlik İşlevleri

Her yeni nesil Windows Sunucu işletim sistemi, Active Directory'e ek güvenlik özellikleri getirmektedir. Bu özellikler ile birlikte varsayılan ayarlar daha güvenli hale gelir. Bu ayarların bazıları yeni nesil işletim sistem kurulumu sonrası, bazıları ise ancak Active Directory etki alanı ve orman fonksiyonel seviyesi yükseltildiğinde kullanılabilir hale gelmektedir.

Etki alanı, mümkün olan en yüksek fonksiyonel seviyede çalıştırılmalıdır. Etki alanının fonksiyonel seviyesi en azından, ihtiyaç duyulan koruma gereksinimlerinin karşılanabilmesi için, tüm güvenlik işlevlerinin sunulabildiği seviyede olmalıdır. Etki alanı fonksiyonel seviyesi tasarım kararı gerekçeleri ile birlikte alınmalı, dokümante edilmeli ve düzenli olarak gözden geçirilmelidir.

Windows Sunucu sürümlerinin öne çıkan en önemli güvenlik işlevleri ve özellikleri şunlardır:

Windows Server 2008 R2 Etki Alanı Fonksiyon Seviyesi:

- Kerberos AES Şifrelemesi desteği

  Bu özellik, Kerberos'tan RC4 HMAC desteğini kaldırır. Ayrıca, Windows 7 ve Windows Server 2008 R2 artık Kerberos'ta DES'i desteklememektedir.
- Yönetilen Hizmet Hesapları kullanımı (Managed Service Accounts)

  Active Directory, bu tür hizmet hesaplarının parolalarını kendisi yönetir.
- Kimlik Doğrulama Mekanizması Güvencesi (Authentication Mechanism Assurance)

Kullanıcılar, ek grup üyeliklerini ancak akıllı kart ile kimlik doğrulanmasından sonra alırlar.

Windows Server 2012 Etki Alanı Fonksiyon Seviyesi:

- Yönetilen Hizmet Hesapları kullanımı (Group Managed Service Accounts)

  Active Directory, bu tür hizmet hesaplarının parolalarını kendisi yönetir.

- Bileşik Kimlik Doğrulaması ve Kerberos FAST (Kerberos Armoring)
  - Kullanıcı ve kullanıcı cihazı kimlik doğrulamasını birleştirir.
  - Kerberos kimlik doğrulama servisi ve TGT arasındaki iletişimi korur.

Windows Server 2012 R2 Etki Alanı Fonksiyon Seviyesi:

- Kimlik Doğrulama Politikaları

  Oturum açılabilecek sistemleri kısıtlayarak ayrıcalıklı hesapları korur.

- Güvenlik grubu “Korumalı Hesaplar” (Protected Users)
  - Bu özelliğin kullanılabilmesi için birincil etki alanı denetleyicisi (PDC) rolündeki etki alanı denetleyicisinin işletim sistemi Windows 2012 R2 olmalıdır.
  - Korumalı hesapların oturum açtıkları (Windows 8.1 ve Windows 2012 R2 ile birlikte gelen özellik) sistemlerde ve etki alanı denetleyicilerinde, aşağıdaki hususlar önlenir:
    - NTLM, Özet Kimlik Doğrulaması veya CredSSP (kimlik bilgileri delegasyonu) ile kimlik doğrulaması
    - Kimlik bilgilerinin önbelleğe alınması
    - Kerberos ön kimlik doğrulamada DES ve RC4 kullanımı
    - Hesap yetkilerinin devri

Windows Server 2016 Etki Alanı Fonksiyon Seviyesi:

- Tüm varsayılan Active Directory özellikleri, Windows Server 2012 R2 etki alanı işlev düzeyinin tüm özelliklerine ek olarak aşağıdaki özellikleri içerir
  - Etki alanı denetleyicileri, PKI kimlik doğrulaması gerektirecek şekilde yapılandırılmış bir kullanıcı hesabı için NTLM kullanımını destekler.
  - Bir kullanıcı, etki alanı üyesi belirli cihazların kullanımı ile sınırlandırıldığında, etki alanı denetleyicileri NTLM kullanımına izin vermeyi destekleyebilir.

- PKINIT ile başarılı bir şekilde kimlik doğrulaması gerçekleştiren Kerberos istemcileri, ortak anahtar kimlik bilgisini alırlar.

Windows Server 2019'un bir çok yeni özelliği vardır ancak bu yeni özelliklerden hiçbiri AD ile ilgili değildir. Windows Server 2019 etki alanı işlev düzeyi (FFL / DFL) bulunmamaktadır. Sadece DC'lerde ESE (Extensible Storage Engine) sürüm deposunu daha iyi destekleyen güncellenmiş bir algoritma ile bir tür performans güncellemesi yapılmıştır.

Dokümantasyon

Her bir Active Directory nesnesi için aşağıdaki hususlar dokümante edilmelidir:

- Active Directory ağaç yapısında, nesnenin ismi, pozisyonu ve hiyerarşide bulunduğu yer (örnek: OU="YTE", üst nesne="BİLGEM"),
- Nesnenin hangi amaca hizmet ettiği (örneğin uzaktan erişim sunucusunda uzaktan erişim yetkisine sahip olan kullanıcılar grubu),
- Nesne ve öznitelikleri için hangi yönetimsel yetkilerin atandığı (örneğin tamamen "Admin1" tarafından yönetilir)
- Active Directory'de izinlerin (üst hiyerarşiden miras alınması, miras devrinin sonlandırılması, vb.) nasıl yapılandırıldığı
- Nesneleri, hangi grup ilkelerinin etkilediği (bkz. UYG.2.2.G3 Grup ilkelerinin planlanması).

Active Directory yönetiminin ve kullanılacak yönetim modelinin planlanması, önemli bir işlemdir. Planlama önerilerine, "UYG.2.2.U2 Active Directory yönetiminin planlanması" maddesinde yer verilmektedir.

Active Directory planlamasının güvenlikle ilgili temel yönleri aşağıdaki şekilde özetlenmiştir:

- Etki Alanları, Active Directory sistem yöneticilerinin yönetim alanlarını sınırlar. Varsayılan ayar olarak bu durum, etki alanı yöneticilerinin yönetim işlerini ilgili etki alanı içinde gerçekleştirebilmelerini ve yönetim yetkililerinin etki alanı sınırının ötesine uzanmamasını sağlar. Çoklu etki alanı mimarisinde ise, etki alanı yöneticileri ("Domain Admins") grubu her bir etki alanı içerisinde bulunur ve bulunduğu etki alanı içinde yönetimsel yetkilere sahiptir. "Enterprise Admins" yönetimsel grubu ise, orman yapısındaki kök etki alanı içerisinde bulunur ve orman

yapısı içerisinde yer alan tüm etki alanlarında yönetimsel yetkilere sahiptir. Bu grubun üyeleri de dikkatli bir şekilde planlanmalı ve düzenli olarak gözden geçirilmelidir.

- Etki alanları arası yönetimsel erişim, ilgili etki alanı yöneticisi tarafından özellikle ve bilinçli bir şekilde tanımlanmadığı sürece, varsayılan ayar itibari ile gerçekleştirilemez. Örneğin; A etki alanına, B etki alanı yöneticisinin yönetim amacı ile erişimi ancak A etki alanı yöneticisi tarafından kendisine özel olarak yetki verilmesi durumunda gerçekleşebilir.
- Yönetimsel yetkilendirme, Active Directory nesne ve özniteliklerine erişim hakkı atanarak sağlanır. Erişim haklarının dağıtımı, kullanılan yönetim modeline göre yapılmalıdır. Hiyerarşik yetkilendirmelerin miras alınması veya özel hakların sağlanması ile Active Directory içerisinde çok karmaşık yetkilendirme yapıları oluşturulabilir. Bu durumda, yetkilendirmelerin yönetilemez duruma geleceği karmaşık bir yapıya ulaşılabilir ve olası hatalı yapılandırmalar, güvenlik açıklarına sebebiyet verebilir. Bu sebeple, hedefe yönelik basit bir yetkilendirme yapısı tercih edilmelidir. Yetki devrini güvenli bir şekilde planlamak ve gerçekleştirmek için, öncelikle asıl gerekliliklerin asgari haklar şeklinde tanımlanması ve dokümante edilmesi (örneğin başlangıçta metin biçiminde) ve daha sonra bunların teknik olarak erişim haklarına dönüştürülmesi tavsiye edilir.
- Şema değişiklikleri kritik işlemlerdir ve dikkatli bir planlama sonrasında, sadece yetkili yöneticiler tarafından gerçekleştirilmelidir.

Sonuç olarak, Active Directory planlamasındaki hatalar, ancak kurulum sonrasında gösterilecek ekstra çabalarla düzeltilebilir. Active Directory kurulumu sonrasında, ağaç ve orman yapıları içerisinde etki alanlarının düzenlenmesi gibi değişikliklerin yapılmasına karar verilmesi durumunda, etki alanlarının yeniden kurulması dahi gerekebilir. Bu yüzden planlama detaylı bir şekilde gerçekleştirilmelidir.

Active Directory Federasyon Hizmetleri (ADFS)

Active Directory Federasyon Hizmetleri (kısaltma olarak ADFS veya AD FS kullanılır), temel olarak federasyon yapısına dâhil edilen kimliklerin eşleştirilmesini sağlar. Bu yapı tesis edildiğinde, kullanıcıların mevcut etki alanında kullandıkları kullanıcı adı ve parola ile kurum dışındaki servislerden yararlanabilmesine imkân sağlanır (SSO: Single Sign On). Bu özellik, Windows Server 2012 ile birlikte, sunucuda hali hazırda var olan bir rol olarak kullanılabilir durumdadır.

ADFS aracılığı ile iki (veya daha fazla) kurum arasında bir güven ilişkisi kurulur. Bir kurumdaki federasyon sunucusu, diğer kurumun hizmet talep eden kullanıcısına yetki verebilir ve ilgili kullanıcı kendisine tanınan yetki dâhilinde diğer kurumda bulunan hizmetten faydalanır. Her kurum kendisine ait kimlikleri yönetmeyi sürdürür, bununla birlikte kurumlar aynı zamanda diğer kurumlarla güvenli şekilde kimlik alış verişi de yapabilirler.

ADFS, Microsoft bulut hizmeti olan "Azure AD" ve benzeri bulut hizmetleriyle entegre olma yeteneğine sahip olduğundan, gün geçtikçe önem kazanmaktadır. Ayrıca, web servis tabanlı veya SAML 2.0 uyumlu federasyon hizmetleriyle de entegrasyonu mümkündür.

Genel olarak federasyonun ve özellikle de ADFS'nin kullanımı, planlanarak, detaylı biçimde test edilerek ve dokümantasyon sağlanarak gerçekleştirilmelidir. Bu yaklaşımda, özellikle gerekli güven ilişkileri de ele alınmalıdır. Etki alanları arası güven ilişkileri minimum seviyede tasarlanmalı ve düzenli olarak gözden geçirilmelidir. Başka bir kurum tarafından, kimlik doğrulama veya yetkilendirme ile tanınan hakların yanlış kullanımının, ne tür riskler oluşturabileceği sistematik olarak tanımlanmalı, değerlendirilmeli ve uygun aksiyonlar alınmalıdır.

UYG.2.2.U2 Active Directory yönetiminin planlanması [Sorumlu Teknik Uzman]

Active Directory, bir ağaç yapısı şeklinde dallanan çeşitli nesnelerden (kullanıcı, bilgisayar, gruplar, vb.) oluşur. Her nesne içerisinde, nesne bilgilerini saklayan çeşitli öznitelikler bulunur. Nesneler, yetkili yöneticiler tarafından Windows sistemini yönetmek için kullanılır. Nesnelere erişimi kontrol etmek amacı ile her bir Active Directory nesnesi özelinde yetki verilebilir. Bu yetkiler, nesnelerin hangi kullanıcılar tarafından değiştirilebileceği, nesnelerin kimler tarafından oluşturulabileceği veya parolalarının kimler tarafından sıfırlanabileceği gibi faaliyetlerin saptanması amacı ile kullanılabilir.

Varsayılan kurulum sonrasında yalnızca yöneticiler, nesnelerde değişiklik yapma ve böylelikle bir etki alanını yönetme hakkına sahiptir. Kullanıcılar azami olarak, sadece okuma yetkisine sahiptirler.

Genel olarak, etki alanı yöneticilerinin yönetim yetkisi etki alanı sınırlarında sona ermektedir. Yalnızca, “Enterprise Admins” grubunun üyeleri, bir orman yapısının her etki alanındaki tüm AD nesnelerine (nesneler için ayarlanan erişim haklarına bakılmaksızın) tam erişim yetkisine sahiptir. Varsayılan olarak bu kullanıcılar, orman yapısının Kök Etki Alanı (FRD: Forest Root Domain) Yöneticileri grubunun üyeleridir.

Büyük etki alanlarının var olduğu orman yapılarında, yönetimsel görevlerin kısmen veya tamamen devredilmesi tavsiye edilir. Bu şekilde, yönetimsel görev yükü farklı yöneticiler

arasında dağıtılabilir. Bazı durumlarda ise rollerin ayrıştırılması yöntemi uygulanabilir. Active Directory'de yönetimsel görevlerin atanması, Active Directory nesnelerine erişim yetkilerinin ilgili yönetici gruplarına verilmesi ile gerçekleşir. Active Directory yetkilendirme yapısı, yetkilerin detaylı bir şekilde verilebilmesine olanak sağlar. Örneğin, yetkilendirilen bir yöneticinin, kullanıcı hesapları oluşturabilmesine ve kullanıcı şifrelerini sıfırlayabilmesine izin verilip, kullanıcı hesaplarını silmesi veya bu hesapları diğer OU'lara taşıması engellenebilir. Bir alt ağaç yapısında benzer yetkilerin tahsisini kolaylaştırmak için, nesnenin yetkilerini üst ağaç yapısından miras alması da mümkündür. Alt ağaç yapısında belirli nesneler için yetkilerin mirasının istenmeyebileceği durumda ise, yetkilerin devralınması engellenebilir. Bu tarz durumlarda, yetki dağılımı hususunda oldukça karmaşık senaryoların oluşması ihtimali vardır. Bu durumun önüne geçmek amacıyla iyi bir planlama yapılmalıdır.

Güvenlik bakış açısı ile Active Directory yönetimini planlarken aşağıdaki hususlar göz önünde bulundurulmalıdır:

- Yetki devrinin kullanıldığı hallerde, sadece ilgili yönetimsel faaliyetleri yürütmek için gerekli olan temel yetkiler devredilmelidir.
- Yetki devri modeli ve son durumda ortaya çıkan devredilmiş yetkiler dokümante edilmelidir.
- Yönetimsel faaliyetlerin gerçekleştirilmesi için yetki devri, herhangi bir çakışmaya mahal vermeyecek şekilde planlanmalıdır. Aksi halde, iki yönetici birbiri ile çakışan değişiklikler yapabilir. Bu durum, replikasyonda da çakışmalara yol açabilir. Buna karşın Active Directory, varsayılan mimarisi itibari ile çakışma durumunu otomatik olarak çözen bir yapıya sahiptir ve bu yapı gereğince son durumda değişikliklerden yalnızca biri etkin olur. Ancak yaşanan bu durum için herhangi bir uyarı üretilmez. Dolayısı ile yönetim modelinin, mümkün olduğunca birbiri ile çakışmayan sorumluluklar oluşturacak şekilde tasarlanması tavsiye edilir. Bu şekilde, replikasyonda çakışmaların oluşması riski azaltılabilir. Replikasyonda çakışmalar bekleniyorsa veya bu durum hali hazırda gerçekleşmişse, son durumda beklenen değerlerin geçerli olup olmadığı, düzenli aralıklarla veya gerçekleştirilen önemli değişikliklerden sonra manuel bir kontrol ile gözden geçirilmelidir.
- Active Directory yönetiminin devredilmesi, Active Directory içerisinde uygun erişim izinlerinin ilgili kullanıcılara verilmesi ile gerçekleştirilir. Bu kapsamda, alt ağaç yapısındaki nesnelere dair izinleri yönetmek için miras mekanizması kullanılır. Ancak, yetki devri ile izinlerin mirası kullanımında karmaşık senaryolardan kaçınılması önerilir. Aksi takdirde güvenlik zafiyetleri ortaya

çıkabilir. Örneğin, bir kullanıcının hedeflenenden çok az veya çok daha fazla yetkiye sahip olması durumu oluşabilir.

- Farklı yönetimsel gruplara üyelik bir politika takip edilerek gerçekleştirilmelidir. Bu politikada özellikle, bir kullanıcı veya kullanıcı grubunun bir yönetim grubuna; neden, ne zaman ve ne kadar süre dâhil edildiğini tanımlayan maddeler yer almalıdır. "Enterprise Admins" grubunun üyeliğini, sınırlandırılmış bir şekilde yönetmek ve kontrol etmek amacı ile özel bir hassasiyet gösterilmelidir. Organizasyon yapısının imkân vermesi halinde, etki alanı yapısını oluşturduktan sonra "Enterprise Admins" grubunun tüm üyelerini gruptan çıkarma, gruba sadece gerekli olduğu durumda üye ekleme ve benzeri kritik işlemlerde en az iki yöneticinin gözetiminde çalışma prensibi benimsenmelidir. Ancak "Enterprise Admins" grubunun sadece tek bir üyesi tarafından gerçekleştirilebilecek işlemlerin olabileceği de unutulmamalıdır (ör. orman yapısına yeni bir etki alanı eklenmesi).
- Active Directory sistem yöneticileri, güvenlik açıklarına neden olabilecek uyumsuz değişiklikleri önlemek için organizasyonda yapılan değişiklikler hakkında bilgilendirilmeli, Active Directory yapısına ve yönetimsel süreçlerine aşina olmalı ve bu konuda eğitim almalıdırlar. Örneğin, yeni bir kullanıcı oluştururken, kullanıcıyı uygun güvenlik gruplarına eklemek, hatta özel bir isimle yeni bir güvenlik grubu oluşturmak gerekli olabilir. Bu unutulur ise, kullanıcılara gerekli olmayan haklar verilebilir.
- Büyük etki alanları için, etki alanı yönetiminin uygun araçlarla desteklenmesine önem verilmelidir. Active Directory yönetimini kolaylaştırabilecek çeşitli ticari ve ücretsiz araçların kullanımı düşünülebilir. Bu tür araçların kullanılması durumunda, Active Directory yönetiminin sadece bu araçlar aracılığıyla yapılması sağlanmalıdır.

Rol Tabanlı Yetkilendirme Kavramı

Her bir hesabın yetkileri üzerinde ayrıntılı kontrol imkânı sağlayan, rol tabanlı yetkilendirme düzeni uygulanması tavsiye edilir.

Tüm yetkiler, rollere uygun şekilde atanmalıdır. Bu tür bir uygulamada, öncelikle güvenlik grupları oluşturularak, bu gruplara ilgili izinler atanır. Ardından, rolleri temsil eden gruplar oluşturulur ve bu gruplar önceden oluşturulmuş güvenlik gruplarına üye edilir. Son olarak, kullanıcı hesapları rolleriyle eşleşen gruplara üye edilir. Ayrıca, özellikle büyük kurumlarda bir kurumsal kimlik yönetimi çözümünün kullanımı, tüm kullanıcı yetkilerinin tanımlanmış kriterlere göre uyarlandığını garanti altına alabilir.

Active Directory Hizmet ve Veri Yönetiminin Ayrıştırılması

Yönetimsel faaliyetler, temel olarak iki farklı sorumluluk alanına, "servis yönetimi" ve "veri yönetimi" şeklinde ayrıştırılabilir.

"Servis yönetimi" terimi, Active Directory hizmetinin yönetimini ifade eder. Servis yöneticileri, etki alanı denetleyicilerini yönetme (ör. işletim sistemi düzeyindeki güncellemeleri yükleme) ve Active Directory yapılandırma (ör. etki alanı güven ilişkileri veya replikasyon mimarisi) faaliyetlerini gerçekleştirirler.

Active Directory ve/veya etki alanına üye bilgisayar nesnelerine ilişkin verilerin yönetiminin ise veri yöneticileri tarafından yapılması önerilir. Veri yöneticileri, Active Directory hizmetinde (replikasyon mimarisi, vb.) herhangi bir değişiklik yapamamalıdırlar. Veri yöneticilerine ilişkin yetkilerin, erişim kontrol listeleri (Access Control List, ACL) kullanılarak, sorumluluk alanları ile sınırlandırılması önerilir.

Servis yöneticileri, görevlerini yerine getirebilmeleri için geniş kapsamlı izinlere ihtiyaç duyarlar. Bu durumun aksine veri yöneticileri, Active Directory'nin yapılandırmasını değiştiremeyecek şekilde daha dar kapsamlı yetkiler ile yetkilendirilmelidirler.

Yönetimsel hesapların kötüye kullanılmasını önlemek için, yukarıdaki rollerin atandığı kullanıcı hesaplarının güvenli bir şekilde korunması tavsiye edilir. Konuya ilişkin gerekli yapılandırmalardan, “UYG.2.2.U7 Active Directory için Güvenlik Yöntemlerinin Uygulanması” maddesinde bahsedilmektedir.

UYG.2.2.U3 Grup ilkelerinin planlanması

Windows 2000'den bu yana, Grup İlkesi olarak bilinen güçlü bir yapılandırma mekanizması kullanıma sunulmuştur. Active Directory grup ilkeleri; bir nesne grubuna, güvenlik ayarları da dâhil olmak üzere birçok yapılandırmayı uygulamak için kullanılır. Grup ilkesi nesnesi (GPO: Group Policy Object), önceden belirlenen yapılandırma parametrelerini içerir. Her bir parametreye, sadece sınırlı bir değer aralığı içerisinden değer atanabilir. Parametre değeri, "tanımlanmamış" şeklinde de atanabilir ki bu durumda, varsayılan Windows ayarları otomatik olarak uygulanır.

Bir grup ilkesi nesnesindeki parametreler, ağaç yapısı benzeri bir biçimde sunulur. Bu yapıda, en üst düzeyde, bilgisayarlar ve kullanıcılar temelinde bir ayrıştırma sağlanır.

Güvenlik yaklaşımı açısından, aşağıdaki ayarlar özellikle dikkate değerdir:

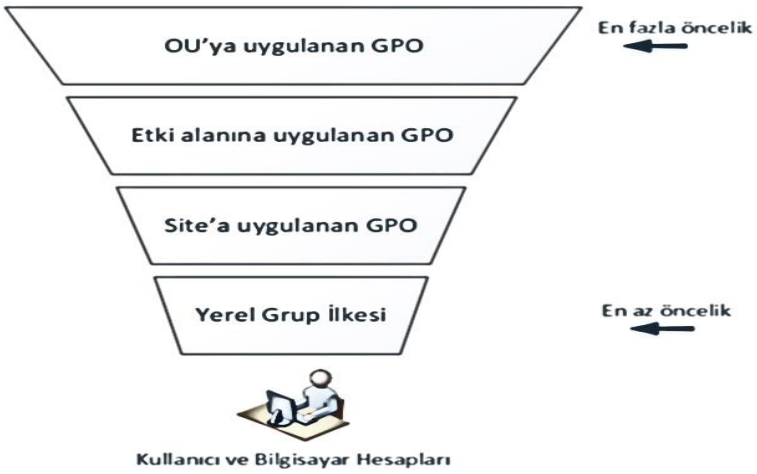
- Bilgisayar Yapılandırması \ Windows Ayarları \ Güvenlik Ayarları

- Bilgisayar Yapılandırması \ Yönetim Şablonları \ Windows Bileşenleri \ Windows Installer
- Bilgisayar Yapılandırması \ Yönetim Şablonları \ Sistem \ Grup İlkesi
- Kullanıcı Yapılandırması \ Yönetim Şablonları \ Windows Bileşenleri \ Microsoft Yönetim Konsolu
- Kullanıcı Yapılandırması \ Yönetim Şablonları \ Windows Bileşenleri \ Windows Installer

Bir bilgisayar veya kullanıcı, birbirinden farklı grup ilkelerine tabi olabilir. Mevcut Windows sistemleri, bir etki alanında oturum açan her bilgisayar ve kullanıcı için, grup ilkesi açısından etkin olan ayarları hesaplar. Aynı nesneye etki eden, farklı GPO'lar tarafından, farklı parametre değerleri tanımlanmış olabileceğinden, bu tür hesaplamalar gereklidir. Bu bağlamda, aşağıdaki seviyelerde GPO'lar tanımlanabilir:

- Her bilgisayarda, yerel olarak tanımlanmış grup ilkesi nesneleri bulunur. Bu şekilde parametre ayarları bilgisayarda yerel olarak tanımlanabilir.
- Grup ilkesi nesneleri, "Active Directory Site" düzeyinde tanımlanabilir. Bu yöntem, belirli "Active Directory Site" içerisinde yer alan nesnelere ilgili ayarların uyarlanmasını sağlar.
- Active Directory ağaç yapısı içerisinde grup ilkesi nesneleri, etki alanı ile direkt olarak ilişkilendirilebilir. Bu durumda yapılandırılan parametreler tüm etki alanı içinde yer alan bilgisayarlar ve kullanıcılar için geçerli olur.
- Grup ilkesi nesneleri, her bir OU nesnesi bazında tanımlanabilir. Bu durumda, ilgili politikalar OU nesnesinin altındaki tüm bilgisayarları ve kullanıcıları etkiler.

Belirli bir bilgisayar veya kullanıcı için etkin olan grup ilkesi parametre ayarları (yerel <- Active Directory Site <- etki alanı <- OU, LSDO) şeklinde bir hesaplama yöntemi ile belirlenir. Bu yöntemde öncelikle, yerel ayarlar dikkate alınır (L, yerel). Bu ayarlara sonrasında, ilişkili AD site (S, Konum) üzerinde tanımlanan GPO ayarları eklenir. Daha sonra, söz konusu nesnenin üyesi olduğu etki alanı (D, domain) üzerinde tanımlanan grup ilke nesne ayarları yapılandırılır. Son olarak, OU nesnelerine ilişkin grup ilkesi nesne ayarları, etki alanı nesnesinden başlayarak ilgili bilgisayarı veya kullanıcıyı içeren OU nesnesine giden yolda, tanımlandıkları sıraya göre uygulanır. Bu durumun daha kolay anlaşılabilmesi için; nesnenin direkt içerisinde yer aldığı OU seviyesinde uygulanan politikanın en son uygulandığı ve dolayısıyla önceliğe sahip olduğu düşünülebilir.



Şekil 9. Grup ilkeleri öncelik sıralaması

Grup ilkelerinin çakışma olasılığına, GPO'ları engelleme ve/veya zorlama seçenekleri ile etki edilebilir. GPO'ları engelleme ve zorlama ayarlarının çakıştığı bir durumda zorlama ayarı etkin olur. Bunlara ilave olarak, OU seviyesinde, bir OU nesnesi için birden fazla GPO tanımlanması mümkündür. Aynı OU'ya bağlanan GPO ayarlarının çakışması durumunda ise bu durum, GPO'ların bağlantı sırasına (link order) göre çözümlenir. Bağlantı sırası yüksek olan GPO önce uygulanır, düşük olan ise sonra uygulanır ve nihai ayarlarda sonra uygulanan politikanın parametreleri etkin olur. Bir OU nesnesi için herhangi bir GPO'yu etkinleştirmek veya devre dışı bırakmak da mümkündür.

Grup ilkesi nesneleri, Active Directory nesneleri bazında yalnızca OU nesneleri ile ilişkilendirilebilir, tek tek bilgisayar veya kullanıcı nesneleri ile ilişkilendirilemez. Yerel olarak tanımlanmış bir GPO, Active Directory'de depolanmaz. Eğer içerisinde birden çok bilgisayar nesnesinin yer aldığı bir OU üzerinde tanımlanmış bir GPO varsa ve OU içerisindeki bazı bilgisayar nesnelerinin bu GPO'dan etkilenmesi istenmiyor ise bu durum, ilgili grup ilkesi nesnesinin erişim haklarının yapılandırılması ile sağlanabilir.

Ancak yukarıda anlatılan, OU nesneleri bazındaki GPO tanımlama süreci pratik kullanımda basitleştirilmiştir. GPO'lar Active Directory'de ayrı bir nesne grubu olarak depolanır. Her oluşturulan GPO bir veya daha fazla OU nesnesiyle ilişkilendirilebilir. Bu ilişkilendirme, bir bağlantı olarak kabul edilir. Bir bağlantının etkin veya devre dışı olarak ayarlanmasıyla ilgili GPO nesnesinin uygulanıp uygulanmayacağı belirlenebilir. Ayrıca, GPO'un özellikleri kontrol edilerek hangi OU için bir bağlantı oluşturulduğu, yani hangi nesneleri potansiyel olarak etkilediği görülebilir.

Güvenlik gereksinimleri açısından, GPO'lar planlanırken ve işletilirken, aşağıdaki hususlar dikkate alınmalıdır:

- Grup ilkesi yaklaşımı mümkün olduğunca basit tutulmalıdır. Birden çok çakışma içerecek karmaşık yapılardan kaçınılmalıdır. Özellikle, GPO'lara sadece istisnai durumlarda erişim hakları atanmalıdır. Genel olarak grup ilkesi yaklaşımı, istisnaların kolayca görülebileceği şekilde dokümante edilmelidir.

- Grup ilkesi yaklaşımı ve OU nesne yapısı birbirleri üzerinde önemli etkiye sahiptir. Çünkü grup ilke nesneleri, Active Directory'deki etki alanı içerisinde yalnızca OU nesnelerine uygulanabilir, bilgisayar veya kullanıcı nesnelerine uygulanamaz. Bu yüzden, OU'lar oluşturulurken, sadece aynı GPO ayarlarıyla yönetilecek nesnelerin bir OU nesnesinde veya alt birim OU nesnelerinde toplanmasına dikkat edilmelidir.

- Grup ilkelerinin uygulanması sonucunda etkin olacak ayarların baştan hesaplanması/planlanması yoluyla, parametre ayarlarının yönetimini farklı noktalara (lokal, Active Directory site, etki alanı nesnesi, OU nesneleri) dağıtmak mümkündür. Bu nedenle, her bir parametrenin hangi seviyede konumlandırılacağına karar verilmelidir. Parametreleri tanımlar iken, bazı parametrelerin, sadece belirli noktalarda tanımlanabileceğine ve ancak bu şekilde etkili olabileceklerine dikkat edilmelidir. Örneğin, Microsoft Windows 2000 ve Windows Server 2003 Active Directory etki alanlarında, Active Directory üyesi tüm kullanıcılara tek bir parola ilkesi ve hesap kilitleme ilkesi uygulanabilir ve bu ilke, etki alanı nesnesi seviyesinde tanımlanabilirken; Windows Server 2008 ile birlikte sunulan "fine-grained password policy" özelliği sayesinde, etki alanında tanımlı farklı kullanıcı grupları için farklı parola politikalarının da uygulanabilmesi mümkün kılınmıştır.

- Grup ilkesi nesneleri, yetkisiz şekilde gerçekleştirilebilecek değişikliklere karşı korunmalıdır. Bunun için bir taraftan, Active Directory'de uygun yetkilendirmelerin tanımlanması ve diğer taraftan kullanıcıların MMC Grup ilkesi yönetim ara yüzü veya kayıt defteri düzenleyicisi gibi araçlara erişimlerinin engellenmesi önerilir.

- Bir GPO içerisinde yer alan, özellikle güvenlik gereksinimleri ile ilgili parametrelere atanacak değerlerin belirlenmesi önemlidir. Uygulama senaryosuna bağlı olarak, örneğin Internet Explorer ayarları gibi, farklı parametreler de güvenlik gereksinimleri ile ilişkili olabilir.

- Varsayılan "Default Domain Policy" ve "Default Domain Controllers Policy" grup ilkelerinde değişiklik yapmak yerine, kurum özelindeki ayarları yeni grup ilkeleri oluşturarak uygulamak; etki alanı seviyesinde grup ilkesi uygulamak yerine grup

ilkelerini daha alt seviye (OU nesneleri) ile ilişkilendirmek ve grup ilkeleri isimlerini açıklayıcı olarak vermek, işletime dair uygulanması önerilen davranışlardır.

Grup ilkesi nesneleri, kurumun güvenlik yönergeleri temel alınarak yapılandırılmalı ve uygulanmalıdır.

Grup İlkesi Güvenlik Ayarları

Aşağıda yer alan grup ilkeleri, güvenlik gereksinimlerine dair temel yapılandırmaları listelemektedir. İlkelere dair parametre değerleri için Microsoft'un ilgili makaleleri incelenmelidir. Ayrıca değerler, kurumun yerel koşullarına göre özelleştirilebilir. Grup ilkelerinin uygulanmasında, özelleştirilmiş değerler farklı grup ilkesi nesnelerine dağıtılmalı ve hedeflenen kullanıma uygun olmalıdır (örneğin sunucular için grup ilkesi nesneleri, istemciler için grup ilkesi nesneleri vb.). Sonuç olarak, hedeflenen uygulama grupları için farklı grup ilkeleri oluşturulabilir.

Parola İlkesi

- En kısa parola uzunluğu
- Parola geçerlilik süresi alt sınırı
- Parola geçerlilik süresi üst sınırı
- Parola geçmişini uygula
- Parolalar karmaşıklık gereklerine uymalıdır
- Parolaları, ters çevrilebilir şifreleme kullanarak depola

Hesap Kilitleme İlkesi

- Hesap kilitleme eşik değeri
- Hesap kilitleme süresi
- Şu süreden sonra hesap kilitleme sayacını sıfırla

Denetim İlkesi

- Dizin hizmeti erişimini denetle
- Hesap oturumu açma olaylarını denetle
- Oturum açma olaylarını denetle
- Hesap yönetimini denetle
- Nesne erişimini denetle
- İşlem izlemeyi denetle
- Ayrıcalık kullanımını denetle

- İlke değişikliğini denetle
- Sistem olaylarını denetle

Kullanıcı hakları ataması

- Hizmet olarak oturum aç
- Sistem saatini değiştir
- Zamanlama önceliğini artır
- İşlem için bellek kotaları ayarla
- Toplu iş olarak oturum aç
- Toplu iş olarak oturum açmayı kabul etme
- Hizmet olarak oturum açmayı kabul etme
- Bu bilgisayara ağ üzerinden eriş
- Programların hatalarını ayıkla
- İşletim sisteminin bir parçası gibi davran
- Bilgisayarı takma biriminden çıkar
- Temsilci seçme için bilgisayar ve kullanıcı hesaplarına güvenilmesini etkinleştir
- Disk belleği dosyası oluştur
- Sistem performansı profili oluştur
- Uzak sistemden kapatmayı zorla
- Güvenlik denetimleri oluştur
- Sistemi kapat
- Etki alanına iş istasyonları ekle
- Aygıt sürücüleri yükle ve kaldır
- Yerel olarak oturum açmaya izin ver
- Yerel olarak oturum açmaya izin verme
- Dosya ve dizinleri yedekle
- Dizin hizmeti verilerini eşitle
- Dosyaların veya diğer nesnelerin sahipliğini al
- Denetim ve güvenlik günlüğünü yönet
- Dosyaları ve dizinleri geri yükle
- Bu bilgisayara ağ üzerinden erişime izin verme

Güvenlik seçenekleri

- Yönetici hesabının adını değiştirin

- Etkileşimli oturum açma: Süre sonuna gelmeden önce kullanıcının parolasını değiştirmesini iste
- Aygıtlar: Kullanıcıların yazıcı sürücüsü yüklemelerini engelle
- Etkileşimli oturum açma: Önbelleğe alınacak önceki oturum sayısı (etki alanı denetleyicisinin olmadığı durumlarda)
- Kapatma: Sanal bellek disk belleği dosyasını temizle
- Aygıtlar: Çıkarılabilir medyayı biçimlendirmeye ve çıkarmaya izin verildi
- Ağ güvenliği: Oturum açma saatleri bitiminde oturumdan çıkmaya zorla
- Microsoft ağ istemcisi: İletişimleri dijital olarak imzala (her zaman)
- Microsoft ağ istemcisi: İletişimleri dijital olarak imzala (sunucu kabul ederse)
- Denetim: Yedekleme ve Geri Yükleme ayrıcalığının kullanımını denetle
- Hesaplar: Konuk hesabının adını değiştirin
- Kapatma: Sistemin oturum açmayı gerektirmeden kapatılmasına izin ver
- Ağ güvenliği: LAN Manager kimlik doğrulama düzeyi
- Etkileşimli oturum açma: Makinede etkinlik yapılmama süresi sınırı
- Etkileşimli oturum açma: En son oturum açmayı gösterme
- Etkileşimli oturum açma: Oturum açmaya çalışan kullanıcılar için ileti başlığı
- Etkileşimli oturum açma: Oturum açmaya çalışan kullanıcılar için ileti metni
- Microsoft ağ sunucusu: İletişimleri dijital olarak imzala (her zaman)
- Microsoft ağ sunucusu: İletişimleri dijital olarak imzala (istemci kabul ederse)
- Etki alanı denetleyicisi: Sunucu işletmenlerinin görevleri zamanlanmasına izin ver
- Etki alanı üyesi: Güvenli kanal verisini dijital olarak imzala (uygun olduğunda)
- Etki alanı üyesi: Güvenli kanal verisini dijital olarak şifrele (uygun olduğunda)
- Etki alanı üyesi: Güvenli kanal verisini dijital olarak şifrele veya imzala (her zaman)
- Etki alanı üyesi: Güçlü (Windows 2000 veya daha sonraki) oturum anahtarı gerektir
- Sistem nesneleri: İç sistem nesnelerinin (simgesel bağlantılar gibi) varsayılan izinlerini güçlendir

- Etkileşimli oturum açma: CTRL + ALT + DEL gerektirme
- Denetim: Güvenlik denetimleri günlüğe alınamıyorsa sistemi hemen kapat
- Etki alanı üyesi: Makine hesabı parola değişikliklerini devreden çıkar
- Microsoft ağ istemcisi: Üçüncü taraf SMB sunucularına şifrelenmemiş parola gönder
- Kullanıcı hesabı denetimi: Yalnızca güvenilir konumlara yüklenmiş UIAccess uygulamalarını yükselt
- Kullanıcı hesabı denetimi: Yalnızca imzalı ve doğrulanmış olan çalıştırılabilen dosyaları yükselt
- Etkileşimli oturum açma: Akıllı kart çıkarma davranışı
- Kurtarma konsolu: Diskete kopyalamaya ve tüm sürücü ve klasörlere erişime izin ver
- Kurtarma Konsolu: Otomatik yönetim oturumu açmaya izin ver
- Aygıtlar: CD-ROM erişimini yalnızca yerel olarak oturum açan kullanıcılarla sınırla
- Aygıtlar: Disket erişimini yalnızca yerel olarak oturum açmış kullanıcılarla sınırla

Olay Günlüğü Hizmeti

- Uygulama: Günlük erişimini yapılandır
- Güvenlik: Günlük erişimini yapılandır
- Sistem: Günlük erişimini yapılandır
- Uygulama: Günlük dosyası boyut üst sınırına ulaştığında Olay Günlüğü'nün davranışını denetle
- Güvenlik: Günlük dosyası boyut üst sınırına ulaştığında Olay Günlüğü'nün davranışını denetle
- Sistem: Günlük dosyası boyut üst sınırına ulaştığında Olay Günlüğü'nün davranışını denetle
- Uygulama: Günlük dosyası boyut üst sınırını belirt (KB)
- Güvenlik: Günlük dosyası boyut üst sınırını belirt (KB)
- Sistem: Günlük dosyası boyut üst sınırını belirt (KB)

Security Compliance Toolkit (SCT)

Microsoft'un Security Compliance Toolkit (SCT) araç seti, Windows ve diğer Microsoft ürünleri için Microsoft tarafından önerilen güvenlik yapılandırması temellerinin analiz edilmesi, test edilmesi, düzenlenmesi ve depolanmasına olanak tanımaktadır. SCT daha önce benzer amaçla kullanımda olan Security Compliance Manager (SCM) aracının yerini almıştır. Active Directory açısından bu araç, grup ilkelerin yönetimini kolaylaştırmaktadır. Bu araç ile grup ilkeleri analiz edilerek, birbirleri ile karşılaştırılıp çakışan noktalar tespit edilebilir. SCT, Microsoft'un ilgili İnternet sitesinden ücretsiz bir şekilde indirilebilir.

"Fine-Grained Password Policy"

Windows Server 2008 ile birlikte tanıtılan "Fine grained password policy" özelliği, bir etki alanındaki farklı kullanıcı grupları için farklı parola politikalarının tanımlanmasına olanak sağlamaktadır.

Bu tür bir parola politikası, Kerberos ayarları dışındaki tüm parola ayarlarının yapılandırılması için kullanılabilir. Varsayılan olarak, ilgili parola politikasını yalnızca "Domain Admins" grubunun üyeleri yapılandırabilirler. Ancak, bu yetki diğer kullanıcılara da devredilebilir.

Bir kurumda uygun parola politikalarının yapılandırılması sürecinde "Fine grained password policy" kullanımı tavsiye edilir.

Shadow Groups

"Fine grained password policy" doğrudan OU'lara uygulanamaz. Belirli bir OU içerisindeki kullanıcılara "Fine grained password policy" uygulamak için, "Shadow Groups" kullanılabilir. "Shadow Groups", bir OU'ya mantıksal olarak atanan global bir güvenlik grubudur. Kullanıcılar, "Shadow Groups"a atandıktan sonra, ilgili parola politikası bu gruba uygulanır. "Shadow Groups" üyelikleri otomatik olarak değişmez. Bu yüzden bir kullanıcıyı başka bir OU'ya taşırken, "Shadow Groups" üyeliklerine dikkat edilmesi gerekmektedir.

GPO ile Parola Yönetimi

Temel olarak GPO ile yerel hesapların oluşturulması, parolalarının atanması gibi işlemler yapılabilir. Ancak böyle bir durumda, kimlik bilgileri tüm etki alanı denetleyicilerinde yer alan SYSVOL paylaşımı içerisindeki XML dosyalarında saklanır. Bu sebeple kimlik bilgileri kolayca okunabilir veya değiştirilebilir.

GPO'lar parolaları belirlemek için kullanılmamalıdır. Eğer mevcut GPO'lar içerisinde parola yer alıyor ise, bu politikalar kaldırılmalı ve karşılık gelen dosyalar silinmelidir. Benzer durum, parola içeren komut dosyaları (örn. VBS veya PowerShell script'leri) için de

geçerlidir. Microsoft, SYSVOL'u tarayarak GPO XML dosyalarındaki parolaların tespit edilmesini sağlayan bir PowerShell komut dosyası sunmaktadır. Bu komut dosyası aracılığı ile parolaların var olup olmadığı tespit edilmeli ve gerekli önlemler alınmalıdır.

UYG.2.2.U4 Active Directory yönetimi eğitimi

Bir Windows ağının yönetimi, Active Directory ve temel kavramları hakkında ayrıntılı bilgi sahibi olmayı gerektirir. Aksi takdirde, yanlış yapılandırmalar önemli güvenlik zafiyetlerine neden olabilir. Bu nedenle, ilgili yöneticilerin Active Directory ile ilgili özellikle güvenlik konularında eğitim almaları önemlidir.

Eğitim İçeriği

Kurum ağının büyüklüğüne ve karmaşıklığına bağlı olarak, Active Directory genelde tek bir yönetici tarafından yönetilemez. Bunun yerine, belirli görevler birçok yönetici tarafından yürütülür. Bu sebeple, Active Directory yönetiminde görev alacak tüm yöneticileri için aynı eğitim içeriğinin uygulanmaması ve eğitim içeriğinin (faaliyet alanına göre) yönetici özeline indirgenmesi ve/veya özelleştirilmesi düşünülebilir. Ancak her yöneticinin, kendi sorumluluk alanındaki faaliyetlerini temel güvenlik prensipleri çerçevesinde gerçekleştirebilmesi için, yeterli temel bilgiye sahip olması gerekir.

Eğitim içeriği, her durumda aşağıdaki temel hususları içermelidir.

Temel Bilgi

- Windows sunucu güvenlik mekanizmalarına genel bakış
- Windows istemci işletim sistemlerinin güvenlik mekanizmasındaki yenilikler (Yeni işletim sistemi sürümleri veya güncel hizmet paketleri tarafından getirilen değişiklikler de dâhil olmak üzere)
- Güvenlik yönetimi (MMC, Güvenlik Editörü, GPMC)
- Active Directory ve DNS
- Etki alanları arası güven ilişkileri
- Etki alanı denetleyicilerinin fiziksel olarak korunması

Active Directory

- Genel Bilgi: Planlama, Kurulum, Yönetim
- Şema Yönetimi
- Replikasyon

- Yedekleme
- Yetkilendirme
- Kimlik Doğrulama
- Grup ilkeleri

PKI (Public Key Infrastructure)

- PKI nasıl çalışır?
- Sertifikalar ve Sertifika Türleri
- PKI Planlama, Kurulum, Yönetim
- PKI ile Kullanıcı Etkileşimi

IPsec

- IPsec nedir?
- IPsec Yapılandırması
- Güvenli bağlantıların başarılı şekilde kurulduğunun kontrol edilmesi

DFS (Distributed File System)

- DFS nedir?
- DFS Yönetimi
- DFS Yapısını Planlama
- DFS kullanımında verilerin korunması

Active Directory'e dair konular, aşağıdaki gibi daha ayrıntılı olarak sunulmalıdır:

Şema Yönetimi

Normal şartlarda, Active Directory şeması (şema değişikliğine ihtiyaç duyulan özel kurulumlar haricinde) sürekli değiştirilmemektedir. Bu nedenle ilgili eğitim, şema değişikliklerinin yol açabileceği etkiler ve sorunlar ile sınırlandırılabilir. Eğer şemada özelleştirmeler yapılıyor ise konunun ilgili yönetici eğitim programlarına eklenmesi gerekmektedir.

Active Directory Replikasyonu

- Active Directory replikasyonunda kullanılan yöntemler (RPC ve SMTP)
- Active Directory replikasyon mimarisi, yapılandırılması

- Active Directory replikasyonunun izlenmesi

Yedekleme

- Active Directory yedekleme mimarisi
- Bir etki alanı denetleyicisinin yedeğini geri yükleme
- FSMO rollerini üzerinde taşıyan etki alanı denetleyicilerinin kesintiye uğraması durumunda alınacak aksiyonlar

Active Directory'de Yetkilendirme

- AD nesnelerine öznitelik düzeyinde erişim haklarının atanması
- Erişim haklarının miras alınması ve miras alınma durumunun engellenmesi
- Tanımlanabilecek erişim hakları
- OU düzeyinde yönetimsel görevlerin devri

Kimlik Doğrulama

- Kerberos
- PKI
- Akıllı Kartlar (Smartcard)

Grup İlkeleri

- Yerel grup ilkeleri ve Active Directory grup ilkeleri
- Grup ilkesi kullanımı ile yapılandırma seçenekleri
- Grup ilkeleri ne zaman uygulanır? Nasıl yapılandırılır?
- Active Directory'de nesne olarak grup ilkesi nesneleri (GPO)
- GPO'ların AD site / etki alanı / OU ile ilişkilendirilmesi
- Grup ilkelerinin işlenme sırası
- Grup ilkeleri uygulanmasını denetleme yöntemleri
    - Grup ilkelerine erişim hakları atama
    - GPO'ların geçersiz kılınamama özelliği
    - AD nesneleri için GPO'ların kalıtımsal olarak etki etmesinin engellenmesi özelliği

- Grup ilkelerinin seçici olarak uygulanma yöntemleri
    - Güvenlik filtresi
    - WMI filtreleri ve bunların uygunsuzluk durumları (performans sorunu nedenleri)

Active Directory Temel Eğitimi

Aşağıdaki bilgiler, Active Directory'e giriş ve Active Directoy güvenliğine dair her yöneticinin sahip olması gereken temel bilgilerdir. Ancak bu bilgiler, konuya dair alınacak kapsamlı bir eğitimin ya da ilgili iş deneyiminin sağlayacağı bilgilerin yerini tutamaz.

Etki alanı, Active Directory'nin en temel bileşenidir. Bilgisayarlar, kullanıcılar ve gruplar bir etki alanı altında toplanırlar ve etki alanı yöneticisi tarafından yönetilebilirler. Etki alanı sınırı, temel olarak yönetimsel sınırlama oluşturur ve yetkilerin kapsamını da sınırlar (bkz. UYG.2.2.U5 Active Directory'nin sıkılaştırılması). Etki alanları birbirleri ile ağaç yapısı şeklinde ilişkilendirilebilir, etki alanları arasında "parent-child" ilişkileri oluşabilir. Bir "child" etki alanı aynı zamanda alt etki alanı olarak adlandırılır. Alt etki alanı adı, ana etki alanından oluşturulmuştur ve kendi adının nokta ile ayrılarak ana etki alanı adına eklenmesiyle türetilir.

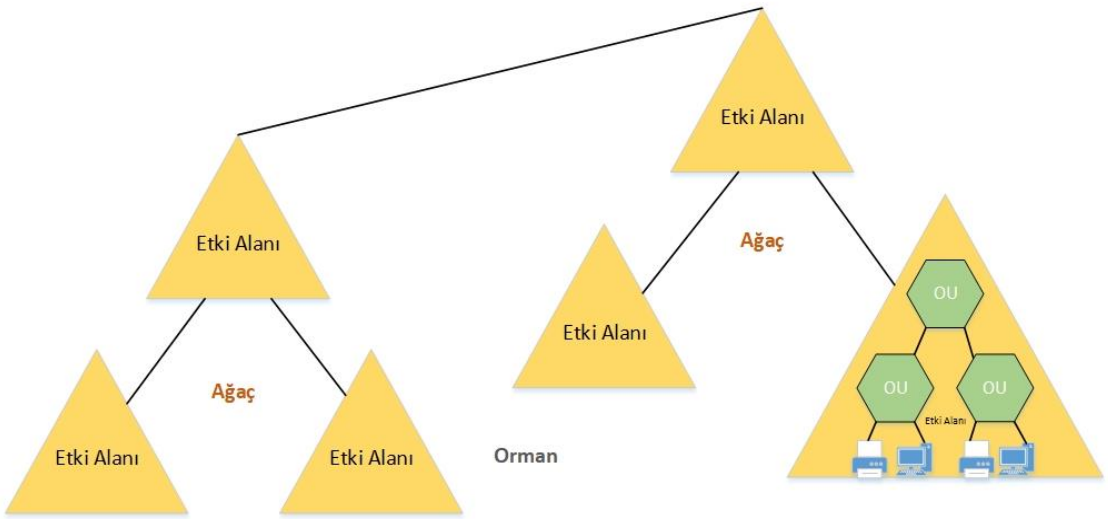
Örnek:

Ana etki alanının adı: tubitak.local

Alt etki alanının adı: bilgem.tubitak.local

Oluşturulan etki alanı adı ile ilgili DNS alan adı aynıdır. Ortak bir ad paylaşan etki alanları birlikte bir ağaç yapısını oluştururlar.

Farklı ağaç yapılarında bulunan etki alanları, farklı alan adlarına sahip olsalar bile, birlikte yönetilebilirler. Bu şekilde birleştirilmiş etki alanı ağaçları bir orman yapısı oluşturur. Özel bir durum olmakla beraber, tek bir bağımsız etki alanı da bir ağaç ve aynı zamanda bir orman oluşturur.



Şekil 10. AD Orman Mimarisi

Bir orman yapısında ilk oluşturulan etki alanı, özel bir konuma sahiptir. Orman Kök Etki Alanı (FRD: Forest Root Domain) olarak da bilinen bu alanın yöneticileri ("Enterprise Admins" grubunun üyeleri) tüm ormanda geniş kapsamlı izinlere sahiptir. Bu yüzden etki alan sınırları, söz konusu yöneticiler açısından yönetimsel sınırları temsil etmemektedir. Bir Windows etki alanı grubu oluştururken, ilk oluşturulan etki alanının her zaman orman kök etki alanı olduğu unutulmamalıdır. Orman kök etki alanının rolü, sonradan başka bir etki alanına aktarılamaz.

Active Directory içerisinde kullanıcı, bilgisayar, vb. çeşitli nesneler bulunur ve her bir nesnenin, nesne türüne özel çeşitli öznitelikleri vardır. Farklı nesne özniteliklerine, telefon numarası veya IP adresi gibi, farklı değerler atanabilir. Active Directory, varsayılan olarak tanımlanmış aşağıdaki farklı nesne türlerini barındırır:

- Etki Alanı Nesnesi: Bu nesne, bir etki alanındaki tüm Active Directory nesnelerinin köküdür ve etki alanı adı gibi, etki alanı hakkında bilgiler içerir. Diğer nesneler, bir etki alanı nesnesi altında planlanabilir.
- OU Nesneleri: Bu nesneler, diğer nesneleri gruplandırmak için kullanılır. Varsayılan olarak OU (Organizational Unit) nesnesi, bu amaçla kullanılabilir. Bir OU nesnesinin altında; bilgisayar, kullanıcı ve kullanıcı grubu nesnelerinin yanı sıra diğer OU nesneleri de yer alabilir.
- Bilgisayar Nesnesi: Bu nesne, temelde istemci ve sunucu bilgisayarlarını temsil eder. Bir bilgisayar nesnesinin altında, başka hiçbir nesne düzenlenemez. Active Directory, temelde Windows bilgisayarlarının yönetimi için tasarlanmıştır. Bu

sebeple bilgisayar nesneleri, Active Directory ile birlikte çalışan, Windows NT'den bu yana geliştirilen Windows işletim sistemlerine sahip bilgisayarları temsil eder. Ancak Windows harici diğer işletim sistemlerine sahip bilgisayarlar da etki alanına üye edilebilmektedir.

- Kullanıcı Nesnesi: Bu nesne, etki alanı kullanıcılarını temsil eder. Bir kullanıcı nesnesinin altında, başka hiçbir nesne düzenlenemez.
- Kullanıcı Grubu Nesneleri: Güvenlik grupları olarak adlandırılan bu gruplar Windows gruplarını temsil eder. Uygulama alanı (etki alanı, orman) ve içerebileceği olası grup üyeleri (etki alanı nesneleri, orman nesneleri) yönünden farklılıklar gösteren birçok grup türü vardır. Bu bağlamda gruplar; “Domain local”, “Global” ve “Universal” gruplar olarak ayrıştırılarak yönetilir. Etki alanı grup türleri ise; güvenlik grupları ve dağıtım gruplarıdır. Güvenlik grupları, izinlerin atanabilmesi amacı için kullanılır. Büyük kurumlarda çok fazla sayıda grup nesnesinin oluşturulması ve yönetimi gerekli olabilir. Bu durumda, konuya özel bir yönetim aracı kullanılması uygun olacaktır. Bu araç, kurum tarafından geliştirilecek komut dosyalarından oluşabileceği gibi, üçüncü parti firmalar tarafından geliştirilmiş ürünler de bu amaçla kullanılabilir. Bununla birlikte, hangi araçların yararlı olup olmadığına, ilgili duruma göre karar verilmelidir.

Genel Active Directory yapısı aşağıdaki gibi temsil edilebilir:

- Etki alanı nesnesi, bir etki alanı Active Directory ağacının köküdür.
- OU nesneleri; bilgisayar, kullanıcı ve kullanıcı grubu nesnelerini yapılandırılmış bir şekilde toplamak için etki alanı nesnesi altında oluşturulur. OU nesneleri iç içe bir yapıda oluşturulabileceğinden bu durum, kuruma özgü bir ağaç yapısının oluşmasına neden olur.

Standart bir ilk kurulum sonrasında, basit ve temel bir Active Directory yapısı oluşur ve bu yapı daha sonra Active Directory planlamasına göre değiştirilebilir. Active Directory ile temelde Windows sistemleri yönetileceğinden, tasarlanan yapının öncelikle bu yönetim amacına uygun olmasına dikkat edilmelidir. Bunun yerine, Active Directory yapısının kurum organizasyonel yapılanmasına en küçük ayrıntısına kadar benzer şekilde kurgulanması, hem yönetimsel sorunlara yol açabilir, hem de yüksek operasyonel maliyetler oluşturabilir.

Active Directory şeması, Active Directory yapısında yer alabilen her nesne sınıfının ve her bir nesnede bulunabilen özniteliklerin tanımlarını içerir ve gerekli durumlarda değiştirilebilir özelliktedir. Ancak şema değiştirme işlemi yalnızca detaylı bir planlama sonrasında yapılmalıdır. Ormanda tek bir şema bulunur ve kopyası her bir etki alanı denetleyicisinde

barındırılır. Bu yüzden, şema değişikliği, ortak yönetilen tüm etki alanlarını etkiler. Şema değişikliği önemli bir işlem olduğundan, bu işlem sadece “Schema Master” rolüne sahip sunucu kullanılarak, “Schema Admins” grubunun üyeleri tarafından gerçekleştirilebilir. Belirli koşullar altında, şema değişiklikleri geri alınamayabilir. Bu yüzden, bu grup üyeliğinin düzenli bir şekilde kontrol edilmesi gerekmektedir.

"Enterprise Admins" grubu üyelerinin (varsayılan olarak orman kök etki alanının yöneticisi bu gruba üyedir), Active Directory yapısında yer alan her etki alanında özel yetkileri vardır. Örneğin, orman yapısına yeni etki alanları ekleyebilmek ve Active Directory'deki tüm etki alanı denetleyicilerinde yönetici haklarına sahip olmak bu yetkilerden bazılarıdır.

Tek bir etki alanının var olduğu mimaride yönetim, etki alanına özgü “Domain Admins” grubunun üyeleri tarafından yapılır. Bu grup üyeleri, bulundukları etki alanı içerisinde sınırsız yönetim ayrıcalıklarına sahiptir. Ancak, diğer kullanıcı hesaplarına da yönetimsel görevleri devretmek mümkündür (bkz. UYG.2.2.U2 Active Directory Yönetiminin Planlanması).

Bir etki alanındaki yönetimsel görevlerin devir işlemi, yalnızca kullanıcı hesaplarının ve bilgisayarların bir kısmının yönetimi devredilerek de yapılabilir. Yönetimsel devir, etki alanı içindeki kullanıcı veya bilgisayar hesaplarını gruplamak için kullanılan OU seviyesinde gerçekleştirilebilir.

Windows istemcilerin yapılandırmasına dair çeşitli parametreler grup ilkeleri içerisinde yer almaktadır. Bu ilkeler, bilgisayarların veya kullanıcı hesaplarının merkezi olarak yapılandırılmasını mümkün kılar. Active Directory'de barındırılan grup ilkelerinin kapsama alanı, tüm etki alanı veya OU'lar olabilir. OU'lar benzer olarak yapılandırılmış bilgisayarları veya kullanıcı hesaplarını toplamak için kullanılır. İç içe yapılandırılabileceklerinden ve bir tek OU’ya birden çok grup ilkesi ile ilişkilendirilebileceğinden, OU içerisinde yer alan bir bilgisayar nesnesini pek çok grup ilkesi parametresi etkiliyor olabilir (Ayrıca bkz. UYG.2.2.U3 Grup ilkelerinin planlanması).

Active Directory, verileri depolamak için ilişkisel yapıda kendine has bir veri tabanı kullanır. Etki alanı denetleyicileri, etki alanındaki kullanıcıların ve bilgisayarların merkezi kimlik doğrulaması ve yetkilendirmesini sağlamak için Active Directory'den yararlanır. Bu amaçla kullanılan çeşitli protokoller aşağıda belirtilmiştir:

- Active Directory nesneleri ve özniteliklerini sorgulamak için LDAP (Lightweight Directory Access Protocol)
- Kullanıcıların ve bilgisayarların kimlik doğrulaması için Kerberos
- Bilgisayar ağındaki dosyaların aktarımı için CIFS (Common Internet File System)

- Ağdaki bilgisayar sistemlerinin isim çözümlemesi için DNS (Etki Alanı Adı Sistemi)

Bazı istisnalar dışında, her bir etki alanı denetleyicisi yalnızca kendi etki alanına ilişkin verileri içerir. Bu istisnalar şunlardır:

- Her etki alanı denetleyicisi, tüm ormanın şema ve yapılandırma verilerini içerir.
- Her etki alanında en az bir etki alanı denetleyicisi, ek olarak "Global Katalog" verilerini içerir.

Active Directory verisi, bir etki alanı içinde yer alan etki alanı denetleyicileri arasında, replikasyon aracılığı ile eşzamanlı olarak senkronize edilir. Etki alanı verisi, yalnızca etki alanı ile ilgili bilgileri içerir. Bir orman yapısındaki diğer etki alanlarına dair bilgilere hızlı bir şekilde erişebilmek için, Global Katalog (GC) olarak adlandırılan rol tesis edilmiştir. Global katalog, Active Directory nesnelerine ait kısmi bilgilerden oluşur ve bu bilgiler orman yapısı içerisinde replike edilir. Böylece global katalog, orman yapısı içerisinde yer alan diğer etki alanlarına dair bilgilerin sorgulanmasını sağlar. Bu yönü ile global katalog, tüm orman yapısını ilgilendiren bilgilerin başvuru adresidir.

Yukarıda bahsi geçen ağaç benzeri, hiyerarşik yapıya ek olarak Active Directory, kurumun organizasyon yapısına ve ağ yapısına uygun olarak kullanılabilecek ”Active Directory Site” yapısı da sunmaktadır. Active Directory site yapısı, kimlik doğrulama işlemlerinin kısa sürede gerçekleşmesi, site bazlı uygulamaların kullanılabilmesi ile beraber etki alanı denetleyicilerinin replikasyon mimarisini de etkiler. Her Active Directory site içerisinde, global kataloğun bir kopyasını tutan en az bir etki alanı denetleyicisi olması gerekir. Global katalog, kullanıcının oturum açma işleminin bir parçası olarak hizmet etmektedir, bu sebeple oturum açma sürecinde bir global katalog sunucusunun her zaman erişilebilir olması gerekir. Bu konuda, Windows sunucunun ilk kurulum esnasında otomatik olarak oluşturmuş olduğu Active Directory site yapısı, kurum koşullarına göre uyarlanmalıdır (ör. farklı şehir veya ülkelerde yer alan ofis alanlarına göre özelleştirilmesi).

Active Directory verileri, çoklu ana çoğaltma yöntemi (Multi-master) ile kurumun etki alanı denetleyicileri arasında replike edilir. Bu yapı sayesinde tüm etki alanı denetleyicileri, ana bir sunucu olmasını beklemeksizin, birbirleri arasında replikasyon yapabilirler. Her etki alanı denetleyicisinin, değiştirilebilir ve gelecek replikasyonda temel olarak kullanabilir olduğu bir Active Directory kopyası vardır. Bir kurumda, birden çok etki alanı denetleyicisi kullanımı, Active Directory'nin yedek kopyalarının oluşturulmasını sağlar ve bu bağlamda topyekûn felaket olasılığını en aza indirir.

Etki alanı denetleyicileri arasındaki verilerin senkronizasyonu, iki farklı replikasyon mekanizması (RPC veya eşzamansız SMTP) aracılığıyla yapılabilir. Hangi mekanizma kullanılırsa kullanılsın, replikasyonun gerçekleşeceği sıklık yapılandırılabilir.

Dağıtık veri tabanı mimarisi sayesinde Active Directory'nin güvenilirliği, yeterli sayıda oluşturulmuş dağıtık yapıdaki etki alanı denetleyicisinin kullanımı ile sağlanabilir. Ancak burada dikkat edilmesi gereken husus, FSMO rollerinin sahiplikleri konusudur.

FSMO Rolleri

Operations Master veya FSMO (Flexible/Floating Single Master Operations), AD'nin etki alanı denetleyicilerine dair bir özelliğidir. FSMO görevleri, normal etki alanı denetleyicileri tarafından gerçekleştirilemeyen ve onların görevlerinden farklı olan, özellikli görevlerdir. Öte yandan, FSMO görevleri sadece, ana veri tabanı adı verilen tek bir veri tabanında (single-master) gerçekleştirilebilir.

Etki Alanı seviyesinde aşağıdaki FSMO rolleri vardır:

- PDC Emulator: Diğer rollerinin yanı sıra zaman senkronizasyonundan da sorumludur.
- RID Master: Etki alanı içerisindeki nesnelere tutarlı tekil ID'ler (SID) atanmasını sağlar.
- Infrastructure Master: Çoklu etki alanları mimarisinde tutarlılığı sağlar.

Orman seviyesinde ise aşağıdaki FSMO rolleri yer alır:

- Schema Master: Şema değişikliklerinin replike edilmesini sağlar (örneğin, etki alanı denetleyicilerini yükseltirken veya kurumda Exchange Server/ Skype for Business, vb. ürünlerin kurulumunu gerçekleştirirken).
- Domain Naming Master: Yeni etki alanı oluşturma veya silme işlemlerinde görev alır.

FSMO rollerine sahip olan etki alanı denetleyicilerinin yüksek önem dereceleri nedeniyle, hassasiyetle korunmaları gerekmektedir.

UYG.2.2.U5 Active Directory'nin sıkılaştırılması

Active Directory, rolü itibari ile kurumun tüm güvenliğine etki edebileceğinden, tüm bileşenlerin eksiksiz bir şekilde sıkılaştırılması gereklidir.

Varsayılan hesapların acil durum hesapları olarak kullanılması

Varsayılan hesaplara, karmaşık parolalar verilmeli ve bu hesaplar sadece acil durum hesapları olarak kullanılmalıdır. Bu amaçla, parolalar güvenli bir yerde saklanmalı ve acil durumda kim tarafından, ne şekilde kullanılması gerektiğine dair bir süreç tanımlanmalıdır.

Korumalı Kullanıcılar Grubu (Protected Users Group)

Ayrıcalıklı hesaplar için korumalı kullanıcılar grubunun kullanılması önerilir. Bu gruba üye olan hesapların kimlik doğrulamasında yalnızca Kerberos kullanılabilir. Bu kullanım şekli "pass-the-hash" saldırılarını önler. Ancak korumalı kullanıcılar grubu özelliğinin kullanılabilmesi için etki alanı seviyesinin en az Windows 2012 olması gerekir. Ağdaki tüm uygulamalar Kerberos ile uyumlu olmalıdır.

Grup Seviyesinde Yönetilen Hizmet Hesapları (Group Managed Service Accounts)

Servis hesabı kullanan SQL, IIS, SCOM, SCCM vb. uygulamalar için grup seviyesinde yönetilen hizmet hesapları kullanılması tavsiye edilir.

Eğer bu durum mümkün değilse, bir hizmet hesabı parolasının "brute force" atakları ile ifşa edilmesini önlemek için, tüm servis hesapları yeterli uzunlukta bir parola ile korunmalıdır. Etki alanı seviyesi Windows Server 2008'den bu yana bu kullanım şekli, parola politikası aracılığı ile uygulanabilir durumdadır.

Windows sunucuyu bir etki alanı denetleyicisi olarak yapılandırma

Etki alanı denetleyicileri, Active Directory hizmeti aracılığı ile bir etki alanını yönetmek için gereken hizmetleri sağlarlar. Genel olarak bir etki alanı denetleyicisi, Active Directory'nin olmazsa olmaz bir servisi olan DNS (Etki Alanı Adı Hizmeti) hizmetini de sunar. Windows ortamında DNS hizmeti, önemli Windows kaynaklarına erişim için referans sağlar ki bu kaynakların bütünlüğü, Windows Sunucu etki alanının düzgün çalışması için önem arz eder. Bir etki alanı denetleyicisi, bir oturum açma sunucusu olarak da hizmet ettiği için Kerberos servisini de çalıştırır. Etki alanı denetleyicisindeki Kerberos bileşenleri, kimlik doğrulama protokolünde kullanılan gizli anahtarları da korur.

Her etki alanı denetleyicisi, bu bağlamda çok önemli bir rol oynadığı ve değerli veriler barındırdığı için, hassasiyetle korunabilmesi amacı ile yapılandırma sürecinde aşağıdaki noktalara dikkat edilmelidir. Bu maddelere ilaveten, işletim sistemi temelindeki önlemler de etki alanı denetleyicisine, kapsamı dâhilinde uygulanmalıdır.

- Bir etki alanı denetleyicisinin güvenliği temel olarak iki ana alandan oluşur: işletim sistemi yapılandırmasının güvenliği ve kendi güvenlik mekanizmalarını kullanan Active Directory'nin güvenliği (ayrıca bkz. UYG.2.2.U4 Active Directory yönetimi

eğitimi). İşletim sisteminin güvenlik ayarları temel olarak grup ilkelerine dayanmaktadır. Active Directory'nin güvenlik ayarları, detaylı bir planlama ve uygulama gerektirir (bkz. UYG.2.2.U1 Active Directory'nin planlaması, UYG.2.2.U3 Grup ilkelerinin planlanması).

- Sadece yetkili yöneticiler yerel olarak bir etki alanı denetleyicisinde oturum açabilir. Bir etki alanı denetleyicisinde, standart kullanıcıların işlem yapmasına izin verilmemelidir. Bu nedenle, standart bir kurulumdan sonra, standart kullanıcıların bir etki alanı denetleyicisine yerel olarak oturum açmasına izin verilmez.
- Bir etki alanı denetleyicisinin, zorunlu standart etki alanı denetleyicisi hizmetleri (örneğin Active Directory, Kerberos ve DNS) dışında, diğer altyapı hizmetlerini (DFS, DHCP gibi) sağlamaması önerilir. Özellikle de DHCP hizmetinin bir etki alanı denetleyicisi aracılığı ile sağlanması, güvenlik nedenleriyle önerilmez.
- Sunucu uygulamalarında yaşanabilecek hatalar, etki alanı denetleyicisini ve dolayısıyla tüm etki alanını tehlikeye atabileceği için, bir etki alanı denetleyicisi herhangi bir uygulama sunucusu hizmeti sağlamamalıdır.
- Bir etki alanındaki yönetimsel verileri bilgisayarlar arasında iletmek için kullanılan kanal yapılandırması, olabildiğince güvenli olmalıdır (bkz. UYG.2.2.U8 Windows ortamında güvenli kanal yapılandırması).
- Bir etki alanı denetleyicisi, "Active Directory Geri Yükleme" modunda açılabilirse, eski bir yedek dosyasından (kısmi veya tamamen) geri yükleme ile Active Directory'de değişiklik yapmak mümkün olur. Bu değişiklikler, geri yüklemenin gerçekleştirildiği etki alanı denetleyicisinin yeniden başlatılması akabindeki süreçte ise, replikasyon yolu ile etki alanındaki diğer tüm etki alanı denetleyicilerine yayılacaktır. Bu nedenle, "Active Directory Geri Yükleme Modu"nun sıkılaştırılmış bir parola ile korunması ve bu modda yapılacak çalışmanın en az iki kişi tarafından gerçekleştirilmesi zaruridir. "Active Directory Geri Yükleme Modu" komut tabanlı çalışır ve komutlardaki yazım hataları ciddi sonuçlara neden olabilir (örneğin, yanlış Active Directory ağaç yapısının silinmesi veya üzerine yazılması gibi). Bu sebeple, işlemin en az iki kişi tarafından gerçekleştirilmesi prensibi, ek bir kontrolü de beraberinde getireceği için de fayda sağlayacaktır.
- Orman Kök Etki Alanı'nın (FRD) Etki Alanı Denetleyicileri, özel rolleri nedeniyle hassasiyetle korunmalıdırlar.

Etki alanı denetleyicilerinin güvenli işletimi

Yapılandırma hatalarını önlemek ve etki alanında tutarlı bir güvenlik düzeyini sağlamak için, etki alanı denetleyicilerinin, referans kurulumdan alınan konfigürasyonlar ile yapılandırılmaları önerilir. Ayrıca, etki alanı denetleyicisinin temel yapılandırılmasında güvenlik ayarları standart şekilde yapılmalıdır. Bu standardizasyon, etkileri öngörülebilir ve yinelenebilir şekli ile tüm sistem yöneticileri tarafından kolayca uygulanabilecek bir sürecinin oluşturulması ile sağlanmalıdır. Bu süreç aşağıdaki hususları içerir:

- Güncel yama ve servis paketlerinin yüklenmesi

  Güncel yama ve servis paketlerinin düzenli aralıklarla yüklenmesi tavsiye edilir. Ancak, yama ve servis paketleri üretim ortamına yüklenmeden önce, bir test ortamında kapsamlı olarak test edilmeli ve etkileri gözlenmelidir. Test edilen yama ve servis paketinin herhangi bir olumsuz etki yaratmayacağı anlaşılırsa, üretim ortamına yükleme gerçekleştirilmelidir.

- Yeterince sıkılaştırılmış parolaların belirlenmesi

  Active Directory kullanıcı hesapları için (özellikle etki alanı yöneticileri için) yeterince sıkılaştırılmış parolalar atanmalıdır. Yeterince sıkılaştırılmış parolaların tanımı, kurum parola kullanımı politikasında yer almalıdır. Karmaşık parolaların oluşturulmasına ek olarak, parolaların ilgili kullanıcı sahiplerine güvenli iletişim kanalları üzerinden aktarılması da sağlanmalıdır. Ayrıca, ilk oturum açma esnasında kullanıcılar, kendilerine bildirilen parolaların kendi belirleyecekleri parola ile değiştirilmesine zorlanmalıdırlar.

Çalıştırılabilir dosyaların yetkilendirilmesi

Etki alanı denetleyicilerinin kök klasörlerini, diskin boş alanının doldurulmasına yönelik saldırılardan korumak için, “Everyone” grubunun yetkileri sınırlandırılmalıdır. "Tam erişim" yetkisi yalnızca yöneticilere sağlanmalıdır.

Etki alanı denetleyicisinin farklı işletim sistemi ile başlatılmasının engellenmesi

Etki alanı denetleyicilerinin farklı işletim sistemleri ile başlatılması durumunda, NTFS erişim kısıtlamaları devre dışı kalabilir ve kritik verilere erişim elde edilebilir. Bu durumun engellenebilmesi için kurumsal düzenlemeler ile sunucunun fiziksel güvenliği sağlanmalıdır.

Ayrıca, uzaktan başlatma ile uzaktan yükleme hizmetlerinin (RIS veya BOOTP) devre dışı bırakılması ve sistem başlangıcında BIOS parolası kullanılması önerilir.

Disk şifreleme ile koruma (Bitlocker)

Etki alanı denetleyicilerinin denetim dışı yeniden başlatılmasını engellemek amacı ile kullanılabilecek daha güvenli olan bir yöntem, yeniden başlatılma sürecinde özel bir parola girilmesini gerektiren disk şifreleme yöntemidir.

Etki alanı ve etki alanı denetleyicileri için güvenli politika ayarları

Active Directory hizmeti veren bir Windows Sunucu, etki alanı ve etki alanı denetleyicileri için varsayılan güvenlik politikası ayarlarından etkilenir. Etki alanı ve etki alanı denetleyicilerinin güvenliğini artırmak için varsayılan politika ayarlarında aşağıdaki değişikliklerin gerçekleştirilmesi önerilir:

- Güvenli Parola Politikası Ayarları

  Etki alanı denetleyicilerine erişim, güçlü mekanizmalarla güvence altına alınmalıdır. Bu amaca yönelik olarak uygulanacak gerekli parola politikası yapılandırmalarına dair daha fazla bilgi, ilgili Microsoft makalelerinde bulunabilir.

- Hesap Kilitleme Politikaları

  Oturum açma girişimlerinin olay günlüğüne kaydedilmesi (ayrıca bkz. UYG.2.2.U11 Active Directory altyapısını izleme) önerilir. Bu şekilde saldırıları algılamak mümkün olacaktır. Örneğin, oturum açma sırasında çok sayıda başarısız parola girişi, kaba kuvvet saldırısı yapıldığına dair bir gösterge olabilir. Hesabın kilitlenmesine dair yapılandırma; hesap kilitleme süresi, hesap kilitleme eşiği ve hesap kilitleme sayacının sıfırlanması gibi parametreler aracılığı ile sağlanır (bkz. UYG.2.2.U3 Grup ilkelerinin planlanması).

- Kerberos Politika Ayarları

  Kerberos, bir kullanıcının veya bilgisayarın kimliğini doğrulamak için kullanılan kimlik doğrulama protokolüdür. Kerberos kimlik doğrulama sürecinde yer alan temel bileşenler, kimlik doğrulaması yapmak isteyen istemci, istemcinin talep ettiği servisi sunan sunucu ve hem istemci hem de sunucu tarafından güvenilir bir iletişim kurulmasını sağlayan KDC (Key Distribution Center) rolüne sahip sunucudur. İstemci, oturum açma esnasında KDC sunucusuna bir kullanıcı tanımı bildirir. KDC ise TGT (ticket granting ticket) adı verilen özel bir bileti istemciye gönderir. İstemci TGT'yi elde ettikten sonra, talep ettiği kaynağa ulaşmak istediğinde TGT'yi etki alanı denetleyicisine iletir, etki alanı denetleyicisi TGT'yi analiz edip kaynağa erişim için süreli bir oturum anahtarı (session key - SA) oluşturarak istemciye gönderir.

İstemci bu oturum anahtarı (session key - SA) sayesinde, biletin kullanım süresi dolana kadar talep ettiği kaynağa erişim sağlar.

Kerberos politikası parametrelerini özelleştirerek, Kerberos biletinin süresi gibi özelliklere dair yapılandırmaları gerçekleştirmek mümkündür (bkz. UYG.2.2.U3 Grup ilkelerinin planlanması).

Güvenli bir etki alanı denetleyicisi politikası için aşağıdakilerin de göz önünde bulundurulması önerilir:

- Kullanıcı hakları, ilgili kullanıcıların etki alanındaki veya etki alanı denetleyicisindeki yalnızca sorumlu oldukları operasyonel veya yönetimsel görevleri gerçekleştirebilmeleri için kısıtlanmalıdır. Kullanıcıların erişim olanakları, etki alanı denetleyicilerinin güvenliğini tehlikeye atmamaları için kısıtlanmalıdır (ayrıca bkz. UYG.2.2.U1 Active Directory'nin planlaması).
- Etki alanı denetleyicilerinin izleme politikası; yönetim veya yapılandırma değişiklikleri gibi hassas operasyonlarının kim tarafından gerçekleştirildiğine dair tespit yapılabilmesini mümkün kılacaktır. İzleme parametreleri; oturum açma denemeleri, hesap yönetimi, Active Directory erişimi, Active Directory nesnelerine erişim girişimleri, grup ilkesi değişiklikleri, yetkilerin kullanımı, çalışan işlemleri ve sistem olaylarının izlenmesini içermelidir (bkz. UYG.2.2.U11 Active Directory altyapısını izleme).
- Önemli Active Directory nesneleri (ör. Active Directory dizinleri), uygun politika ayarları ile izlenmelidir. Bunun sağlanabilmesi için, dizin bölümlerinin (Active Directory veri tabanının mantıksal bölümleri) izlenmesi gerekir. Dizin bölümleri "Schema", "Configuration", "Domain" ve "Application" bölümleridir.

Politika ayarlarının yapılmasına ilişkin yukarıdaki önerilerin uygulanması ile birlikte, daha fazla sayıda olayın izlenmesi ve kaydedilebilmesi için, güvenlik günlüğünün varsayılan maksimum boyutunun artırılması gerekir. Kayıtlar belirli aralıklar ile izlenmeli ve değerlendirilmelidir. Ayrıca, zamanında arşivleme için bir prosedür tanımlanmalı, güvenlik ve sistem olay kayıtları düzenli olarak yedeklenmelidir. Bu şekilde, hiçbir olay kaydının kaybolmaması veya değiştirilmemesi güvence altına alınmış olur.

Ayrıca, farklı ormanlardaki etki alanları arasında, uygulama paylaşımı gibi bir sebeple bir işbirliğini sağlamak amacıyla, dış güven ilişkilerinin oluşturulması gerekebilir. Ancak, dış güven ilişkileri güvenlik sınırlarını ihlal ettiği için potansiyel bir güvenlik riski oluşturur. Bu nedenle, güvenilen etki alanındaki etki alanı denetleyicileri, kullanıcı yetki verisini

filtrelemeli ve kullanıcı hesabının etki alanıyla ilgili olmayan güvenlik tanımlayıcılarını (SID) kaldırmalıdır.

Etki alanı denetleyicileri için güvenlik politikası ayarları, Windows Sunucu işletim sistemlerinin güvenlik yapılandırması ayarlarını etkilediği için dikkatli bir şekilde ayarlanmalıdır. Bu durum, sadece Active Directory ile ilgili yapılandırma için değil, aynı zamanda, Windows sunucu işletim sistemleri (ağ, dosya sistemi ve kullanıcı oturum açma, güvenlik yapılandırma ayarları) bileşenleri için de geçerlidir.

Etki alanı denetleyicileri için virüs koruması

Bir kurumda, bilgisayar virüslerine ve diğer zararlı programlara karşı yeterli bir koruma için, kapsamlı bir virüs koruma planı uygulanmalıdır. Bu kapsamda, kurumun etki alanı denetleyicileri de virüs koruma planı içerisinde değerlendirilmelidir.

Ancak bir etki alanı denetleyicisi için kullanılan virüs koruma programının olumsuz bir etkiye sebep olmaması açısından, bazı özel durumlara dikkat edilmelidir. Bu önlem kapsamında rehberde yer alan öneriler, genel talimatlar olarak kabul edilmelidir. Bazı özel durumlarda, kullanılan virüs koruma yazılımı üreticisinin özel talimatları da dikkate alınmalıdır.

Bir virüs koruma yazılımı seçerken, yazılımın bir etki alanı denetleyicisi rolünde sağlıklı çalışabilirliğinin desteklendiği net bir şekilde teyit edilmelidir. Aksi durumda virüs koruma yazılımı, tarama yaptığı dosyaların meta verilerinin değişimine sebep olabilir. Bu durumda, FRS (File Replication Service), değiştirilen dosyanın kurum içerisinde çoğaltılmasına neden olur. Bu tür gereksiz replikasyonlar, sistem performansının kaybına neden olabilir ve bu durumdan kaçınılmalıdır.

Virüs koruma yazılımının amacına yönelik performanslı bir şekilde çalışma durumu, yazılımın üretim ortamına yaygınlaştırılmasından önce, bir test ortamında kapsamlı bir şekilde test edilmelidir. Kullanılan test ortamı, üretim ortamının koşullarını mümkün olduğunca yansıtıyor olmalıdır.

Kötü amaçlı yazılımların sızmasını önlemek için, etki alanı denetleyicileri yalnızca Active Directory servisini sunmalı ve mümkünse başka bir hizmet sunmamalıdır. Özellikle bir etki alanı denetleyicisi, standart istemci işlemleri için kullanılamaz. Örneğin, bir etki alanı denetleyicisinde yerel olarak oturum açan kullanıcılar, Internet'te gezinememeli, e-posta alamamalı veya USB bellek gibi harici ortamlara erişememelidir.

Benzer şekilde etki alanı denetleyicisi, bir dosya paylaşım sunucusu olarak kullanılmamalıdır. Dosyalar, etki alanı denetleyicisinde paylaşıma açılırsa, zararlı yazılımın eriştiği her an, virüs koruma yazılımı tarafından taranırlar ki bu durum etki alanı

denetleyicisinde performans kayıplarına neden olabilir. Etki alanı denetleyicisindeki dosya paylaşımları, bu nedenle devre dışı bırakılmalıdır.

Temel olarak, virüs koruma yazılımı tüm dosya erişimlerini arka planda şeffaf olarak izlemelidir. Ancak, Windows Sunucu işletim sistemlerindeki bazı dosyalara (ör. dizin hizmeti veri tabanı, günlük dosyaları, dosya çoğaltma hizmeti veri tabanı vb.) bir virüs koruma programı tarafından erişilmesi, etki alanı denetleyicisinin işlevlerini engelleyebilir. Bu nedenle, virüs koruma yazılımı sebebi ile ilgili dosyaların kilitlenmesini önlemek ve etki alanı denetleyicisinin sağlıklı çalışmasını sağlamak için aşağıdaki temel dizinlerde bulunan ilgili dosyaların tarama kapsamı dışında bırakılmasına dikkat edilmelidir.

Varsayılan dizin olarak %windir%\Ntds altındaki

- Ntds.dit, Ntds.pat, EDB*.log, Res*.log, Edb*.jrs ile Temp.edb, Edb.chk dosyaları

Varsayılan dizin olarak %windir%\Ntfrs altındaki

- %windir%\Ntfrs\jet\sys klasöründeki edb.chk
- %windir%\Ntfrs\jet klasöründeki Ntfrs.jdb
- %windir%\Ntfrs\jet\log klasöründeki *.log, Edb*.jrs
- %systemroot%\Sysvol\Domain ve %systemroot%\Sysvol_DFSR\Domain

  altındaki *.adm, *.admx, *.adml, Registry.pol, *.aas, *.inf, Scripts.ini, *.ins, Oscfilter.ini dosyaları

Antivirüs yazılımı tarafından tarama kapsamı dışında bırakılması gereken dizin ve dosyalara dair detaylı bilgiye Microsoft'un ilgili makalesinden ulaşılabilir.

RDP

Bir RDP oturumu sonlandırılır iken, kullanıcının otomatik olarak oturumu kapatması sağlanmalıdır. Bu yapılandırma GPO aracılığı ile gerçekleştirilebilir.

Ayrıca uzaktan bağlantıda "Restricted Admin Mode" kullanımı önerilir. Bu mod etkinleştirildiğinde, RDP yoluyla örneğin Windows 8.1 istemciden bağlantıyı başlatıp, Windows 2012 R2 sunucuda oturum açar iken, bağlantının gerçekleştirilmiş olduğu son kullanıcı işletim sistemi ile bağlantının yapıldığı Windows Sunucu 2012 R2 işletim sistemi arasında, kullanıcı kimlik bilgileri gidip gelmeyecektir. Geliştirilen bu güvenlik özelliği, "Pass-the-Hash (PtH)" yöntemi kullanılarak gerçekleştirilebilecek saldırıların engellenebilmesi amacı ile sunulmuştur.

UYG.2.2.U6 Active Directory'nin operasyonel güvenliğini sağlamak

Sistem yöneticileri, üretim ortamında kullanılan etki alanı denetleyicilerinin, önceden belirlenmiş olan güvenlik düzeylerini koruyacak şekilde faaliyetlerini sürdürmeli ve güvenlik gereksinimleri arttığında yeni duruma göre güvenlik seviyesini arttırmalıdırlar. Sistemde gerek bakım gerekse farklı sebeplerle yapılacak olan değişikliklerin ne şekilde gerçekleştirileceklerine dair yönergeler ayrıca oluşturulmalıdır.

Güven ilişkilerinin kısıtlanması

Etki alanları arası ve özellikle diğer orman yapıları ile kurumun orman yapısı arasında oluşturulan güven ilişkileri; halen ihtiyaç duyulup duyulmadıkları, doğru tipte oluşturulup oluşturulmadıkları (örneğin iki yönlü bir güven ilişkisinin gerçekten gerekli olup olmadığı) ve yeterli güvenlik sıkılaştırılmalarının sağlanıp sağlanmadığı gibi noktalar açısından düzenli olarak değerlendirilmelidir.

"Bu güven ilişkisi silinirse ne olur?" sorusunun kurulu tüm güven ilişkileri için sorulması önerilir. Eğer bu tür bir soruya cevap verilemiyorsa ya da durum net değilse, standart test prosedürleri ve geri dönüş planlaması dikkate alınarak, güven ilişkisi devre dışı bırakılabilir. Güven ilişkisinin devre dışı bırakılması akabindeki testlerde de herhangi bir sorun ortaya çıkmaması durumunda, güven ilişkisi tamamen silinebilir.

Servis yönetici hesaplarının hüvenliği

Active Directory hizmetinin yapılandırılmasının ve işletiminin sorumluluğu, yalnızca güvenilir kişilere devredilmelidir. Bu kişiler, kurumun mevcut güvenlik kurallarına aşina olmalı ve sorumluluk alanlarındaki faaliyetlerini bu kurallar kapsamında yürütmelidirler.

Servis yöneticilerinin yetkileri, kendilerine verilen görevleri yerine getirebilmeleri için yeterli ve asgari düzeyde tutulmalı ve yalnızca hedeflenen görevler için kullanılmalıdır. Yönetimsel ayrıcalıklara sahip hesaplar, periyodik olarak gözden geçirilmeli ve gerektiğinde yeniden yapılandırılmalıdır. Ayrıca, yönetici hesaplarının üye sayısı gerekli asgari düzeyde tutulmalıdır. Yönetici gruplarına üye hesaplar için yeterince sıkılaştırılmış parolaların kullanılması zorunlu olmalıdır. Ayrıca, işletim sisteminde oturum açmak için akıllı kartların kullanımı gibi güçlü kimlik doğrulama yöntemleri kullanılması düşünülebilir.

Domain Admins Grubu'nun sınırlandırılması

İdeal durumda, etki alanı yöneticileri grubu (Domain Admins) boş olmalı, yönetim için yeni gruplar oluşturularak, her bir gruba yalnızca faaliyet alanları için ihtiyaç duyulan hakların atanması sağlanmalıdır.

Active Directory'deki yönetici hesapları, sadece etki alanı ve etki alanı denetleyicileri üzerinde tam yönetimsel hakları elde etme ihtiyaçları var ise, ilgili etki alanının yöneticileri grubuna (Domain Admins) üye edilmelidirler. Sadece bu tür bir sorumluluğun verileceği kişiler, bu grubun üyesi haline getirilmelidirler.

Acil durumlar için bir etki alanı yöneticisi hesabı (ör. kurulumla birlikte varsayılan olarak yer alan ve güçlü bir parola ile korunan etki alanı yöneticisi hesabı) hazır bulundurulmalı, güvenli bir şekilde muhafaza edilmeli ve etki alanı yöneticilerinin hiçbirinin kurumda bulunmadığı durumlarda kolayca erişilebilir olmalıdır.

Aktif olmayan hesapların Active Directory'den kaldırılması

Kullanılmayan hesaplar Active Directory'de devre dışı bırakılmalı ve kurum güvenlik politikasında belirtilen zaman sonrasında silinmelidir. Bu sayede saldırganlar tarafından kötü amaçlı kullanım engellenebilir. Devre dışı bırakılmış hesabın kullanımına dair bir teşebbüsün, güvenlik tehdidi olarak değerlendirilmesi önerilir.

Bu konuda takip edilebilecek en güvenli yol; kullanım amacı sonlandığı zaman hesapların otomatik olarak Active Directory'den kaldırılmasıdır. Bu çözüm, teknik veya organizasyonel yapılandırma ile sağlanabilir.

Temel yapılandırma bilgisinin güncelliğini korumak

"Temel yapılandırma bilgisi" ifadesi, Active Directory'nin en önemli yapılandırma parametrelerini özetler. Söz konusu temel yapılandırma bilgileri dokümante edilmelidir. Temel yapılandırma bilgileri en azından aşağıdaki hususları içermelidir:

- İzleme politikası
- Grup ilkesi nesneleri ve ilişkilendirilme durumları
- Mevcut güven ilişkileri
- Etki alanı denetleyicilerinin ve servis yöneticilerinin OU yapısı
- FSMO rol yapısı
- Replikasyon topolojisi
- Veri tabanı özellikleri
- Etki alanı denetleyicileri ve yönetim amaçlı kullanılan istemcilerde yüklü olan hizmet paketi ve yamalar ile bunların güncel durumu
- Mevcut yedekleme mimarisi
- Yedekleme ortamının kontrolü
- Servis yöneticisi yetkilerinin kontrolü

Dokümante edilen bu temel bilgiler sayesinde Active Directory'de yapılan değişiklikleri izlemek ve incelemek mümkün hale gelir. Tüm etki alanı denetleyicilerine dair temel yapılandırma bilgilerinin, bir veri tabanında konsolide edilmesi önerilir. Bu tür bir veritabanı ek olarak, hali hazırda kullanılan bileşenlere dair genel bir bakış sağlar. Temel bilgilerin korunmasına yönelik sorumluluklar da net olmalıdır.

UYG.2.2.U7 Active Directory için güvenli yönetim yöntemlerinin uygulanması [Sorumlu Teknik Uzman]

Standart ve ayrıcalıklı hesapların ayrıştırılması

Yönetici hesaplarının ve yönetim amacıyla kullanılan izole sistemlerin, günlük standart operasyonlar için kullanılmaması gerekir. Yönetici hesapları ve yönetim sistemlerinin, İnternet erişimi için de kullanılmaması önerilir.

Yönetim faaliyetini yürütecek olan her kullanıcının, genel kullanım için standart bir kullanıcı hesabına sahip olması, yönetim faaliyetlerini ise ayrı bir hesap ile yürütmesi önerilir. Yönetim hesabı, hiç bir biçimde, genel faaliyetler için kullanılmamalıdır.

Hesapların ilişkilendirilmesi

Kullanılan her bir hesap, bir çalışana net bir şekilde atanmalıdır. Bu, sadece çalışan sorumluluğunu arttırmakla kalmaz aynı zamanda bir saldırı durumunda izlenebilirliği de kolaylaştırır.

Yönetici hesaplarının oturum açma seçeneklerini kısıtlama

Active Directory yöneticilerinin oturum açtığı sistemlerin sayısı mümkün olduğunca sınırlandırılmalıdır. Active Directory yöneticileri yalnızca yönettikleri sistemlerde ve dolaylı olarak da yönetim amacı ile kullandıkları sistemlerde oturum açarlarsa, kimlik bilgilerinin izlenebildiği yerler kısıtlanabilir. Bu nedenle, sunucu yöneticisi hesapları istemcilerde, etki alanı yönetici hesapları da istemci veya sunucularda kullanılmamalıdır. Ayrıcalıklı bir hesabın, başka bir katmandaki bir sisteme giriş yapmak için kullanılmasına teknik olarak da imkân verilmemesi önerilir.

Etki alanı fonksiyon seviyesi 2012'den bu yana, grup ilkesi aracılığı ile bir katmandan diğerine etkileşimli oturum açılması engellenebilmektedir. Bu durum, bir etki alanı yöneticisinin bir üretim veya ofis BT sisteminde oturum açamamasını sağlar. Bir sunucu yöneticisi de, bir etki alanı denetleyicisinde veya ofis BT sisteminde oturum açamamalıdır.

Active Directory servis ve veri yönetimi

Bir etki alanını yönetmek için sorumluluklar ve görev alanları, ek alt gruplara ayrılır. Yönetim gruplarında yer alan kullanıcı hesapları; servis yöneticileri (dizin hizmetini

yönetmek için gereken görevleri gerçekleştirmekle sorumludur) ve veri yöneticileri (Active Directory'de depolanan veya Active Directory tarafından korunan verinin yönetilmesinden sorumludur), geniş kapsamlı erişim yetkilerine sahip olduklarından dolayı, bu hesapları korumak için özel önlemler alınmalıdır.

Servis yöneticisi hesapları

Orman yapısı içerisindeki her etki alanının kurulumu sırasında, varsayılan yönetici hesabı oluşturulur. Bu hesap, varsayılan bir hesap türü olduğundan, saldırılara özellikle açıktır. Yönetici hesabı devre dışı bırakılamadığından veya silinemediğinden, bir koruma tedbiri olarak yeniden adlandırılmalıdır. Hesap yeniden adlandırırken, hesabın açıklamasının da değiştirildiğinden emin olunmalıdır. Hesap yeniden adlandırıldıktan sonra, ayrıcalıklı herhangi bir yetkiye sahip olmayan "Administrator" adlı bir hesabın oluşturulması ve bu hesabın da günlük işlemlerde kullanılmaması önerilir. Günlük olay kayıtlarının analizi yapılırken, ayrıcalıklı olmayan “administrator” adlı kullanıcı hesabı ile başarılı veya başarısız girişlerin olup olmadığı fark edilebilir.

Servis ve veri yöneticilerinin sayısı, asgari düzeyde tutulmalıdır. Etki alanı kullanıcılarının yönetimi gibi Active Directory'nin yapılandırmasını etkilemeyen rutin yönetim faaliyetlerinin, servis yöneticileri tarafından gerçekleştirilmemesi, bu tarz faaliyetlerin veri yöneticilerine devredilmesi önerilir.

Yönetici hesapları mümkün olduğunca az kullanılmalıdır. Etki alanında, yönetici yetkileri ile gereksiz oturum açma eğiliminden kaçınılmalıdır. Bu nedenle kurumun sistem yöneticilerinin; günlük, yönetim amaçlı olmayan (ör. İnternet’ten bilgi edinme gibi) faaliyetlerini, ayrıcalıklı olmayan kullanıcı hesaplarını kullanarak gerçekleştirmeleri tavsiye edilir.

Servis yöneticisi hesaplarının yönetimi, yalnızca servis yöneticisi grubunun üyeleri tarafından gerçekleştirilebilir. Özellikle, daha az ayrıcalıklara sahip kullanıcılar (ör. veri yöneticileri), servis yönetici hesaplarında değişiklik yapamazlar. Çünkü bu durumda daha az ayrıcalıklı kullanıcılara genişletilmiş ayrıcalıklar sağlanabilir.

Bu nedenle, servis yöneticisi hesaplarını yönetmek için, örneğin “Servis yöneticileri” isminde, özel bir OU yapısı oluşturulması ve servis yönetici gruplarının (Domain Admins, Enterprise Admins ve Schema Admins), oluşturulan bu yeni OU yapısına taşınması önerilir. Bu OU için yetkilendirmeler aşağıdaki gibi yapılandırılmalıdır:

- Üst nesne izinlerinin miras alınmasının devre dışı bırakılması
- Erişim izinleri (alt nesneler dâhil)
    - Administrators: Full Control

- Enterprise Admins: Full Control
- Domain Admins: Full Control

Ayrıca, etki alanı yöneticilerinin yönetimsel kullanıcı hesapları, yeni OU yapısı altında oluşturulan örnek olarak “Kullanıcı ve Gruplar” OU’suna, yönetim amaçlı kullanılan bilgisayar hesapları ise yine örnek olarak, yeni oluşturulan “Yönetim İstemcileri” OU’suna taşınmalıdır. Etki alanı denetleyicisi hesaplarının taşınmaması gerektiği unutulmamalıdır.

Ayrıca, servis yönetici hesaplarının ve bilgisayar nesnelerinin değiştirilmesi, silinmesi ve oluşturulması ile ilgili politika değişikliklerinin kayıt altına alındığının izlenmesi gereklidir.

Kurulumla birlikte gelen önceden tanımlanmış hizmet yöneticisi hesaplarından bazıları, yeni oluşturulan OU yapısına taşınamadığından, bu hesapların ayrıca korunması gerekir.

Yerel yönetim hesapları

Yerel yönetim hesaplarının, birbirinden farklı ve güçlü parolalara sahip olmaları önerilir. Microsoft Firmasının ücretsiz olarak sağladığı Yerel Yönetici Parolası Çözümü (LAPS), bu parolaların otomatik olarak oluşturulması ve yönetilmesine olanak sağlamaktadır.

AdminSDHolder nesnesi

“CN=AdminSDHolder,CN=System,DC=<domain_component>,DC=<domain_component>” dizininde yer alan AdminSDHolder nesnesinin amacı, etki alanındaki korunan hesap ve gruplar için bir izinler şablonu sunmaktır. Active Directory içerisinde yer alan diğer nesnelerden farklı olarak bu nesnenin sahipliği “Domain Admins” grubuna atanmıştır.

Active Directory, korunan yönetici hesaplarının düzenli olarak kontrol edildiği bir mekanizmaya sahiptir.. Bu mekanizma, PDC emulator rolüne sahip olan etki alanı denetleyicisi üzerinde, varsayılan olarak her 60 dakikada bir çalışan SDProp işlemi sayesinde gerçekleşir. Bu işlem, AdminSDHolder nesnesinde tanımlanan yetkiler ile etki alanındaki korunan grup ve kullanıcılara atanan yetkileri karşılaştırır ve eğer farklılık tespit eder ise yetkileri, varsayılan AdminSDHolder nesnesinde tanımlanan yetkilere döndürür.

Bu mekanizma, “Administrators”, “Domain Admins”, “Enterprise Admins” ve “Schema Admins” ile "Server Operators", "Account Operators", "Backup Operators", "Print Operators" korumalı grupları için çalışır.

Personel

Servis yöneticisi gruplarında yer alan kişilerin, Active Directory yönetimi hakkında yeterli bilgiye sahip olmaları gerekir. Servis yöneticileri, kurumun güvenlik politikalarının doğru bir şekilde uygulanması için ilgili politika ve kavramlara da aşina olmalıdırlar.

Servis yöneticisi gruplarının üyeleri yalnızca kendi Active Directory orman yapısı kullanıcılarından oluşabilir. Uzak etki alanlarında (farklı kurumlarda) bulunan servis yöneticilerine güvenilmesi, durumunda, kurum otomatik olarak uzak etki alanının (farklı kurumun) güvenlik önlemlerine güvenir hale gelir. Bu güvenlik önlemlerine müdahale etmek genellikle mümkün olmayacağından, kurum dışı kullanıcılar için, kendi orman yapılarında yeni bir kullanıcı hesabı oluşturulması önerilir. Bu şekilde, kurumun etki alanlarına erişim yetkileri daha rahat düzenlenebilir ve kurum dışı kullanıcıların, otomatik güven ilişkisi nedeniyle kazanmış olabilecekleri mahiyeti bilinmeyen erişim yetkileri engellenebilir.

Geniş kapsamlı izinleri nedeniyle, servis yöneticisi hesapları saldırı için özellikle tercih edilen hedeflerdir. Güvenlik gereksinimleri nedeni ile tüm servis yöneticisi gruplarının üyelik bilgilerine erişimin, ayrıcalıklı olmayan kullanıcılar için engellenmesi önerilir.

Ancak, bazı sunucu uygulamalarının sorunsuz çalışabilmeleri için servis yöneticisi gruplarının üyelik bilgilerini okuma yetkisine ihtiyaç duydukları bilinmelidir. Bu nedenle yapılması gereken, kurumda bu tarz sunucu uygulamalarının kullanılıp kullanılmadığını belirlemektir. Sunucu işlemlerini başlatan kullanıcı hesapları, özellikle bu amaca yönelik olarak oluşturulacak gruba üye edilmelidir (ör. “sunucu uygulamaları” grubu).

Active Directory “Backup Operators” grubunun üyeleri, etki alanı denetleyicisi sistem dosyalarını geri yükleyebildikleri için, servis yöneticileri olarak kabul edilmelidir. Bu kullanıcı gruplarının üye sayısı da mümkün olduğunca az tutulmalıdır. Bu nedenle, Active Directory içerisindeki uygulama sunucularının yedekleme ve yedekten geri yükleme işlemlerinden sorumlu olan yöneticilere, Active Directory “Backup Operators” grubunda yer verilmemelidir. Bunun yerine, ilgili kullanıcı hesapları, uygulama sunucusunun "Backup Operators" yerel gruplarına üye edilmelidir.

Active Directory “Account Operators” grubu, veri yönetimi (hesap yönetimi için olduğu gibi) için kullanılmamalıdır. Çünkü böyle bir durumda, grup üyeleri kendi haklarını genişletme imkânına sahip hale gelirler. Güvenlik çekincesi nedeniyle, “Account Operators” grubunda herhangi bir üyenin yer almaması önerilir.

Aynı durum, Active Directory "Schema Admins" grubu için de geçerlidir. Active Directory şemasındaki değişiklikler nadiren yapıldığından, güvenilir yöneticiler yalnızca gerekli olduğu zaman “Schema Admins” grubuna eklenmelidir. Şema değişiklikleri yapıldıktan hemen sonra, üyelerin tekrar gruptan çıkarılmaları tavsiye edilir.

Bir kurumun Active Directory orman yapısının kök etki alanındaki “Domain Admins” ile “Enterprise Admins” gruplarında yer alan kullanıcı hesapları, geniş ayrıcalıklarından dolayı özel olarak korunmalıdır. Bu nedenle, bu hesapların her birine iki yönetici atanması ve

şifrenin ikiye bölünmesi düşünülebilir. İki yöneticinin her biri şifrenin sadece bir yarısını bilebilir, böylece ilgili kullanıcı hesabı ile gerçekleştirilecek olan işlem, ancak iki yöneticinin bir araya gelmesi yoluyla gerçekleştirilebilir. Bu şekilde bir kullanım, Active Directory ormanında kök etki alanı servis yöneticisi hesaplarının kontrol dışı kullanımının önlenmesine yardımcı olur.

İki yöneticinin bir araya gelerek hesabın kullanım prensibinin alternatifi olarak, akıllı kartların kullanımı (PIN ve akıllı kartın ayrı ayrı yöneticilere verilmesi) da düşünülebilir.

Servis ve veri yönetici hesaplarının korunmasına ek olarak, yöneticilerin yönetim amaçlı kullandıkları sistemler de aşağıdaki şekilde güvence altına alınmalıdır:

- Yöneticilerin kullanıcı hesapları, yalnızca belirli sistemlerde oturum açabilecek şekilde yapılandırılmalıdır. Bu yöntem, ele geçirilen yönetici hesaplarının yalnızca sınırlı sistemlerde kullanılabilmesini sağlar.
- Kullanıcı tarafından belirli süre işlem yapılmadığında, otomatik ekran kilitleme etkinleştirilmelidir. Ekran kilidini kaldırmak için önbelleğe alınmış verinin kullanılamaması, kullanıcının kimlik doğrulamasını yeniden etki alanı denetleyicisi aracılığı ile gerçekleştirmesi, zorunlu hale getirilmelidir. Bunun gerçekleştirilebilmesi için HKLM \ Software \ Microsoft \ WindowsNT \ CurrentVersion \ Winlogon \ dizinindeki “ForceUnlockLogon” kayıt defteri anahtarının değeri "1" olarak yapılandırılmalıdır.
- Yöneticilerin istemcilerinde ve kullandıkları yönetim amaçlı sistemlerde, virüs koruma yazılımları kullanılmalıdır.
- Uygulamalar, yönetici hesabı yetkisi ile çalıştırılmamalıdır. Etki alanına yeni bir istemci/sunucu eklenirken, ilgili istemci/sunucunun yerel “Administrators” grubuna etki alanı “Domain Admins” grubunun otomatik olarak eklenmediğinden emin olunmalıdır.
- İşlemlerin, ”Domain Admins” izinleriyle çalıştırılmaması önerilir. Bunun yerine, gerekli olduğu durumda, istemcinin/sunucunun yerel yönetici grubu yetkileri kullanılmalıdır.
- Yöneticilerin istemcileri ve kullandıkları yönetim sistemleri ile etki alanı denetleyicileri arasındaki veri trafiği korunmalıdır. Bu amaçla LDAP istemci imzalama özelliği etkinleştirilebilir. Bunun gerçekleştirilebilmesi için HKLM \ System \ CurrentControlSet \ Services \ LDAP \ içinde “LDAPClientIntegrity” kayıt defteri anahtarının değeri "2" olarak yapılandırılmalıdır.

Etki alanı denetleyicilerinin uzaktan yönetiminde, yalnızca trafiğin şifrelenmesini sağlayan protokoller kullanılmalıdır.

Veri yöneticisi hesapları

Temel olarak, veri yöneticisi hesaplarının yapıları ve yetkileri, büyük ölçüde ilgili kurumun yapısına bağlıdır. Bu nedenle, aşağıda bahsi geçen hususların, kurumun gereksinimleri ile uyumlu hale getirilip getirilmediği teyit edilmelidir.

Veri yönetimi, uygun kullanıcı haklarının atandığı gruplar kullanılarak delege edilir. Grup ilkesi ayarları bu gruplara uygulanır. Bu adımlardan sonra, yetkilendirilme amaçlı oluşturulmuş gruplara, kullanıcı hesaplarını eklemek yeterlidir. Bu yöntem, maksimum güvenlik sağlar ve yöneticilerin kendilerine atanmış görevleri gerçekleştirmelerine olanak tanır.

Grup ilkelerini oluşturma ve değiştirme yetkisi verilen kullanıcılar, diğer kullanıcı hesaplarına yüksek ayrıcalıklar verebilirler. Bu nedenle Grup ilkelerine erişim, güvenilir kişilerle sınırlandırılmalıdır.

Veri yöneticileri, oluşturdukları nesnenin sahibi yetkisine de haiz olurlar. Windows Sunucu erişim denetimi modelinde, bir nesnenin sahibi, nesne üzerinde (ve o nesnenin tüm alt nesneleri üzerinde) tam erişim yetkisine sahiptir. Söz konusu kişi, nesnenin erişim kontrol listesini (ACL) değiştirme, ACL üst nesnelerden miras kalıtımını engelleme ve servis yöneticilerinin bu nesneye erişimini engelleme gibi yetkilere de sahiptir.

Her etki alanındaki “Administrators” ve “Domain Admins” gruplarının, etki alanı kök nesnesinin de sahibi olduğunun farkında olmak gerekir. Bu kök nesnelerin sahipleri, söz konusu bölümdeki diğer tüm nesnelerin (kök nesnenin tüm alt nesnelerinin) güvenlik ayarlarını değiştirebilirler.

Hesap yönetimi faaliyetlerini planlarken, sorumluluk kapsamındaki grup üyeliği değişimlerinin tek bir veri yöneticisi tarafından gerçekleştirildiğinden emin olunmalı veya bu faaliyet, birden fazla veri yöneticisi tarafından gerçekleştirilecek ise, işlemin koordineli bir şekilde yürütülmesi sağlanmalıdır. Eğer iki farklı etki alanı denetleyicisi, replikasyon esnasında grup üyeliğinde gerçekleştirilen eşzamanlı iki değişiklik arasında bir çakışma tespit eder ise, hesaba ilişkin en son gerçekleştirilen değişiklik, önceliğe sahiptir. Replikasyon tamamlanana kadar ise, o sunucuda ilgili hesaba dair yapılan değişiklik geçerli olur.

Geri dönüşüm kutusu

Yanlışlıkla veya bilinçli bir şekilde silinmiş olan Active Directory nesnelerinin daha sonra ihtiyaç duyulduğunda geri getirilebilmesi, Windows Sunucu 2008’e kadar ancak yedekten

geri yükleme ile mümkün olabiliyor idi. Windows Sunucu 2008 R2 ile birlikte, Active Directory için “Geri Dönüşüm Kutusu” özelliği getirilmiştir. Başlangıçta sadece komut satırından çalıştırılabilen bu özellik, Windows Sunucu 2012 ile birlikte, hem PowerShell üzerinden hem de GUI aracılığıyla çalıştırılabilecek bir hale getirilmiş ve kullanımı gayet kolay ve pratik bir geri dönüşüm kutusu yapısı kullanıma sunulmuştur.

Geri Dönüşüm Kutusu özelliği, varsayılan olarak devre dışıdır. Silinen AD nesnelerinin geri döndürülebilmesi amacı ile etkinleştirilmelidir. Etkinleştirildiğinde ise özellik, tekrar pasif hale getirilemez. Özelliğin etkinleştirilmesi, en az Windows Sunucu 2008 R2 etki alanı fonksiyonel seviyesini gerektirdiğinden, tüm orman etki alanı denetleyicilerinin en azından bu düzeyde olması gerekir. Geri dönüşüm kutusu etkinleştirildiğinde, etki alanı fonksiyonel seviyesi eski haline geri döndürülemez, bu nedenle ilk etkinleştirme öncesinde kapsamlı bir planlama yapmak gerekir. Active Directory'deki tüm değişiklikler gibi bu değişiklik de, öncelikle bir test ortamında test edilmelidir.

Etkinleştirme işlemi, ADAC (AD Administrative Center) aracı ile ve ”Enterprise Admin” veya ”Schema Admin” yetkisi ile gerçekleştirilebilir. Daha sonra, etkinleştirme işleminin başarılı olup olmadığını kontrol etmek için ADAC ekranı yeniden yüklenmelidir. Silinen nesnelerin geri getirilebilmesi için gerçekleştirilen bu değişim orman yapısı içerisinde replike edilmelidir.

Kurumsal kimlik yönetimi

Özellikle büyük kurumlarda, tüm kullanıcı haklarının, tanımlanmış standartlara uygun olmasını sağlamak için, bu amaca yönelik bir kurumsal kimlik yönetimi çözümü kullanılabilir.

2.2 2. SEVİYE UYGULAMALAR

1.seviye gereksinimler sonrasında, Active Directory kullanımını daha güvenli bir seviyeye getirmeyi hedefleyen kurum ve organizasyonlar aşağıdaki gereksinimleri dikkate alarak, iyileştirme/geliştirme faaliyetlerini gerçekleştirebilirler.

UYG.2.2.U8 Windows ortamında güvenli kanal yapılandırması

Etki alanı denetleyicileri, birbirleri arasında yönetimsel verileri iletirler. Genel olarak, bu iletişim hassas veriler içerdiğinden veri güvenli bir şekilde iletilmelidir. Bu amaçla, Windows NT zamanlarından beri yer alan, Windows 2000 ve sonraki sürümlerde de kullanılabilir durumda bulunan “Güvenli Kanal” mekanizmasından yararlanılabilir. Yapılandırma, güvenlik gereksinimleri ile yerel koşullara göre özelleştirilebilir. Güvenlik mekanizmaları; iletişimi gerçekleştirecek her iki taraf için kimlik doğrulaması, gizliliği sağlamak için şifreleme ve bütünlüğü sağlamak için imzaları kullanılır.

Güvenli kanal yapılandırması, grup ilkeleri aracılığıyla gerçekleştirilir. Windows Sunucu için (Windows XP'den bu yana istemciler de dâhil olmak üzere) ilgili ayarlar şunlardır:

- Etki alanı üyesi: Güvenli kanal verilerini dijital olarak imzala (mümkün ise)
- Etki alanı üyesi: Güvenli kanal verilerini dijital olarak şifrele (mümkün ise)
- Etki alanı üyesi: Güvenli kanal verilerini dijital olarak şifrele veya imzala (her zaman)
- Etki alanı üyesi: Güçlü oturum anahtarı gerekli (Windows 2000 veya sonraki sürümler için 128 bit şifreleme)
- Etki alanı üyesi: Bilgisayar parola değişikliklerini devre dışı bırak
- Etki alanı üyesi: Bilgisayar parolalarının maksimum süresi (varsayılan: 30 gün, normal şartlarda daha büyük değerler atanmamalıdır)

Bu parametreler: Bilgisayar Ayarları | Windows Ayarları | Güvenlik Ayarları | Yerel Politikalar | Güvenlik Seçenekleri altında bulunabilir.

İlgili grup ilkeleri yapılandırırken, aşağıdaki hususlar göz önünde bulundurulmalıdır:

- Karşılıklı kimlik doğrulaması her zaman garanti edilirken, şifreleme ve imza mümkün ise talep edilebilir. İletişimi gerçekleştirecek taraflardan bir tanesi, talep edilen koruma metodunu desteklemiyorsa, metot kullanılmaz. Bu durumda iletişim, şifreleme ve/veya imza olmaksızın, güvenli olmayan şekilde gerçekleşir.
- Şifreleme veya imza, iletişim için gerekli bir koşul olarak belirtilebilir. İletişimi gerçekleştirecek taraflardan bir tanesi, koruma metodunu desteklemiyorsa, iletişim isteği engellenir, iletişim gerçekleşmez. Bu durum, istemcilerin bir etki alanına giriş yapamamasına neden olabilir. Bu seçenek, yalnızca bir etki alanındaki tüm BT sistemleri (ve güven ilişkisi kurulan etki alanlarının tüm BT sistemleri) şifreleme ve imzalamayı destekliyorsa etkinleştirilmelidir. Bahsi geçen yöntem ancak, Windows Sunucu 2000 ve üzeri sistemlerin yer aldığı yapılarda uygulanabilir.

UYG.2.2.U9 Active Directory kullanımında kimlik doğrulamanın korunması

Active Directory, ağda yer alan paydaşlar arasında güvenli iletişimin kurulabilmesi için, kimlik doğrulama ve yetkilendirme unsurlarını sağlayan merkezi bir bileşendir. Active Directory kimlik doğrulama güvenlik seviyesini artırmak için, LAN Manager kimlik doğrulaması devre dışı bırakılmalıdır. Buna ek olarak, gerek etki alanı denetleyicilerinin kendi aralarındaki, gerekse etki alanı denetleyicileri ile etki alanına üye bilgisayarlar arasındaki sunucu ileti bloğu (SMB) trafiğinin imzalı hale getirilmesi tavsiye edilir. Ayrıca,

Windows 2000 öncesi sistemlerin erişiminin devre dışı bırakılması ve etki alanı denetleyicilerine anonim erişimin kısıtlanması önerilir.

Kimlik doğrulama

Yüksek düzeyde güvenlik; ancak tüm etki alanı denetleyicilerin, üye sunucuların ve istemcilerin en az NTLMv2 (NT LAN Manager Sürüm 2) kimlik doğrulama protokolünü desteklemeleri ile sağlanabilir. NTLMv2, Windows NT 4.0 SP4'ten itibaren varsayılan olarak kullanılabilir durumdadır. Bu kapsamda, Windows'un daha önceki sürümlerindeki eski kimlik doğrulama protokolleri, daha düşük seviyede güvenlik sağlarlar. Örneğin, LAN Manager Kimlik Doğrulama Protokolünde (LM) hesap parolaları, güvenli olmayan bir LM hash formatında saklanır. Windows NT kimlik doğrulama protokolü NTLM ve NTLMv2 için parolalar NTLM hash formatında saklanır. NTLM hash, kriptografik olarak LM hash formatından daha güçlüdür.

LM ve NTLMv1 kimlik doğrulaması yöntemlerinin kullanımının GPO aracılığıyla yasaklanması önerilir. Eğer bu durum, ağda yer alan eski sistemlerin varlığı sebebi ile hemen gerçekleştirilemiyor ise, NTLMv2'ye geçiş planlanmalıdır (yinelenen saldırılar açısından NTLMv2 de bir takım zayıflıklar içermektedir). Kerberos kimlik doğrulama yöntemine geçiş de kapsama alınarak geçiş için bir son tarihin belirlenmesi önerilmektedir.

Windows Sunucu 2008 R2 veya daha sonraki sürümler, NTLM veya daha eski yöntemler ile gerçekleştirilen ve güvenli olmayan ağ kimlik doğrulamasını saptayabilir ve rapor edebilir, bu özellik sayesinde geçiş planlanması daha rahat yapılabilir.

SMB imzalama

SMB protokolü, Microsoft dosya ve yazıcı sunucusu paylaşımı ve Windows'un uzaktan yönetimi gibi birçok diğer ağ işlemleri için temel oluşturur. SMB protokolü, iletim sırasında SMB paketlerini değiştirebilen ortadaki adam saldırılarını önlemek için, SMB paketlerinin dijital olarak imzalanmasını desteklemektedir.

Bu amaçla: Bilgisayar Ayarları \ Windows Ayarları \ Güvenlik Ayarları \ Yerel İlkeler \ Güvenlik Seçenekleri altında yer alan aşağıdaki dört ayar etkinleştirilmelidir:

- Microsoft Ağ İstemcisi: İletişimi dijital olarak imzala (Her zaman)
- Microsoft Ağ Sunucusu: İletişimi dijital olarak imzala (Her zaman)
- Microsoft Ağ İstemcisi: İletişimi dijital olarak imzala (Sunucu destekliyorsa)
- Microsoft Ağ Sunucusu: İletişimi dijital olarak imzala (İstemci destekliyorsa)

UYG.2.2.U10 Active Directory ortamında DNS'nin güvenli işletimi

Bir Active Directory kurulumu, genellikle farklı dizin bölümlerinde yer alacak birden çok sunucudan oluşur. Active Directory yapısı içerisinde yer alan sunucuların, hem istemci hem de diğer sunucular tarafından bulunabilmesi amacıyla kullanılan alan adı sistemi (DNS), Active Directory yapısının temel bir bileşeni olarak düşünülmelidir.

Active Directory bütünlüğünün ve erişilebilirliğinin sağlanması için DNS sorgularının, ağdaki yetkisiz sistemler tarafından farklı yerlere yönlendirilmediğinden emin olunmalıdır. Windows ortamında DNS verisinin korunması, etki alanı denetleyicilerinde “Active Directory-integrated” DNS bölgelerinin kullanımı ile sağlanabilir. Bu durumda, bölgeye özgü DNS verisi, Active Directory'nin "MicrosoftDNS" kapsayıcısında depolanır. “Active Directory-integrated” DNS bölgeleri için yapılandırma verisi, Windows kayıt defterinde depolanır. Yapılandırma verilerine erişim, yönetim hesaplarıyla sınırlandırılmalıdır.

Aşağıdaki metinde Windows sunucularının, “Active Directory-integrated” DNS bölgelerinin ve dolayısıyla Active Directory’nin güvenli işletimini destekleyen özellikler sunulmaktadır. DNS'in kendisini korumak amaçlı detaylı önlemlerden bu rehberde bahsedilmemiştir.

DNS altyapısının güvenliğini sağlamak için; DNS sunucuları, DNS sunucularında barındırılan DNS verisi ve DNS istemci sorgularına verilen DNS yanıtlarının bütünlüğü korunmalıdır.

Etki alanı denetleyicisinde, önbellekte geçici olarak barındırılan DNS verilerinin bütünlüğünü sağlamak için, DNS sunucusunda verinin kirletilmesinin engellenebilmesi amacıyla, “Secure cache against pollution” seçeneğinin etkinleştirildiğinden emin olunmalıdır. Bu seçenek, önbelleğe yalnızca doğrulanmış DNS kayıtlarının yerleşebilir olmasını sağlar.

DNS erişimi, sadece DNS hizmeti alma şeklinde kısıtlanmalıdır. Örneğin, iki ağ segmenti arasındaki güvenlik ağ geçitlerinde sadece DNS hizmeti erişimine (TCP/UDP port 53) izin verilerek bu durum sağlanabilir. DNS hizmeti, aşağıdaki bileşenler için erişilebilir olmalıdır:

- DNS istemcileri ve istekte bulundukları DNS sunucusu arasında
- Barındırdıkları DNS bölgelerinin birbirlerine transferlerini gerçekleştiren DNS sunucuları arasında
- Belirli DNS bölgelerine dair istemci isteklerini, ilgili DNS bölgelerine delege eden ve bu DNS bölgelerinden sorumlu DNS sunucuları arasında

- DNS sunucuları (istemci isteklerini yönlendiren) ile hiyerarşide daha üst düzeyde bulunan DNS sunucuları arasında

Ayrıca, ağ aktivitelerinin DNS sorgu istekleri özelinde izlenmesi önerilir. DNS sunucusuna yapılan yüksek sayıda ve kısa aralıklı DNS sorgusu istekleri, bir hizmet aksatma amaçlı saldırı (DoS saldırısı) işareti olabilir. Bu durumda saldırgan hızla tespit edilmeli ve uygun karşı önlemler devreye alınmalıdır.

IPsec (Internet Protokolü Güvenliği), DNS trafiğinin gizliliğini, güvenilirliğini ve bütünlüğünü sağlamak için kullanılabilir. Ancak şifreleme veya imzalamanın etkinleştirildiği IPsec kullanımında, ağda oluşacak iletim trafiği artabilir. Bu yüzden IPsec kullanımı öncesinde ağda yeterli kaynağın var olduğu teyit edilmelidir.

DNS verilerinin korunması

Sunucuda DNS verilerini korumak için, aşağıdaki hususlar dikkate alınmalıdır:

- Tüm Windows Sunucu işletim sistemlerinde, DNS hizmeti sunma seçeneği yer alır. Bu hizmetin kullanıldığı durumda DNS sunucusu, yalnızca Active Directory yapısı içerisinde yer alan kimliği doğrulanmış istemcilerinden gelen kayıt isteklerini işlemek üzere yapılandırılmalıdır. Hizmet kullanılmıyor ise devre dışı bırakılmalıdır.
- Eğer üçüncü parti bir DNS sunucusu kullanılıyorsa, sunucunun DNS verisini güvenli ve dinamik olarak güncelleme yöntemini desteklediğinden ve bu yönde yapılandırıldığından emin olmak gerekir.
- Kullanıcıların ilgili “MicrosoftDNS” Active Directory kapsayıcısında yer alan DNS verilerine erişimleri, ACL kullanılarak yalnızca ”Administrators”, “Domain Admins”, “Enterprise Admins” ve “DNS Admins” gruplarının ilgili etki alanı verisine tam yetkileri olacak şekilde yapılandırılmalıdır.
- DNS sunucularının ve dolayısıyla da DNS verilerinin yönetimi, Active Directory'nin yapılandırılması kadar önemlidir. Bu nedenle yönetici yetkilendirmelerinde, servis yöneticisi hesaplarının yetkilendirmeleri için kullanılan süreç işletilmelidir (bkz. UYG.2.2.U2 Active Directory yönetiminin planlanması).
- İkincil DNS bölgesi bilgisi Active Directory içerisinde değil etki alanı denetleyicisinde, metin tabanlı bir dosya formatında depolanır. Mümkünse, her bir DNS sunucusunun yalnızca bir bölgeyi yönettiği ve istemci isteklerinin diğer sorumlu olan ilgili DNS sunucusuna yönlendirildiği bir DNS mimarisi kullanımı önerilir. İlgili veri dosyası, NTFS izinleriyle yetkisiz erişime karşı

korunmalıdır. Yalnızca ”Administrators”, “Domain Admins”, “Enterprise Admins” ve “DNS Admins” grupları, ikincil DNS bölgesi verilerine tam erişim yetkisine sahip olmalıdır.

DNS sunucularının yapılandırılması hakkında ek bilgi Microsoft TechNet'te bulunabilir.

UYG.2.2.U11 Active Directory altyapısını izleme

Active Directory altyapısının güvenlik durumu, sistem olayları günlüğe kaydedilerek izlenir ve değerlendirilir. Kaydedilen olaylara ilişkin detay seviyesinin, ilgili gerekliliklere göre uyarlanması ve kayıtların düzenli olarak gözden geçirilmesi önerilir.

Olay günlükleri düzenli olarak değerlendirilmelidir. Ek olarak, kaydedilen verinin, daha önce kaydedilen olay günlüklerinden elde edilen referans veriler ile karşılaştırılması da tavsiye edilir.

Active Directory

Oluşturulan günlük verilerinin değerlendirilmesi, veri büyüklüğüne bağlı olarak, manuel veya özel izleme yazılımları yardımıyla yapılabilir. Büyük Active Directory yapılarında, izleme verilerinin tamamen manuel olarak değerlendirilmesi genellikle mümkün değildir.

İzleme işlemlerinin sonuçları, düzenli olarak oluşturulan raporlarda özetlenmeli ve değerlendirilmelidir. Böylece temel güvenlik sorunları erken bir aşamada tespit edilip çözümlenebilir.

Güvenlik uyarıları kayıt sırasında da oluşabilir. Bu durumda kurumun acil durum planında öngörüldüğü üzere, acil durum aksiyonlarının alınması gerekir.

Temel olarak, etki alanı denetleyicisinin veya Active Directory'nin güvenlikle ilişkili yapılandırma parametrelerindeki değişiklikleri tespit edebilmek için iki yöntem kullanılabilir. Bunlardan biri olay bildirimi diğeri ise eğilim (trend) analizidir.

Olay bildirimi için, Active Directory veya etki alanı denetleyicisinde yer alan yapılandırma parametreleri için eşikler veya limitler tanımlanır. Bir yapılandırma parametresi değiştirilir ve tanımlanmış bir eşik veya limit değeri aşılırsa bu olay, işletim sistemi tarafından kayıt altına alınır.

Eğilim (trend) analizi sürecinde ise, tanımlanan sabit parametreler düzenli aralıklarla uzun bir süre boyunca kaydedilir. Bu verilerde tespit edilen aşırı sapmalar, güvenlikle ilişkili olaylara işaret edebilir. Örneğin, disk alanının düzenli olarak gözlemlendiği durumda, disk alanı tüketiminde fark edilen hızlı ve büyük bir artış, etki alanı denetleyicisine karşı gerçekleştirilen bir hizmet engelleme saldırısının (DoS) varlığını işaret edebilir.

Etki alanı denetleyicisindeki durum değişiklikleri

Etki alanı denetleyicilerindeki değişiklikler, Active Directory'nin güvenliğini etkileyebilir. Bu nedenle en azından, etki alanı denetleyicilerinin erişilebilirliği ve etki alanı denetleyicileri tarafından kullanılan sistem kaynakları izlenmelidir.

Etki alanı denetleyicilerinin erişilebilirliği çeşitli şekillerde izlenebilir. Kurumda bir izleme yazılımının bulunması durumunda, söz konusu yazılımın bu amaçla kullanımı düşünülebilir. Alternatif olarak, izleme amaçlı kullanılacak bir istemci bilgisayarından, etki alanı denetleyicilerine düzenli olarak LDAP sorguları gönderilebilir. Bu yöntem sayesinde, etki alanı denetleyicisinin aktif olup olmadığının belirlenmesi ile birlikte, sorgu yanıt süresi parametresi kullanılarak etki alanı denetleyicisinin sistem yükü hakkında da sonuç elde edilmesi mümkün olacaktır.

Etki alanı denetleyicilerinin yeniden başlatılması olaylarının (reboot/retart) izlenebilirliği önem arz eder. Çünkü bir etki alanı denetleyicisinin yetkisiz bir şekilde yeniden başlatılması, bir saldırıya işaret edebilir. Bu sebeple, bir kurumdaki tüm etki alanı denetleyicilerinin sistem olay günlükleri, yetkisiz bir şekilde gerçekleştirilen sistem yeniden başlatmalarının tespiti için incelenmelidir.

Etki alanı denetleyicilerinin doğrudan erişilebilirliğine ek olarak, sistem kaynaklarının kullanımları da izlenmelidir. Sistem kaynaklarının kullanımında gözlemlenen bir değişiklik mutlaka bir saldırı olduğu anlamına gelmez. Bu değişiklik, büyüyen Active Directory yapılarında yanlış yapılandırma veya eski donanımların kullanımı nedeni ile de ortaya çıkabilir.

Kurumdaki tüm etki alanı denetleyicilerinde, alt ve üst sınır değerleri kurum bazında özelleştirilebilmekle birlikte, aşağıdaki unsurların izlenmesi önerilir:

- İşlemci kullanımı yüzdesi (üst sınır: % 80)
- Active Directory veri tabanının yer aldığı diskte boş alan yüzdesi (alt sınır: % 25)
- Kullanılabilir bellek yüzdesi (alt sınır: % 10)
- LDAP bağlantıları için bağlanma süresi (sürenin olağandışı yüksek olması analiz edilmesi gereken bir duruma işaret edebilir)
- Bir saniyedeki başarılı LDAP bağlantılarının sayısı (Kurumdaki LDAP bağlantı sayılarının eğilimine bağlı olarak, LDAP bağlantı sayısındaki olağandışı bir artış analiz edilmesi gereken bir duruma işaret edebilir)

Active Directory'deki değişiklikler

Etki alanı düzeyinde yapılan değişiklikler; genellikle tüm etki alanı denetleyicilerini, etki alanına üye sunucuları, kullanıcıları ve iş istasyonlarını etkiler. Aşağıdaki değişiklikler bu bağlamda değerlendirilebilir:

- Etki alanında “Operations Master” rollerini değiştirme

  “Operations Master” rollerinde yapılan değişiklikler tüm etki alanını etkiler. Etki alanında yer alan “Operations Master” rolleri: “RID Master, PDC Emulator ve Infrastructure Master” rolleridir. Örneğin PDC Emulator rolünde yapılacak yanlış bir yapılandırmanın, tüm etki alanının tasarımında ve ağ üzerinde ciddi olumsuz etkileri olacaktır. Bu sebeple, herhangi bir “Operations Master” rolünde gerçekleştirilecek olan değişiklik öncesinde, dikkatli bir planlama yapılması gerekir.

- Güven İlişkilerinde yapılan değişiklikler

  Güven ilişkileri, bir kurumun farklı etki alanları arasında kurulabilir. Güven ilişkilerinde meydana gelen değişikliklerin (özellikle yeni güven ilişkilerinin eklenmesi) izlenmesi, güven ilişkisinden doğabilecek gereğinden fazla hakların oluşması durumunun mümkün olan en kısa sürede tespit edilebilmesi açısından gereklidir.

- AdminSDHolder nesnesindeki değişiklikler

  AdminSDHolder nesnesi PDC Emulator tarafından, servis yöneticisi gruplarına üye kullanıcıları ve servis yöneticisi gruplarını, izinlere dair yapılan yetkisiz değişikliklerden korumak için kullanılır. Bu amaçla PDC Emulator, yukarıda belirtilen hesapların sistem yöneticisi tarafından tanımlanan yetkilerinin, AdminSDHolder nesnesinde tanımlı yetkiler ile eşleşip eşleşmediğini kontrol eder. Yetkilerin birbirinden farklı olması durumunda, ilgili hesapların yetkileri, AdminSDHolder nesnesinde tanımlı ayarlara döndürülür.

- GPO'larda ve GPO ilişkilendirmelerinde yapılan değişiklikler

  GPO'larda yapılan bazı değişiklikler (ör. kullanıcı parola politikası), tüm etki alanını ve söz konusu etki alanındaki tüm etki alanı denetleyicilerini etkileyebilir, bu yüzden izlenmelidir. Buna ek olarak, etki alanı ve etki alanı denetleyicilerinin yer aldığı OU ile direkt ilişkilendirilen GPO’lar da izlenmelidir.

- Önceden tanımlanmış servis yöneticisi grup üyeliklerindeki değişiklikler

  “Administrators” veya “Backup Operators” gibi önceden tanımlanmış servis yöneticisi gruplarında yetkisiz bir şekilde gerçekleştirilen kullanıcı ekleme veya

kullanıcı silme işlemleri bir saldırıya işaret edebilir. Bu nedenle, servis yöneticisi gruplarının üyeliklerinde yapılan değişiklikler izlenmelidir.

- Ayrıcalıklı grup üyeliklerindeki değişikliklerin izlenmesi

  Active Directory yönetim haklarına sahip grupların (özellikle bu gruplara yeni üyeler eklendiğinde) düzenli olarak gözden geçirilip, değerlendirilmesi gerekir. Ayrıcalıklı gruba bir hesap eklemeden önce resmi bir onay mekanizması işletilmesi daha etkin bir yöntem olarak önerilmektedir (bu yöntem teknik veya organizasyonel bağlamda uygulanabilir). Bu yöntem ile onayı verilen kullanıcılar üyelik süreleri sona erdiğinde, ilgili gruplardan çıkarılabilir.

- Etki alanı izleme politikalarının değiştirilmesi

  İzleme politikalarında yapılacak bir değişiklik, izleme sürecini olumsuz etkileyebilir, hatta tamamen devre dışı bırakabilir. İzleme sürecinde yaşanacak olumsuzlukları tespit edebilmek için izlemeye dair politikalar üzerinde gerçekleştirilen değişiklikler de izlenmelidir.

Yapılan değişikliklerin kurumun tüm Active Directory ağaç yapısını etkileyebileceği unutulmamalıdır. Bu kapsamda ele alınabilecek değişiklikler:

- Etki alanı denetleyicisi sınıflandırmasındaki değişiklikler

  Etki alanı denetleyicisi rolü yüklenmesi veya bu rolün geri alınması, etki alanı denetleyicisi sınıflandırmasında gerçekleştirilen bir değişikliktir.

- Active Directory şema değişiklikleri

  Active Directory içinde yer alan nesne sınıfları veya nesne özniteliklerinde yapılan değişiklikler yoluyla, dizin hizmeti veri tabanı yapısının değiştirilmesi Active Directory şemasını değiştirir.

- LDAP politikası değişiklikleri

  LDAP politikaları, LDAP isteklerini, dolayısıyla Active Directory verilerine LDAP erişimini kısıtlamak için kullanılabilir.

- Replikasyon topolojisindeki değişiklikler

  Replikasyon topolojisi değişiklikleri; Active Directory “site”, “site link” ve “subnet” nesnelerinin oluşturulması, silinmesi ve değiştirilmesini içerir.

- DS-Heuristic özniteliğinin değiştirilmesi

Active Directory'deki DS-Heuristic özniteliği, Active Directory ormanının tümünde yer alan etki alanları ve Active Directory etki alanı denetleyicilerinin davranışlarında (kullanıcı parola özniteliğinin davranışı, AdminSDHolder nesnesi aracılığı ile korunan gruplar, görünürlük modu, vb. gibi) genel değişiklikler yapmak için kullanılabilir.

- Orman düzeyindeki FSMO rollerinde yapılan değişiklikler

  ”Schema Master” ve “Domain Naming Master” rollerinde yapılan değişiklikler, orman düzeyindeki FSMO rollerinde yapılan değişikliklerdir.

Yukarıda belirtilen etki alanı ve tüm orman düzeyi bazında gerçekleşebilecek değişikliklerin, bir kurumdaki tüm etki alanı denetleyicilerinde izlenmesi ve değerlendirilmesi gerekir. Bir etki alanı denetleyicisinin güvenlik izleme günlüklerinin değerlendirilmesi sırasında, yetkisiz şekilde gerçekleştirilen bir değişiklik tespit edilmesi durumunda önceden detayları planlanmış olan ilgili acil durum planları devreye alınmalıdır.

Bazı olaylarda günlük dosyaları, hangi nesnelerin veya özniteliklerin değiştiğini göstermez. Bu nedenle, Active Directory şemasının dokümante edilmesi gerekir. Böylece istendiğinde, şema üzerinde yetkisiz biçimde gerçekleştirilen değişiklikler saptanabilir ve gerekirse daha sonra referans şema ile mukayese edilerek manuel yapılandırma ile değişiklik geri döndürülebilir.

Active Directory'de yetkisiz olarak gerçekleştirilen değişiklikler tam olarak geri alınamamış ise, orman yapısını tamamen geri yükleme seçeneği düşünülebilir.

Servis yöneticileri grubunda yer alan kullanıcı hesaplarının oluşturulması, silinmesi ve değiştirilmesi; yönetim amaçlı kullanılan iş istasyonlarının eklenmesi veya silinmesi izlenmelidir.

Active Directory veri tabanının yer aldığı etki alanı denetleyicisindeki disk alanı dolduğunda, Active Directory'de yeni nesneler oluşturulamaz. Bu nedenle, Active Directory nesneleri tarafından kullanılan disk alanının sürekli olarak izlenmesi önerilir.

Bu tür bir izleme ile sadece Active Directory veri tabanı için disk alanının azalma durumu gözlenmez, aynı zamanda disk alanı kullanımının kısa bir sürede önemli ölçüde artmasına sebep olan saldırılar da tespit edilebilir. Bu tarz saldırılara hızlı müdahale için, etki alanı denetleyicilerinde herhangi bir boyutta rezerv dosyası oluşturulabilir. Saldırı durumunda, etki alanı denetleyicilerinde oluşturulmuş olan bu rezerv dosyası silinerek, geçici süre ile bir boş disk alanı açıp normal çalışma sağlanabilir. Daha sonra saldırı sebebiyle Active Directory'de oluşan nesneler tespit edilmeli ve silinmelidir.

Kritik dosyalardaki değişiklikler

Hem etki alanı denetleyicileri, hem de yönetim amaçlı kullanılan iş istasyonlarında yer alan kritik dosyalardaki değişiklikler izlenmelidir. Asgari seviyede, işletim sistemi yapılandırma dosyaları ile uygulamaların kullandıkları dosyaların izlenmesi önerilir. Ayrıca, yönetici iş istasyonlarındaki yönetim araçları gibi uygulamaların kullandıkları kritik dosyaların da değişiklikler açısından izlenmesi tavsiye edilir.

Sistem konfigürasyonunu izlemek için ilk adım, uygun bir izleme aracının seçimidir. Daha sonra, izlenecek işletim sistemleri için güvenilir bir referans konfigürasyonun oluşturulması tavsiye edilir.

İzleme yazılımında bu referans konfigürasyonun bir şablonu oluşturulur ve bu şablon, gelecekteki izleme işlemleri için temel olarak kullanılacak şekilde saklanır. Etki alanı denetleyicilerinin veya yönetici iş istasyonlarının mevcut durumdaki konfigürasyonlarının, referans konfigürasyona göre değişip değişmediği, düzenli aralıklarla kontrol edilmelidir. Tespit edilen sapmalar incelenmeli, sapmanın yetkisiz bir şekilde gerçekleştirilen bir değişiklik nedeniyle meydana geldiği anlaşılırsa, sistem, orijinal durumuna mümkün olan en kısa sürede geri döndürülmelidir.

UYG.2.2.U12 Etki alanı denetleyicilerinin yedeklerinin alınması

Etki alanı denetleyicileri, ağda yer alan önemli kaynaklara erişim için merkezi bir kimlik doğrulama ve yetkilendirme imkânı sağlamaktadır, bu yüzden etki alanı denetleyicisinin hizmet verememe durumu, ciddi sorunlara yol açabilir. Bu nedenle, merkezi BT bileşenleri olan etki alanı denetleyicileri için uygun bir veri yedekleme prosedürü oluşturulmalıdır. Buna ek olarak, Active Directory için veri yedekleme politikası geliştirilirken, etki alanı denetleyicisine özgü özellikler de göz önünde bulundurulmalıdır. Veri yedekleme politikası hazırlanırken, aşağıdaki hususların dikkate alınması önerilir:

- Etki alanı denetleyicileri düzenli ve izlenebilir bir şekilde yedeklenmelidir.
- Yedekleme için özel kullanıcı hesaplarının kullanılması önerilir.
- Yedekleme sistemleri, sadece donanım ve ilgili medyanın güvenliğinin garanti edildiği yerlerde işletilmelidir.
- Alınan yedeklerin, etki alanı denetleyicilerine geri yüklenebildiği, periyodik olarak test edilmelidir.
- Elden çıkarılacak yedekleme medyası güvenli bir biçimde imha edilmelidir.

Geleneksel sunucu yedeklemelerine ek olarak etki alanı denetleyicileri için aşağıdaki noktalar da dikkate alınmalıdır:

- Felakete uğrayan bir etki alanı denetleyicisini kurtarma işlemi nadiren, sadece yedeklenen verinin geri yüklenmesi ile gerçekleştirilir. Pratikte felakete uğrayan etki alanı denetleyicisini kurtarmak yerine, etki alanına üye bir sunucuya, etki alanı denetleyicisi rolü yüklenerek ve akabinde Active Directory verisi hali hazırda çalışmakta olan diğer etki alanı denetleyicilerinden bu sunucuya replike edilerek yeni bir etki alanı denetleyicisi oluşturulur. Ancak tabii ki bu yöntem, bir veya birden fazla sistemin felakete uğraması durumunda dahi, Active Directory ortamında en az bir geçerli etki alanı denetleyicisinin var olması durumunda kullanılabilir.
- Eğer etki alanı denetleyicilerinin felaket durumu akabinde ortamda hiç tutarlı bir Active Directory kopyası kalmamışsa, etki alanı denetleyicilerinin kurtarma işlemi, yedekten geri yükleme yöntemi ile yapılmalıdır. Bu durumda, eksik/hatalı yedekleme medyası, eksik kurtarma prosedürleri veya sorumlu kişilerin sürece dair bilgi eksiklikleri gibi nedenlerden dolayı, problemlerin oluşabileceği bilinmelidir. Bu sorunları yaşamamak için, yöneticilerin kurtarma prosedürleri hakkında detaylı bilgiye sahip olmaları gereklidir.

Uygun yedekleme yazılımının seçimi

Yedekleme yazılımı, yedekleyeceği dosyaların metadata verilerini düzgün bir şekilde işlemez ise bu durum, yüksek sayıda dosyanın gereksiz yere replikasyonuna sebep olabilir.

Antivirüs programlarının (bkz. UYG.2.2.U5 Active Directory'nin sıkılaştırılması) seçimine benzer biçimde, etki alanı denetleyicileri için kullanılacak yedekleme yazılımını seçerken, yazılımın etki alanı denetleyicileri için sağlıklı bir şekilde kullanılabileceğine dair yazılım üreticisinden teyit alınması gereklidir.

Özel güvenlik gereksinimleri

Etki alanı denetleyicilerini yedeklemek için kullanılan servis hesabının, servis yöneticisi ayrıcalıklarına ve dolayısıyla yüksek ayrıcalıklara sahip olması gerekir. Bu hakların kötüye kullanılmasını önlemek için bu hesaplara erişimi olan kullanıcı sayısı mümkün olduğunca sınırlı sayıda tutulmalıdır.

Bu nedenle, etki alanı denetleyicilerinde çalışacak yedekleme ajanı için kurumun diğer sunucularında kullanılan servis hesaplarından farklı hesaplar kullanılması önerilir. Etki alanı denetleyicileri ve diğer sunucularda farklı servis hesaplarının kullanımı, kurumun etki

alanı denetleyicisi haricindeki bir sunucunun ele geçirilmesi durumunda etki alanı denetleyicisini korur.

Ayrıca, “Backup Operators” grubunun üyeleri, sistem dosyalarını yedeklemekle görevli olan kullanıcılarla sınırlandırılmalıdır. Uygulama verilerini yedeklemekle sorumlu olan kullanıcılar, etki alanı denetleyicisinde “Backup Operators” grubunun üyesi olmamalıdır. Bu kullanıcılar, ilgili uygulama sunucusunun yerel "Backup Operators" grubunda üye olarak yer almalıdırlar.

Etki alanında yer alan ”Backup Operators” grubu, varsayılan olarak korunmaz. Bu korumayı sağlamak için, ilgili AdminSDHolder nesnesine erişim mümkün olduğunca sıkı bir şekilde kontrol edilmelidir (bkz. UYG.2.2.U7 Active Directory için güvenli yönetim yöntemlerinin uygulanması).

Etki alanı denetleyicilerinin veri yedeklemeleri düzenli aralıklarla gerçekleştirilmelidir. Uygun bir yedekleme aralığı tanımlanırken, silinmesi için işaretlenmiş Active Directory nesnelerinin doğrudan Active Directory'den kaldırılmadığı, önce Active Directory'nin Silinmiş Nesneler ("Deleted Objects") kabına taşındığı dikkate alınmalıdır. Silinmek için işaretlenmiş bu nesneler, eski veya "mezar taşı" nesneleri olarak adlandırılır.

Bu silinen nesneler, ayarlanabilir bir süre (varsayılan olarak 60 gün) sonunda tamamen silinir. Bu yöntem, yanlışlıkla silinen nesnelerin son tarihi gelmediği süre içerisinde yeniden etkinleştirilebilmesi imkânını sunar. Hesap veya nesne, silindiğinde devre dışı bırakılır, böylece artık kullanılamaz. Ancak istenilir ise, hızlı bir şekilde kurtarılabilir.

Yedeklerin replikasyon sorunlarına yol açmaması için, yaşam süreleri aşılmış olan en az sayıdaki eski nesneyi içerdiğine dikkat edilmesi önerilir. Bunun garanti altına alınabilmesi için, düzenli yedek alınırken, eski nesnelerin kullanım ömrünün yaklaşık %75'inden sonra, yedekleme ortamının üzerine yazılması gerekir. Bu yöntem, verinin mümkün olduğunca sık bir şekilde yedeklenmesini ancak yedekleme ortamının 45 gün sonra alınan yeni yedek ile üzerine yazılmasını (yaşam ömrü 60 gün olduğu varsayılan nesne örneğinde) önerir ki bu şekilde eski nesnelerin artık yedekten de geri yüklenememesi sağlanır.

Etki alanı denetleyicisinin yedekleme medyası Active Directory veri tabanındaki tüm bilgileri içerdiğinden, etki alanı denetleyicilerinde uygulanan fiziksel güvenlik önlemleri, yedekleme medyası için de uygulanmalıdır. Özellikle uzak uç şube yedeklemeleri için, yedekleme donanım ve medyasının güvenliğinin yeterli biçimde sağlanıp sağlanmadığı kontrol edilmelidir. Bu hususta aşağıdaki seçenekler mevcuttur:

- Uzak uç şubelerdeki etki alanı denetleyicilerinin yedeğinin alınmaması

- Uzak uç şubelerdeki verinin yedeğinin, güvenli veri merkezlerinde çalışan yedekleme sistemleri aracılığı ile uzaktan yedekleme yöntemi (çevrimdışı ortam) ile alınması
- Uzak uç şubelerdeki verinin yedeğinin, yerel yedekleme sistemleri aracılığı ile yedekleme medyasına (çevrimiçi ortam) alınması

Yedekleme yönetimi, yedekten geri yükleme ve güvenlik ölçütleri açısından bu seçenekler değerlendirilmelidir. Yedekleme yapılıyorsa, yedekleme medyasının mevcut durumu ve işe yararlılığı, düzenli aralıklarla yedekten geri yükleme işlemleri gerçekleştirilerek kontrol edilmelidir.

Kullanılan yedekleme medyası, verilerin değişmesini veya çalınmasını önlemek için güvenli ve izlenen bir yerde saklanmalıdır. Yedekleme medyası (ör. kartuş) sadece yedekleme ve geri yükleme sırasında sürücüye yerleştirilmelidir. Arşivden yedekleme medyası talep edilir iken yetkili yöneticilerin onaylarını gerektiren prosedürler ayrıca oluşturulmalıdır.

Yedeklenecek etki alanı denetleyicilerinin seçimi

Etki alanı denetleyicileri birden çok konuma dağıtılmışsa (uzak uç şubeleri, vb.), yedekleme süreci ve medyasının korunmasını da sağlayacak bir veri koruma çözümünün yapılandırılmasına dikkat edilmelidir. Veri yedekleme politikasının, farklı konumlarda yer alan tüm etki alanı denetleyicileri için uygulanmasını sağlamak önemlidir. Örneğin, uzak uç şubelerden herhangi birinde yedekleme medyasını korumak için güvenli bir depolama imkânı yok ise medya uygun bir lokasyona taşınmalıdır.

Uzak uç şubeler için, yedeklenecek verilerin ağ üzerinden merkezi bir konumda toplandığı çözümler düşünülebilir. Bu tarz bir veri yedekleme çözümü kullanımında aşağıdaki noktalara dikkat edilmelidir:

- Ağ üzerinden iletilen verilerin bütünlüğü ve gizliliği uygun önlemlerle korunmalıdır. (örneğin, yedeklenecek verinin iletim öncesinde veya sırasında şifrelenmesi).
- Ağ üzerinde yeterli bant genişliği bulunmalıdır. Bu sayede uzaktan yedekleme sırasında, yedekleme veya diğer rutin işlemler kesintiye uğramaz.
- Yedekleme önce uzak uç ofislerde yerel olarak gerçekleştirilip, daha sonra yedeklenen veri, merkezi bir konuma toplanır ise erişimin güvence altına alınması gerekir. Örneğin, yedekleme verilerini içeren dosya paylaşımlarına erişimin sadece etki alanı yöneticileri ile kısıtlanması düşünülebilir.

Artımlı yedekleme yöntemi

Disk alanı tasarrufu sağlamak amacı ile sistem dosyalarını yedeklemek için sıklıkla artımlı (incremental) veri yedekleme yöntemi kullanılır. Bu yöntemde, sadece son yedeklemeden bu yana değişen dosyalar yedeklenir. Bununla birlikte, geri yükleme durumunda ise, bu yöntem daha fazla zaman gerektirir. Etki alanı denetleyicileri için artımlı yedekleme yönteminin kullanılmaması önerilir.

Yedekten geri yükleme yöntemleri

Artımlı yedekleme yönteminin kullanıldığı durumda, yalnızca son tam yedeklemeden bu yana yeni oluşturulan veriler yedeklenir, eski güncellemeler dikkate alınmaz. Ancak bazı durumlarda, eski güncelleme durumlarını geri yükleme ve bunları replike ettirme ihtiyacı olabilir. Bu durumdan etkilenen verilere, komut satırından "ntdsutil" aracı kullanılarak replikasyon için öncelik verilebilir. Öncelik verme işlemi, hangi verilerin yedekten geri yükleneceğini veya hangi verilerin olduğu gibi kalacağını belirler. Ancak verilere öncelik verme işlemi, genel yapıda tutarsızlıklara yol açabileceğinden dikkatli bir şekilde yapılmalıdır.

Etki alanı denetleyicilerinin imajlarının alınarak (sanal ortam mimarisinde snapshot kullanılarak) gerekli durumlarda imajın geri yüklenmesinin gerçekleştirilmesi, Active Directory'de tutarsızlıklar oluşturabileceği ve USN (güncelleştirme sıra numarası) geri alma işlemi gerektirebileceği için önerilmemektedir.

Alınan yedeklerin kullanılabilirliği

Alınan yedeklerin acil bir durumda kullanılabilir olduğunu güvence altına almak için, her yedekleme işleminin sonunda, yedeğin hatasız bir şekilde alındığından emin olunmalıdır.

Yedeklerin kullanılabilmesi için aşağıdaki hususların sağlanması gereklidir:

- Düzenli olarak (örneğin her hafta) etki alanı denetleyicilerinin başarılı bir şekilde yedeklendiğinden emin olunmalıdır.
- Oluşturulan yedekleme medyasının, etki alanı denetleyicisinin açık adı ve yedekleme tarihi yer alır şekli ile etiketlendiğinden emin olunmalı ve yedekleme medyası güvenli bir şekilde muhafaza edilmelidir. Etikette, yedeği alınan etki alanı denetleyicisinin rolü bilgisinin de yer alması, gerekli durumlarda yedeğin hangi etki alanı denetleyicisine ait olduğunun saptanması için yardımcı olur.
- Başarısız şekilde sonuçlanan bir yedekleme durumunda, hata en kısa zamanda düzeltilmelidir.

Alınan yedeklerden, geri yüklemenin başarılı bir şekilde yapılıp yapılamadığı düzenli aralıklarla test edilmelidir. Bu testten başarı ile geçen yedekleme medyası, yapılan test bilgisini içerir şekilde işaretlenmelidir. Bu testler, üretim ortamından ayrı izole bir test ortamında gerçekleştirilmelidir.

Yukarıda yer alan uygulama maddelerinde detaylandırılan Active Directory güvenliğini sağlamaya yönelik hususlar aşağıdaki şekilde özetlenebilir:

- Uygulamalar ve işletim sistemleri güncel versiyonları ile kullanılmalıdır.
- Uygulama ve işletim sistemlerinin kullanılan versiyonlarına dair yayınlanan güncellemeler kurum yama güncelleme prosedürüne uygun şekilde, düzenli olarak yüklenmelidir.
- Antivirüs uygulamaları güncelliği takip edilerek kullanılmalı ve ilgili olaylar izlenmelidir.
- Active Directory ve Windows olay kayıtları düzenli olarak takip edilmelidir.
- Kritik verilere erişimi olan kullanıcı hesapları korunmalı ve izlemelidir
- Ayrıcalıklı hesapların güvenli olmayan sistemlerde kullanımı önlenmelidir.
- Ayrıcalıklı gruplarda sürekli üyeliğe izin verilmemelidir. Bu gruplara sadece ihtiyaç duyulduğu zaman ve onay mekanizması işletilerek üye olunabilmelidir.
- Etki alanı denetleyicileri üzerinde çalıştırılabilecek (onaylanmış) uygulamaların listesi hazırlanarak sadece bu uygulamaların çalıştırılmasına izin verilmelidir.
- Sahip olunan varlıklar kritiklik seviyesine göre önceliklendirilmelidir. Bu varlıkların güvenlik sıkılaştırılmaları yapılmalı ve izlenmeleri sağlanmalıdır.
- Etki alanı, destekleyici altyapısı ve etki alanına üye sistemlerin yönetiminde; en az ayrıcalık ilkesi ve rol tabanlı erişim denetimleri yöntemi uygulanmalıdır.
- Eski sürüm/desteği bitmiş uygulamalar tespit edilerek önce izole edilmeli, akabinde devre dışı bırakılmalıdır.
- Yapılandırma yönetimi ve değişiklik yönetimi süreci düzenli şekilde uygulanmalı, her yeni donanım veya yazılım sürümü uyumluluk açısından gözden geçirilmelidir.
- İş sürekliliği ve felaket kurtarma planları yapılarak dokümante edilmeli, düzenli olarak bu planlar test edilmeli ve herhangi bir felaket durumunda pratikte uygulanabilir olmalıdır.

2.3 3. SEVİYE UYGULAMALAR

Aşağıdaki öneriler, standart koruma seviyesinin ötesine geçen ve arttırılmış koruma ihtiyaçları için göz önünde bulundurulması gereken önlemlerdir. Parantez içindeki harfler, önlem özelinde hangi temel değerler için öncelikli koruma sağlandığını gösterir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

UYG.2.2.U13 İki faktörlü kimlik doğrulama (GBE)

Active Directory'deki ayrıcalıklı hesapların, iki faktörlü kimlik doğrulama ile korunmaları önerilir. Bu amaçla akıllı kartlar kullanılabilir. Ancak akıllı kartlar, oturum açma sürecinde NTLM hash kullanmaları sebebiyle, güvenliğin ihlal edilmesine karşı tek başlarına yeterli olmazlar. Doğru yapılandırılmayan bir ortamda hash değerleri saldırganlar tarafından ele geçirilebilir ve "pass-the-hash" saldırısı amacıyla kullanılabilir. Dolayısı ile bu önlemin, AD'nin güvenli yapılandırılması ve sıkılaştırılması önlemleri ile birlikte alınması önerilmektedir.

UYG.2.2.U14 Ayrıcalıklı yönetici sistemleri (GBE)

Active Directory hizmetinin yönetimini yalnızca bu amaç için özel olarak sağlanmış sistemler aracılığı ile gerçekleştirmek mümkündür. Özellikle yönetim görevleri için sıkılaştırılmış bu sistemlere, diğer sistemlerin yönetimsel amaçla erişimleri engellenmiştir. Bu sistemler, özellikle bu görevleri için sıkılaştırılmış sistemlerdir ve diğer tüm sistemlerin bu sistemlere yönetimsel amaçla erişimleri engellenmiştir. Bu sistemler genellikle, PAW (Privileged Access Workstations: Ayrıcalıklı Erişim İş İstasyonları) veya Microsoft iç kaynaklarında SAW (Secure Admin Workstations: Güvenli Yönetici İş İstasyonları) olarak adlandırılır.

Ayrıcalıklı yönetici sistemlerinin sıkılaştırılması için gerekli önlemler aşağıdaki hususları içerir:

- UEFI / TPM / Güvenli Önyükleme / Ölçülen Önyükleme
- BitLocker
- Standart Kullanıcı Yapılandırması
- AppLocker
- USB Ortam Kısıtlamaları
- Device Guard (Windows 10)
- Credential Guard (Windows 10)
- Giden trafik kısıtlamaları (İnternet yok)
- Gelen trafik kısıtlamaları (Varsayılanı engelle)
- Otomatik güncellemeler
- Uç nokta koruması
- Emin olunan güvenli medya oluşturma süreci
- Hızlı oluşturma süreci
- Oturum açma kısıtlamaları

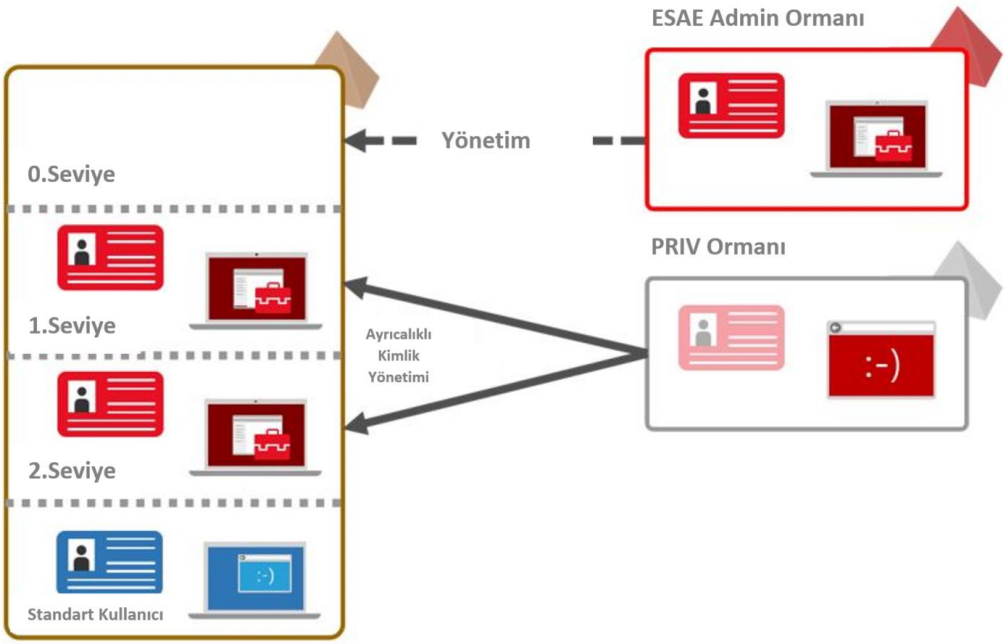
- Microsoft güvenlik uyum yöneticisi (SCM)
- İmzasız kod analizi
- OU ve GPO ACL Kilitlenmeleri
- Sadece yetkili yönetim araçları

UYG.2.2.U15 Yönetim ve canlı ortamın ayrıştırılması (GBE)

Kullanıcı verilerinin bölümlenmesi amacı ile yönetim ortamı için ayrı bir orman yapısı tesis edilebilir. Yönetim ormanı ile kullanıcı verilerinin yer aldığı üretim ormanı arasında tek yönlü bir güven ilişkisi oluşturulur ve üretim ormanı, yönetim ormanına güvenir. Bu mimaride, yönetim ormanı üretim ormanına erişimi denetleyeceğinden, yönetim ormanının güvenliği garanti altına alınmalıdır. Yönetim ormanı, uygulama ve servisleri barındırmamalıdır. Yönetim ormanında yer alıp üretim ormanına ayrıcalıklı haklar ile erişim yetkisi atanan kullanıcıların, yönetim ormanında ayrıcalıklı hesapları olmamalıdır. Bu kullanıcılar tarafından standart hesaplar kullanılmalı ve yönetim ormanına yönetimsel amaçlı erişim, gerekirse manuel bir süreç ile sıkı bir şekilde kontrol edilmelidir. Yönetim ormanı, Microsoft güvenlik uyum yöneticisi ayarları kullanılarak sıkılaştırılabilir. Ayrıca işletim sistemi güncellemeleri, düzenli bir şekilde uygulanmalıdır. Güven ilişkisinde seçici kimlik doğrulama yöntemi kullanılarak, servislerden yararlanabilecek hesapların belirlenmesi ile daha fazla kısıtlama gerçekleştirilebilir.

Microsoft tarafından bu konuda geliştirilen güvenlik modeli, "Gelişmiş Güvenlik Yönetimsel Ortamı (ESAE: Enhanced Security Administrative Environment)" olarak adlandırılmıştır. Bu mimaride yönetimsel hesaplar; istemciler, sunucular ve etki alanı denetleyicileri seviyesinde yönetim amacı ile sınıflandırılmışlardır.

Aşağıda Şekil 3'te görüleceği üzere mimarinin farklı bir şekilde kullanımında ise, Microsoft Kimlik Yöneticisi (MIM) veya Ayrıcalıklı Erişim Yönetimi (PAM) gibi ek yazılımlar kullanılarak üretim ortamına ayrıcalıklı yetkiler ile erişim, bir iş akış süreci ile kontrol edilebilir. Bu mimaride MIM yazılımı, üretim ortamına ayrıcalıklı yetkiler ile erişecek kullanıcıları, sadece erişim süreleri boyunca, yönetim ortamı ormanında oluşturulan ilgili gruplara üye eder.



Şekil 11. Artırılmış Güvenlikli Yönetimsel Ortam Mimarisi

Her kurum, kendi artan güvenlik gereksinimlerine göre, kendi katman kavramını oluşturmalı ve pratikte de uygulanabilirliğini doğrulamalıdır.

Koruyucu katmanların derecelendirilmesi

Etki Alanı Denetleyicileri > Sunucular > İş İstasyonları

Tüm sistemler üç kategoriye ayrılmalıdır:

- Diğer sistemler üzerinde kontrol sahibi olan kritik sistemler (Etki Alanı Denetleyicileri, Sertifika Otoriteleri (CA), vb.)
- Sunucular (BT üretim)
- İş İstasyonları (BT Ofis)

Alt katmanda bulunan sistemler, üst katmanda yer alan herhangi bir sistem üzerinde, kontrol sahibi olmamalıdır.

Efor ve karmaşıklık

Birden fazla orman yapısını kurmak ve işletmek, pek çok sistem ve servisin her bir orman yapısı için ayrı ayrı oluşturulmasını gerektirdiği için, yüksek düzeyde karmaşıklığı ve potansiyel olarak önemli operasyonel maliyetleri beraberinde getirmektedir. Bu durum, yalnızca Active Directory altyapısını değil, aynı zamanda WSUS, antivirüs, yedekleme mimarisi ve istemci gibi diğer altyapı bileşenlerinin de tasarımını ve işletimini etkiler.

3 DETAYLI BİLGİ İÇİN KAYNAKLAR

Active Directory ile ilgili detaylı konulara, aşağıdaki referans ve kaynaklardan ulaşılabilir:

- Active Directory Hizmeti
  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services
- Active Directory Federasyon Hizmetleri
  https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services
- Active Directory'nin Güvenliğini Sağlama
  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
- Active Directory'de Ayrıcalıklı hesaplar ve gruplar
  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b--privileged-accounts-and-groups-in-active-directory
- Active Directory'de ayrıcalıklı erişimin güvenli hale getirilmesi
  https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access
- Active Directory Geri Dönüşüm Kutusu'nu Yapılandırma
  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/introduction-to-active-directory-administrative-center-enhancements--level-100-
- Active Directory Antivirüs taramasına dair öneriler
  https://support.microsoft.com/en-us/help/822158/virus-scanning-recommendations-for-enterprise-computers-that-are-runni

EKLER

EK-A: KONTROL SORULARI

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
UYG.2.2.U1	Active Directory'nin planlanması	Active Directory mimarisi kurum ihtiyaçları da gözetilerek detaylı bir şekilde planlanmış mıdır?
		Etki alanı ve orman fonksiyon seviyeleri nelerdir? Etki alanı ve orman fonksiyon seviyelerinin düşük kalma durumu var ise yükseltme için bir planlama yapılmış mıdır?
		Etki alanı denetleyicileri sanal yapıda mı yoksa fiziksel olarak mı hizmet vermektedir?
		Active Directory site/subnet tasarımı ne şekilde gerçekleştirilmiştir? Uzak uç ofisler var ise onlar için bu kapsamda ne şekilde bir planlama yapılmıştır?
		Active Directory replikasyon mimarisi kurum ihtiyaçlarına göre tasarlanmış mıdır?
		Active Directory OU yapılandırması teknik gereksinimler ve/veya Kurum organizasyonel yapısı dikkate alınarak planlanmış mıdır?
		Güvenlik ve dağıtım gruplarının oluşturulmasına dair bir politika mevcut mudur?
		Etki alanı denetleyicilerinin FSMO rolleri üretici firma önerilerine uygun şekilde konumlandırılmış mıdır? Global katalog rolünün etki alanı denetleyicilerine dağıtımı planlanmış mıdır? Global katalog rolünün hangi nesne özniteliklerini barındıracağı belli midir?
		Planlanan Active Directory yapısı, şema değişikliklerini de içerecek şekilde dokümante edilmiş midir?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
UYG.2.2.U2	Active Directory yönetiminin planlanması	Yönetimsel faaliyetler ve buna dair yetkilendirmeler planlanarak dokümante edilmiş midir?
		Yönetimsel görevlerin devri söz konusu mudur? Devir işlemi ne şekilde gerçekleştirilmektedir? Yönetimi tamamen devredilen bir etki alanı mevcut mudur?
		Rol tabanlı yönetim metodu uygulanmakta mıdır?
UYG.2.2.U3	Grup ilkelerinin planlanması	Active Directory grup ilkelerinin ne şekilde oluşturulacağına dair bir politika/prosedür var mıdır?
		Grup ilkeleri hangi seviyede (etki alanı/etki alanı denetleyicileri/OU/site) uygulanmaktadır?
		Grup ilkesi planlamasında olası birden çok çakışma durumu gözetilerek bu durum engellenmiş midir?
		Grup ilkelerinin uygulanmasındaki istisnai durumlar kolayca gözlenebilecek şekilde bir dokümantayon oluşturulmuş mudur?
		Tüm grup ilkeleri nesnelerine erişimler yetkili kişiler tarafından mı yapılmaktadır?
		Her bir grup ilkesi nesnesindeki parametreler için değer ataması gerçekleştirilmiş midir?
		Logon/logoff veya startup scriptleri içerisinde parola bilgilerini barındıran GPO'ların bulunmadığı teyit edilmekte midir?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
UYG.2.2.U4	Active Directory yönetimi eğitimi	Active Directory sistem yöneticileri yeterli sayıda mıdır? İlgili personel sorumluluk alanı temelinde yedekli midir?
		Active Directory sistem yöneticileri, sorumluluk alanlarına uygun eğitimleri almışlar mıdır?
		Active Directory sistem yöneticileri sorumluluk alanlarına uygun olarak Active Directory güvenlik mekanizmalarına aşina mıdır?
UYG.2.2.U5	Active Directory'nin sıkılaştırılması	Etki alanı denetleyicileri güvenli bir ortamda hizmet etmekte midir?
		Etki alanı denetleyicilerine erişim yetkileri işletim sistemi seviyesinde kısıtlanmış mıdır?
		Etki alanı denetleyicileri “native mode” metodunda hizmet vermekte midir? (Windows 2000 işletim sistemi öncesi işletim sistemleri ile uyumluluk modu pasif midir?)
		Etki alanı denetleyicileri yetkisiz yeniden başlatmalara karşı korunmakta mıdır?
		Active Directory Geri Yükleme modu güçlü bir parola ile korunmakta mıdır? Bu modda yapılacak çalışmanın en az iki kişi tarafından gerçekleştirilme (dört göz) ilkesi uygulanmakta mıdır?
		Kullanıcı hesaplarına yeterince güçlü parolalar atanmakta mıdır?
		“Everyone” grubunun yetkileri sınırlandırılmış mıdır?
		“ADminSDHolder” nesnesine erişim, yetkilendirme yapısının korunması amacı ile kısıtlanmış mıdır?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		Ayrıcalıklı hesaplar için “protected groups” mimarisi kullanılmakta mıdır?
		Servis hesapları için “Group Managed Service Accounts” mimarisi kullanılmakta mıdır?
		Etki alanı ve etki alanı denetleyicileri politikaları; parola, hesap kilitlenmesi, Kerberos kimlik doğrulama, kullanıcı yetkileri ve izleme hususlarında güvenli ayarları içermekte midir?
		Etki alanı denetleyicileri güncel antivirüs uygulamaları ile korunmakta ve ilgili klasörler tarama dışı kalacak şekilde yapılandırılmakta mıdır?
		Bir etki alanı denetleyicisinde sadece Active Directory hizmetini vermeye yönelik servisler çalışmakta mıdır? Dhcp, dosya sunucusu vb. diğer servislerin çalışması engellenmiş midir?
		Etki alanı denetleyicilerinin uzaktan RDP ile erişilerek yönetildiği durumda “Restricted Admin mode” yöntemi kullanılmakta mıdır?
UYG.2.2.U6	Active Directory'nin operasyonel güvenliğini sağlamak	Yetkili hesaplar ve ilgili grupları asgari seviyede tutulmakta ve düzenli olarak denetlenmekte midir?
		Yönetimsel amaçlı kullanılan hesaplara sadece sorumluluk alanlarındaki faaliyetleri sürdürebilecekleri şekilde kısıtlı bir yetkilendirme yapılmakta mıdır?
		Etki alanları ve orman yapıları arasındaki güven ilişkileri kısıtlanmış mıdır? Pratikteki kullanım durumları düzenli olarak sorgulanmakta mıdır?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		Active Directory'de kullanılmayan nesneler düzenli olarak gözden geçirilmekte ve temizlenmekte midir?
		Temel Active Directory bilgileri dokümante edilmiş midir?
UYG.2.2.U7	Active Directory için güvenli yönetim yöntemlerinin uygulanması	Standart ve ayrıcalıklı hesaplar ayrıştırılmış mıdır?
		Active Directory servis yöneticisi ve veri yöneticisi hesapları gerekli olan minimum sayıda ve güvenilen kişiler ile sınırlandırılmış mıdır?
		Standart "Administrator" hesabı yeniden adlandırılmış mıdır? Herhangi bir yetkisi olmayan bir "Administrator" hesabı oluşturulmuş mudur?
		Günlük, yönetimsel olmayan rutin işler, yönetimsel olmayan hesaplar ile mi gerçekleştirilmektedir?
		Servis yöneticisi hesapların yönetimi sadece servis yöneticisi grubu tarafından gerçekleştirilmekte midir?
		Yönetici hesapları gerektiğinde ve süreli olarak mı bu yetkiyi almaktadırlar?
		"Account Operators" ve "Domain Admins" gruplarının içi boş mudur? Varsayılan domain admin hesabı parolası güvenli bir ortamda muhafaza edilmekte midir?
		"Schema Admins" grubuna üye atanması sadece şemada değişiklik yapılacağı zaman ve geçici süre ile mi yapılmaktadır?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		"Enterprise Admins" ve "Domain Admins" üyeliği yetkileri ile kök etki alanında gerçekleştirilecek olan işlemler, en az iki yöneticinin birlikte çalışma prensibine uygun olarak yürütülmekte midir?
		Active Directory Recycle Bin özelliği etkinleştirilerek kullanılmakta mıdır?
UYG.2.2.U8	Windows ortamında güvenli kanal yapılandırması	Windows'ta güvenli iletişim kanalı, güvenlik ve Kurum gereksinimlerine göre yapılandırılmış mıdır?
		Windows'ta güvenli iletişim kanalının yapılandırılması, ilgili grup ilkesi parametrelerini dikkate almakta mıdır?
		Etki alanı denetleyicilerine uzaktan bağlantı ile yönetim durumunda aradaki veri iletişimi şifrelenmekte midir?
UYG.2.2.U9	Active Directory kullanımında kimlik doğrulamanın korunması	Active Directory kullanımında kimlik doğrulamanın korunması amacı ile kullanılan protokoller güçlü kimlik doğrulama yöntemlerini içermekte midir?
		Etki alanı denetleyicilerine anonim erişim engellenmiş midir?
UYG.2.2.U10	Active Directory ortamında DNS'nin güvenli işletimi	"Active Directory-integrated" DNS bölgesi kullanılmakta mıdır?
		"Secure cache against pollution" ve "secure dynamic update" ayarları DNS sunucularında aktif midir?
		DNS istemci ve sunucuları arasındaki iletişim sadece ilgili servis portuna izin veren bir şekilde sınırlandırılmış mıdır?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		DNS trafiği izlenmekte ve normal dışı bir trafik gözlemlendiği durumda müdahale edilmekte midir?
UYG.2.2.U11	Active Directory altyapısını izleme	Active Directory yapısı sistem olayları açısından izlenmekte ve olaylar kayıt altına alınmakta mıdır?
		Active Directory güvenlik olay kayıtları düzenli olarak gözden geçirilmekte midir?
		Etki alanı denetleyicilerinin kullanılabilirlik durumu ve sistem kaynakları izlenmekte midir? Tanımlanan eşik değerlerine uygun olarak uyarı üretilmesine yönelik bir mekanizma mevcut mu?
		Etki alanı ve orman seviyesindeki değişiklikler izlenmekte, kayıt altına alınmakta ve değerlendirilmekte midir?
UYG.2.2.U12	Etki alanı denetleyicilerinin yedeğinin alınması	Kurumda, etki alanı denetleyicilerinin yedeğini alma ve yedekten geri yükleme politikası mevcut mudur?
		Kurumda kullanılan yedekleme yazılımının, etki alanı denetleyicilerinin yedeğini de sağlıklı bir şekilde alma özelliğine sahip olduğu teyit edilmiş midir?
		Etki alanı denetleyicilerinin yedeği düzenli olarak alınmakta mıdır?
		Etki alanı denetleyicilerinin yedeğini almak amacı ile servis yöneticisi haklarına sahip ayrı bir yedekleme hesabı oluşturulmuş mudur?
		”Backup Operators” grubuna üye olan hesapların sayısı asgari seviyede tutulmakta mıdır?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		Yedekleme medyası, uygun ve güvenli bir alanda muhafaza edilmekte midir?
		Muhafaza edilen yedekleme medyasının ihtiyaç durumunda kolay erişilebilmesini sağlamak amacı ile medyaların düzeni, belirli aralıklarla kontrol edilmekte midir?
UYG.2.2.U13	İki faktörlü kimlik doğrulama	Ayrıcalıklı hesapların kullanımında iki faktörlü kimlik doğrulama yöntemi kullanılmakta mıdır?
UYG.2.2.U14	Ayrıcalıklı yönetici sistemleri	PAW(privileged access workstation) mimarisi Active Directory yönetiminde kullanılmakta mıdır?
		Active Directory yönetimi amacı ile kullanılan istemciler güçlü bir şekilde korunmakta mıdır?
UYG.2.2.U15	Yönetim ve canlı ortamın ayrıştırılması	Active Directory yönetim amacı ile "red forest" mimarisi kullanılmakta mıdır?

TÜBİTAK BİLGEM
Yazılım Teknolojileri Araştırma Enstitüsü

İşçi Blokları Mahallesi Muhsin Yazıcıoğlu Caddesi
No:51/C 06530 Çankaya - ANKARA
T 0312 284 92 22 **F** 0312 286 52 22
E epid.yte@tubitak.gov.tr

www.yte.bilgem.tubitak.gov.tr
www.dijitalakademi.gov.tr