
GAZİ ÜNİVERSİTESİ
Gazi
1926

KURUMSAL AĞLARDA
AYRICALIKLI HESAP ERİŞİM KONTROL SİSTEMİ
UYGULAMA MODELİ

Erhan SİNDİREN

YÜKSEK LİSANS TEZİ
ADLİ BİLİŞİM ANABİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

OCAK 2018

Erhan SİNDİREN tarafından hazırlanan "KURUMSAL AĞLARDA AYRICALIKLI HESAP ERİŞİM KONTROL SİSTEMİ UYGULAMA MODELİ" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Adli Bilişim Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç.Dr. Bünyamin CİYLAN

Adli Bilişim Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum ……...……

Başkan : Prof. Dr. O. Ayhan ERDEM

Teknoloji Fakültesi, Bilgisayar Mühendisliği Bölümü, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum ……..……...

Üye : Yrd. Doç. Dr. Mustafa SERT

Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Başkent Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum ……...

Tez Savunma Tarihi: 22 / 01 / 2018

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

Doç. Dr. Aslıhan TÜFEKÇİ

Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Erhan SİNDİREN

22/01/2018

KURUMSAL AĞLARDA AYRICALIKLI HESAP ERİŞİM KONTROL SİSTEMİ UYGULAMA MODELİ

(Yüksek Lisans Tezi)

Erhan SİNDİREN

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Ocak 2018

ÖZET

Kuruluşların bilgi sistem alt yapısını oluşturan çok sayıda bilgisayarın, kullanıcı hesaplarının, yazıcıların, sunucuların vb. merkezi olarak yönetilmesi amacıyla dizin hizmeti uygulamaları kullanılmaktadır. Dizin hizmeti kullanılan ağ altyapıları içerisindeki bileşenlerin ve ağ hizmetlerinin yürütülmesi görevini yerine getirmek için sıradan kullanıcı hesaplarından daha fazla yetkisi bulunan ayrıcalıklı hesaplar kullanılmaktadır. Bu ayrıcalıklı hesaplar dizin hizmeti içerisindeki tüm bileşenler üzerinde çok geniş yetkilere sahiptir. Bu tür sistemlere yapılan siber saldırılarda ana hedeflerden biri de bu hesapların parolalarını ele geçirmektir. Son derece değerli olan bu tür ayrıcalıklı hesaplar kesinlikle kontrolsüz ve savunmasız bırakılmamalıdır. Bu çalışmada ayrıcalıklı hesapların kontrolünün, yönetiminin ve takibinin gerçekleştirilmesini en az maliyet ile sağlayacak bir uygulama modeli tasarlanmış ve gerçekleştirilmiştir. Bu uygulama modeli, ayrıcalıklı kullanıcı hesaplarına ait parolaların temel bilişim teknolojileri güvenlik ilkeleri doğrultusunda belirlenmesi ve parola saldırılarına karşı daha güçlü parolalar oluşturulmasını sağlamıştır. Bilişim teknolojileri personelinin görev sınırlarını netleştirerek iş yükünün azalmasını sağlarken kuruluş yöneticilerinin iş akışına dâhil edilmesi sayesinde yöneticilerin bilişim teknolojileri güvenliği konusunda farkındalıklarının arttırılması hedeflenmiştir.

Bilim Kodu	: 92403
Anahtar Kelimeler	: Ayrıcalıklı hesap yönetimi, yerel yönetici hesapları yönetimi, kimliğe dayalı erişim kontrolü, parola saldırıları
Sayfa Adedi	: 91
Danışman	: Doç. Dr. Bünyamin CİYLAN

PRIVILEGED ACCOUNT ACCESS CONTROL SYSTEM APPLICATION MODEL IN ENTERPRISE NETWORKS

(M. Sc. Thesis)

Erhan SİNDİREN

GAZI UNIVERSITY

INSTITUTE OF INFORMATION

January 2018

ABSTRACT

Directory applications are utilized in order to centrally manage the high number of computers, user accounts, printers, servers, and etc. constituting the information system infrastructure of the companies. While using the directory service, the privileged accounts having more authority than ordinary accounts are used in order to execute the operation of components and network services within the network infrastructures. These privileged accounts have wide authorizations on all the components within the directory service. One of the objectives of cyber-attacks on such systems is to achieve the passwords of such accounts. These accounts, which are very valuable and important for the companies, should not be left uncontrolled and unprotected. For this reason, a model is designed and presented in this study in order to enable the privileged accounts to be controlled, managed, and followed at minimum costs. This application model enabled determination of the passwords of privileged user accounts in accordance with the fundamental IT security principles, establishment of passwords that are stronger against the password attacks, clarification of the limits of duties of IT personnel and decrease in their work load, and increase in the awareness of managers about the IT security by including the enterprise managers into the workflow.

Science Code : 92403
Key Words : Privileged account management, local administrator account management, identity-based access control, password attacks
Page Number : 91
Supervisor : Assoc. Prof. Dr. Bünyamin CİYLAN

TEŞEKKÜR

Tezin hazırlanması aşamasında bana her türlü desteği veren danışmanım sayın Doç.Dr. Bünyamin CİYLAN'a, yüksek lisans ve tez çalışmam boyunca göstermiş olduğu sevgi, anlayış ve sabır ile bana destek olan eşime, desteklerini benden esirgemeyen mesai arkadaşlarıma sonsuz teşekkürlerimi sunmayı bir borç bilirim.

İÇİNDEKİLER

Sayfa

ÖZET ... iv
ABSTRACT ... v
TEŞEKKÜR ... vi
İÇİNDEKİLER ... vii
ŞEKİLLERİN LİSTESİ ... ix
ÇİZELGELERİN LİSTESİ ... xi
KISALTMALAR ... xii
1. GİRİŞ ... 1
2. KAPSAM ... 5
3. AYRICALIKLI HESAP ERİŞİM KONTROL SÜRECİ ... 9
3.1. Kimlik Yönetim Süreci ... 11
3.2. Dizin Hizmeti Ve Basit Dizin Erişim Protokolü ... 14
3.2.1. Dizin hizmeti ... 15
3.2.2. Kullanım alanlarına göre dizin hizmetleri ... 17
3.2.3. Dizin hizmetinin sağladığı görevler ... 18
3.2.4. Dizin hizmetinin doğuşu ... 19
3.2.5. X.500 dizin hizmeti ... 19
3.2.6. Basit dizin erişim protokolü ... 21
3.2.7. Aktif dizin ... 31
3.2.8. Aktif dizin uygulamalarındaki ayrıcalıklı hesapların yetenekleri ... 35
3.3. Parola Kullanımı ve Parola Saldırıları ... 37
3.3.1. Parola kullanımında yapılan hatalar ... 38
3.3.2. Parola saldırıları ... 43
4. METOD ve MATERYAL ... 53
5. AYRICALIKLI HESAP ERİŞİM KONTROL SİSTEMİ UYGULAMA MODELİ ... 57
5.1. Dizin Hizmeti Ayrıcalıklı Hesap Erişim Kontrol Modülü ... 58

Sayfa

5.1.1. Kiralanacak ayrıcalıklı hesaplar ve hesap gruplarının oluşturulması.. 59

5.1.2. Kiralık ayrıcalıklı hesap ve tahsis havuzu ile BT personelinin ilişkilendirme işlemleri..... 61

5.1.3. Tahsis havuzundan ayrıcalıklı hesap kiralama……..... 64

5.1.4. Kiralık hesaplar için üretilen parolanın özellikleri ve yenilenmesi.... 65

5.1.5. Dizin hizmeti ayrıcalıklı hesap erişim kontrol modülü günlük kayıt işlemi..... 68

5.2. Yerel Yönetici Hesaplarına Ait Parola Kontrolü..... 69

5.2.1. Yetkili kullanıcı hesaplarının belirlenmesi……...…… 71

5.2.2. Uygulama kapsamındaki bilgisayarların tespiti……..……..……. 71

5.2.3. Yerel yönetici hesap parolalarının değiştirilmesi, gösterilmesi ve saklanması……..…..……..…….. 73

5.2.4. Yerel yönetici hesapları parola kontrol modülü günlük kayıt işlemi.. 75

5.3. Pilot Kullanım Sonuçları……..... 76

6. SONUÇ VE ÖNERİLER..... 79

KAYNAKLAR..... 83

ÖZGEÇMİŞ…..... 91

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 3.1. AHEKS uygulamasının örnek bir BT altyapısındaki konumu..... 10
Şekil 3.2. Dijital kimlik temel bileşenleri……..…… 12
Şekil 3.3. Kimlik yönetim süreci iş akış bileşenleri…….…... 12
Şekil 3.4. Kimlik yönetim süreci iş akış şeması …….. 14
Şekil 3.5. Dizin hizmeti bileşenleri..... 17
Şekil 3.6. Örnek bir sunucu küme yapısı..... 19
Şekil 3.7. X.500 dizin hizmeti ana bileşenleri 20
Şekil 3.8. İstatiksel incelemesi yapılan LDAP dizin sistemi mimarisi..... 23
Şekil 3.9. Slapd entegrasyonu sonrası LDAP sistem mimarisi 24
Şekil 3.10. İstemci ve LDAP sunucusu arasında tek girdi transferi etkileşimi..... 24
Şekil 3.11. İstemci ve LDAP sunucusu arasında çoklu girdi transferi etkileşimi..... 25
Şekil 3.12. İstemci tarafından gönderilen çoklu LDAP arama isteği etkileşimi..... 25
Şekil 3.13. Normal bir LDAP alışverişi..... 27
Şekil 3.14. Tipik dizin yapısından bir bölüm..... 27
Şekil 3.15. Bir dizin girdisinin sunduğu nitelikler, türler ve değerler……..... 28
Şekil 3.16. Tipik bir LDAP dizin bölümü……..…… 29
Şekil 3.17. Farklı kapsayıcılar içerisinde yer alan aynı göreceli seçkin adlar…… 29
Şekil 3.18. Bir LDAP API'sinin dizin etkin uygulamalardaki konumu……. 30
Şekil 3.19. Aktif dizin hiyerarşik bir nesne yapısı örneği..... 33
Şekil 3.20. Hiyerarşik yapının bir kısmının görüldüğü grafik ara yüzü…… 34
Şekil 3.21. Aktif dizin kullanıcı hakları yapılandırma bölümü ekran görüntüsü……... 36
Şekil 3.22. Parola oluşturulurken kullanılan karakter çeşitliliği oranları..... 39
Şekil 3.23. Ortadaki adam saldırı yöntemi temsili..... 46
Şekil 3.24. Ağ trafiği dinleme saldırı yöntemi temsili 46
Şekil 3.25. Basit bir kelime listesi içeriği……..…….. 47
Şekil 3.26. Hydra saldırıcı aracı ile yapılan bir sözlük saldırısı sonucu..... 48
Şekil 3.27. The powerful rainbowcrack aracıyla gerçekleştirilen örnek saldırısı sonucu…….. 50
Şekil 3.28. Windows işletim sisteminden hashdump ile elde edilen parola bilgileri…. 51
Şekil 5.1. Ayrıcalıklı hesap erişim kontrol sistemi uygulama model şeması..... 57
Şekil 5.2. Dizin hizmeti ayrıcalıklı hesap erişim kontrol modülü temel iş akışı…..... 58

Şekil **Sayfa**

Şekil 5.3. Örnek proje sorumluluk dağılımı..... 59
Şekil 5.4. Örnek dizin hizmeti kullanıcı grupları ve kiralanacak hesaplar..... 60
Şekil 5.5. Tahsis havuzuna kullanıcı ekleme ara yüzü ekran görüntüsü..... 62
Şekil 5.6. Tahsis havuzu yönetici onayı arayüzü ekran görüntüsü……... 63
Şekil 5.7. Tahsis havuzundan ayrıcalıklı hesap kiralama arayüzü ekran görüntüsü..... 65
Şekil 5.8. Rastgele parola üretmek için kullanılabilecek örnek C# kod parçacığı……. 66
Şekil 5.9. Örnek parola için kombinasyon ve saldırı süreleri sonuçları…… 66
Şekil 5.10. Yerel yönetici hesapları parola kontrol modülü temel iş akışı…….. 70
Şekil 5.11. Yerel yönetici hesapları parola kontrol modülü temel işlem adımları…….. 70
Şekil 5.12. Seçkin ad karşılaştırma süreci..... 72
Şekil 5.13. Uygulama kapsamındaki bilgisayarların tespiti alt iş akışı..... 73
Şekil 5.14. Yerel yönetici hesapları parola kontrol modülü ara yüzü ekran görüntüsü.. 74
Şekil 5.15. Uygulama kapsamındaki bilgisayarların otomatik parola değiştirme alt iş akışı..... 75

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 3.1. Temel LDAP C API fonksiyonları 31
Çizelge 3.2. En yaygın kullanılan nitelik türleri…..... 34
Çizelge 3.3. Hatalı parola oluşturma davranış örnekleri…….....……. 40
Çizelge 3.4. Hatalı parola kullanım davranışı örnekleri..... 41
Çizelge 3.5. Bazı kriptografik özet algoritmaları özellikleri…….. 49
Çizelge 3.6. "Gazi Üniversitesi" olarak yapılan girdinin farklı kriptografik özet algoritmaları ile elde edilen kriptografik özet bilgisi..... 49
Çizelge 3.7. "Gazi üniversitesi" olarak yapılan girdinin farklı kriptografik özet algoritmaları ile elde edilen kriptografik özet bilgisi…….……. 50
Çizelge 4.1. Uygulama karşılaştırma çizelgesi…… 55
Çizelge 5.1. Örnek hesap grupları, proje tanımları ve sorumlu birim eşleştirme tablosu……..… 60
Çizelge 5.2. Veri tabanı örnek kullanıcı hesapları ilişkilendirme tablosu..... 62
Çizelge 5.3. Üretilen örnek parola için kombinasyonlar ve saldırı süreleri……..... 67

KISALTMALAR

Bu çalışmada kullanılan bazı kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklama
AHEKS	Ayrıcalıklı Hesap Erişim Kontrol Sistemi
API	Uygulama Programlama Arayüzü (Application Programming Interface)
BGYS	Bilgi Güvenliği Yönetim Sistemi
BT	Bilişim Teknolojileri
CCITT	Uluslararası Telgraf ve Telefon Danışma Komitesi (The International Telegraph And Telephone Consultative Committee)
CN	Ortak Ad **(**Common Name)
DAP	Dizin Erişim İletişim Kuralı **(**Directory Access Protocol)
DAS	Dizin Yardımı Hizmeti (Directory Assistance Service)
DC	Etki Alanı Bileşeni (Domain Component)
DISP	Dizin Bilgileri Gölgelendirme İletişim Kuralı (Directory Information Shadowing Protocol)
DIXIE	Etkili Uygulanan X.500 Dizin Arayüzü (Directory Interface to X.500 Implemented Efficiently)
DMZ	Yarı Güvenli Ağ (Demilitarized Zone)
DN	Seçkin Ad **(**Distinguished Name)
DNS	Alan Adı Sistemi (Domain Name System)
DOP	Dizin Operasyonel Bağlama İletişim Kuralı (Directory Operational Binding Protocol)
DSA	Dizin Sistemi Aracısı (Directory System Agent)
DSP	Dizin Sistemi İletişim Kuralı (Directory System Protocol)
DUA	Dizin Kullanıcı Aracısı (Directory User Agent)
FIPS	Federal Bilgi İşleme Standardı (Federal Information Processing Standard)
FTP	Dosya Transferi İletişim Kuralı **(**File Transfer Protocol)
ICMP	Internet Denetim İletisi İletişim Kuralı **(**Internet Control Message Protocol)
IDC	Uluslararası Veri Şirketi (International Data Corporation)

Kısaltmalar	Açıklama
IP	İnternet İletişim Kuralı **(**Internet Protocol)
ISO	Uluslararası Standartlar Teşkilâtı (International Organization for Standardization)
ITU	Uluslararası Telekomünikasyon Birliği (The International Telecommunication Union)
LDAP	Hafif Dizin Erişimi İletişim Kuralı (Lightweight Directory Access Protocol)
MD5	İleti Özeti Algoritması 5 (Message Digest Algorithm 5)
NDS	Netware Dizin Hizmeti (Netware Directory Service)
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology)
NOS	Ağ İşletim Sistemi (Network Operating System)
NTLM	Yeni Teknoloji Yerel Ağ Yöneticisi **(**New Technology Local Area Network Manager)
OSI	Açık Sistemler Ara Bağlaşımı (Open System Interconnection)
OU	Kuruluş Birimi **(**Organizational Unit)
RFC	Yorum istekleri (Requests for Comments)
SASL	Basit Doğrulama ve Güvenlik Katmanı (Simple Authentication and Security Layer)
SDK	Yazılım Geliştirme Aracı *(*Software Development Kit)
SHA	Güvenli Özet Algoritması **(**Secure Hash Algorithm)
SLAPD	Bağımsız LDAP Arka Plan Uygulaması **(**Stand-Alone LDAP Daemon)
TCP	İletim Denetimi İletişim Kuralı **(**Transmission Control Protocol)
TLS	Taşıma Katmanı Güvenliği **(**Transport Layer Security)
WBEM	Web Tabanlı Kurumsal Yönetim (Web Based Enterprise Management)
WMI	Windows Yönetim Aletleri (Windows Management Instrumentation)
VT	Veri Tabanı

1. GİRİŞ

Bilgisayar kullanımının yaygınlaşmasıyla beraber, ortaya çıkan ihtiyaçlar nedeniyle bilgisayarların birbiriyle iletişim halinde olması gerekliliği ortaya çıkmış, geliştirilen ağ protokolleri sayesinde birden fazla bilgisayar birbirine bağlanarak kullanılmaya başlanmış ve bilgisayarlar arası veri iletişimi mümkün hale gelmiştir. Zamanla ağ altyapısı içerisinde yer alan bilgisayar sayılarının artması bilgisayarların, kullanıcıların ve ağ içerisindeki diğer bileşenlerin yönetilmesi zorunluluğunu ortaya çıkmıştır [1].

Bu maksatla kuruluşların ağ altyapısı içerisinde kullanıcı hesaplarının, bilgisayarların, yazıcıların ve diğer bileşenlerin yönetilmesini amaçlayan bir çeşit veri tabanı olarak tanımlanabilecek dizin hizmeti uygulamaları kullanılmaya başlanmıştır. Dizin hizmeti uygulamaları, sahip olduğu hiyerarşik yapı sayesinde belirlenen ilkeler doğrultusunda dizin hizmetine dâhil edilen tüm bileşenlerin yönetilmesine imkân sağlamaktadır [1-3].

Günümüzde ücretsiz ve ticari olarak kullanımda olan Microsoft Aktif Dizin (*Active Directory*), 389 Directory Server, Novell eDirectory, Oracle Directory Server, OpenLDAP, Apache Directory Studio ve IBM Tivoli Directory Server gibi farklı dizin hizmeti uygulamaları mevcuttur. Microsoft Aktif Dizin uygulaması Windows platformlarında çalışmaktadır [4]. Diğer dizin hizmeti uygulamaları Linux [5-7] veya platform bağımsız olarak çalışmaktadır [8-10].

Dizin hizmeti, bilişim teknolojisi (*BT*) alt yapısına sahip birçok kuruluş tarafından kullanılmakta ve sağladığı avantajlar sayesinde bilgisayarlara bağımlı kuruluşların ayrılmaz bir parçası haline gelmiştir. Ancak sağladığı avantajların yanı sıra farklı güvenlik önlemlerine de ihtiyaç duymaktadır. Dizin hizmeti uygulamalarının BT altyapısı için merkezi yönetim imkânı sunduğu göz önünde bulundurulduğunda alınacak güvenlik tedbirlerinin aslında tüm BT altyapısı için olduğu görülmektedir [11].

Kuruluş içerisindeki idari çalışanlar, kendilerine tahsis edilen ve dizin hizmeti içerisinde yer alan kullanıcı hesapları aracılığıyla bilgisayarlarında oturum açmaktadırlar. Bu kullanıcı hesaplarına, dizin hizmeti uygulamalarının sağladığı imkânlar sayesinde çeşitli izinler verilmekte ve bazı kısıtlamalar yapılmaktadır. Bu yapılandırma, kullanıcıların sadece kendilerine ayrılmış kaynak ve nesnelere erişmelerini sağlamaktadır [12-14].

Bu tür hesaplar, dizin hizmeti içerisinde "*kullanıcı hesapları"* olarak adlandırılan bir topluluğa üyedir ve BT altyapısı bileşenleri üzerinde değişiklik, silme ve ekleme gibi işlemler yapamazlar. BT altyapısı bileşenleri üzerinde değişiklik, silme ve ekleme gibi işlemleri yapabilmek için dizin hizmeti içerisinde "*ayrıcalıklı hesaplar*" olarak adlandırılan topluluğa üye hesaplara ihtiyaç vardır. Ayrıcalıklı hesaplar, BT altyapısı ve bileşenlerinin idamesini sağlamakla görevli BT personeli tarafından kullanmaktadır. BT personeli tarafından kullanılan bu ayrıcalıklı yönetici hesapları birçok yetkiye sahiptir ve bu hesaplar kuruluşlar için bilişim sistemleri içerisinde korunması gereken değerler arasında ilk sıralarda yer almaktadır [15-17]. Dizin hizmeti uygulaması içerisinde *ayrıcalıklı hesaplara* dâhil bir hesabın saldırganlar tarafından ele geçirilmesi tüm bilişim sisteminin ele geçirilmesine neden olabilir [18].

Geniş BT altyapısına sahip kuruluşlar içerisinde tüm bileşenlerden tek bir BT personelinin sorumlu olması beklenemez. Bu nedenle bu tür kuruluşlarda birçok BT personeli çalışır ve doğru olan uygun görev dağılımını yapmaktır. BT personelinin görev dağılımı yapılırken, BT personeli tarafından kullanılan ayrıcalıklı hesapların erişim yetkilerinin düzenlenmesi genellikle ihmal edilmektedir. Örneğin web sunucularından sorumlu bir BT personeli, sahip olduğu ayrıcalıklı hesabı sayesinde dosya sunucularına, FTP sunucularına, veri tabanı sunucularına, günlük kayıtların saklandığı sunuculara ve en önemlisi dizin hizmeti uygulama sunucularına erişebilmektedir. İdare tarafından görevlendirilmediği halde yetkisi dışında bu sistemler üzerinde işlem yapabilmektedir. Bu nedenle doğru bir kimlik yönetimi sadece idari çalışanlar için değil BT personeli içinde bir gerekliliktir [19-24].

Bu çalışmada, dizin hizmeti kullanan kuruluşların bilgisayarlarına ait yerel yönetici hesaplarının ve dizin hizmetindeki ayrıcalıklı hesap parolalarının yönetimini, takibini ve saldırılara karşı dayanıklılığını arttıracak *Ayrıcalıklı Hesap Erişim Kontrol Sistemi* (AHEKS) uygulama modeli sunulmaktadır. Bu uygulama modeli, *Basit Dizin Erişim Protokolü* (Lightweight Directory Access Protocol-LDAP) [25] uyumlu tüm dizin hizmetlerinde kullanılabilmektedir. Bu uygulama modeli, ayrıcalıklı hesaplara sahip BT personeli için kimlik yönetimi gerçekleştirerek, bilgi güvenliği temel bileşenlerinden gizlilik ve bütünlüğü doğrudan, dolaylı olarak erişilebilirliğin korunmasını amaçlamıştır. Uygulama modeli, kuruluş bünyesinde temel yazılım geliştirme bilgisine sahip bir BT personeli tarafından hayata geçirebilecek yapıdadır ve bu sayede kuruluşa ilave bir maliyet getirmeden tüm bu yetenekleri sunmaktadır.

Bu tez çalışmasında, AHEKS'in neden gerekli olduğu ve kapsamı Bölüm 2'de açıklanmıştır. AHEKS'in hangi platformlarda çalıştığı, hangi güvenlik gereksinimleri karşıladığı ve BT altyapısında ki yeri Bölüm 3'de belirtilmiştir. Bölüm 4'de eşdeğer işlevlere sahip diğer uygulamalar ile AHEKS'in sahip olduğu özellikler karşılaştırılmıştır. AHEKS uygulamasının iş akışı, ana ve alt modülleri, kullanımı, uygulama ara yüzlerinin ekran görüntüleri ve pilot kullanım sonuçları Bölüm 5'de sunulmuştur. Bölüm 6'da sonuçlar ve önerilere yer verilmiştir

2. KAPSAM

Kuruluşlar, gelişen bilişim teknolojilerinin her türlü imkânından faydalanmak ve güncel kalabilmek adına her gün kendilerine ait sistemlerin geliştirilmesi ve ihtiyaçlarının daha kolay giderilmesi maksadıyla teknoloji gelişimini teşvik etmekte, arkadan itici bir güç olarak geliştiricileri zorlamaktadır. Kuruluşlar güncel teknolojileri imkânları ölçüsünde sistemlerine dâhil ederek her geçen gün çalışma alanlarını bilişim sistemlerinin üzerine aktarmakta ve bilişim teknolojileriyle daha entegre şekilde çalışmaktadırlar. Gelişen ve genişleyen kuruluşlar farklı coğrafi konumlara dağılmakta, bunun sonucu bilişim sistemlerini farklı şehirler, ülkeler ve hatta kıtalara konumlandırmaktadırlar. Bilişim sistemlerinin dağıtık bir yapıya sahip olması, bilişim sistemlerine yönelik saldırı yüzeyini genişletmesi nedeniyle tehdit oranını arttırmaktadır. Bunun doğal bir sonucu olarak kuruluşlar, kendi bilişim sistemlerini ve bilgilerini korumak adına gelişen teknolojiye paralel güvenlik tedbirlerini arttırmakta ve her geçen yıl buna çok yüksek bütçeler ayırmak zorunda kalmaktadırlar [26].

Kuruluşlar birçok BT güvenlik sistemini, içeriden ve dışarından bilişim sistemlerine tehdit oluşturabilecek bilinçli veya bilinçsiz davranışların önüne geçmek için kullanmaktadır. Her gün farklı saldırı yöntemleri, farklı güvenlik açıkları ve davranışlarla karşılaşılan BT güvenliği alanında, güncel tedbirler geliştirilmesi konusunda çalışmalar devam ederken, saldırılardan korunmak adına alınması gereken geleneksel BT güvenlik önlemleri unutulmakta veya ihmal edilmektedir. Bunun neticesinde her gün yeni bir saldırı türünün ortaya çıkabileceği olasılığına karşı bilişim sistemlerini korumaya çalışan kuruluşların, günü kurtarmak adına geçici çözümlere başvurduğu veya sadece teknoloji temelli çözümlere odaklandığı görülmektedir [22,27]. Kuruluşlar, tüm saldırıları engellemesi beklenen ancak yeni geliştirilen saldırıları engellemekte yetersiz kalabilen BT güvenlik sistemlerine yüksek maliyetler harcamakta, unutulmaması ve en başta alınması gerekenin geleneksel güvenlik tedbirleri olduğunu çok acı tecrübelerle öğrenmektedir [28].

Geleneksel BT güvenliği denildiğinde akla ilk gelen ve en önemli güvenlik tedbiri olarak değerlendirebileceğimiz konu parola güvenliğidir [29]. Çünkü saldırganların nihai amaçlarına ulaşmak maksadıyla ilk hedefleri sistemde kullanılan parolalardır [30]. Dizin yapısının kullanıldığı sistemlerde sıradan kullanıcı hesaplarının yanı sıra BT personeline ait olan ve sistem içerisinde ayrıcalıklı yetkilere sahip olan yönetici hesapları da

bulunmaktadır. Bu hesaplar BT sistemlerinin bakım, onarım ve idamesi amacıyla kullanılmaktadır. Bu hesaplardan birinin parolasının saldırganlar tarafından ele geçirilmesi tüm sistemin ele geçirilmesi anlamına gelecektir. Bu ayrıcalıklı hesaplar için, yani bilişim sistemini yönetmek için kullanılan bu ayrıcalıklı haklara sahip yönetici hesapları için bazı çalışmalarda "*Krallığın Anahtarı*" (*Key to the Kingdom*) tabiri kullanılmaktadır [31-33].

Ayrıcalıklı hesapların kontrol edilmesi ve yönetilmesi kuruluşlar için ilave bir önlem değil, öncelikli olarak değerlendirilmesi gereken bir zorunluluktur. Güçlü parola kullanımı, her bir bilgisayar için yerel yönetici hesap parolasının farklı olması ve kısa periyotlarla değiştirilmesi, dizin hizmetindeki ayrıcalıklı hesapların görev bazlı olarak yetkilendirilen personele teslim edilmesi ve tüm bu süreçlerin takip edilmesi, kuruluşları içeriden ve dışarıdan gelecek birçok siber saldırıdan koruyacaktır [34-38].

Dizin Yapısı içerisinde ayrıcalıklı hesaplara sahip BT personeli, dizin yapısı içerisindeki veri tabanları, dosya sunucuları, uygulama sunucuları, kullanıcı bilgileri, elektronik posta sunucuları, dizin sunucuları vb. nesnelerin tümüne erişim hakkına sahiptir. Örneğin, veri tabanı üzerinde işlem yapması için görevlendirilen BT personeli, dosya sunucuları, uygulama sunucuları, kullanıcı bilgileri, elektronik posta sunucuları, dizin hizmeti uygulama sunucuları vb. nesnelerin tümüne erişim sağlayabilir. Bu ayrıcalığa sahip olanların BT personeli olması nedeniyle ilk bakışta bu yetkilendirme normal görünebilir, ancak BT güvenliğinin bütünlük, erişilebilirlik ve gizlilik temel bileşenlerinden gizlilik ve bütünlük bileşenlerinin açıkça ihlali anlamına gelmektedir. Gizlilik, *"hassas verilerin güven içerisinde tutulması, bireylerden ve kuruluşlardan uygun görülenlerle sınırlanmasıdır"* [39]. Yani gizlilik bileşeni, bilgiye erişim sağlamasına müsaade edilen kişiler ve sistemler tarafından erişilmesini sağlanmak ve yetkisiz kişilerin eline geçmesini önlemek anlamına gelmektedir. Bütünlük, *"güvenilir, bozulmamış veya mükemmel durumda olmaktır"* [39]. Yani bütünlük bileşeni, bilgiyi sadece erişim sağlamasına müsaade edilen kişilerin ve sistemlerin değişiklik yapmasını garantileyecek şekilde bilgi güvenliğinin sağlanmasıdır [40,41]. Ayrıca ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi (BGYS) Standardında risk değerlendirmesi varlık, açıklık ve tehdit temeline dayandırılırken, yerine gelen ISO 27001:2013 BGYS Standardında, bilişim güvenliğinin temel bileşenleri olan gizlilik, bütünlük ve erişilebilirlik temeline dayalı bir risk değerlendirmesine yerini bırakmıştır [42]. Tüm bunlar değerlendirildiğinde BT personelinin yetkileri dâhilindeki bilişim sistemlerine erişim sağlayabilecek şekilde

yetkilerinin sınırlandırılması gerekliliği, yani kuruluş içerisinde bilişim sistemleri ve BT personeli için sağlıklı bir kimlik yönetimine ihtiyaç bulunmaktadır.

Uluslararası Veri Şirketi (IDC) tarafından yapılan "*Türkiye Güvenlik Yazılımı Pazarı 2013-2017 Tahmin Raporu (IDC # CEMA20494)*" 2013-2017 yılları arasında Türkiye'de güvenlik yazılımları için yapılacak harcamanın toplam 127.140.000,00 Amerikan doları olacağını öngörmektedir [43]. Yüksek değerler göz önüne alındığında yapılacak harcamaların ülke içerisinde kalması hedeflenmeli ve bunun için yerli BT güvenliği ürünleri kullanılmalıdır. Ancak Türkiye'de BT güvenliği alanında yazılım ve donanım sağlayan firmaların birçoğunun yurt dışı kaynaklı şirketlerin ürünlerine teknik destek ve pazarlama hizmeti vermek üzere çalışmakta olduğu bilinmektedir ve çok azı kendi ürünlerini tasarlamaktadır. Son yıllarda yerli BT güvenliği ürünlerinde bir artış olsa da günümüzde halen yeterli seviyede değildir. Bu nedenle kuruluşların bu alandaki yapacakları yüksek hacimli harcamaların yurt dışına gideceği, BT güvenliği konusunda dışa bağımlılığın devam edeceği ve yerli BT güvenlik ürünleri kullanılmadığı müddetçe BT güvenliğinin istenilen seviyede olamayacağı anlamına gelmektedir. Yerli bir BT güvenlik şirketi yetkilisi ile 2015 yılının haziran ayında yapılan röportajda Türkiye'de BT güvenlik yazılımı sektöründeki şirketlerin kendi uygulamalarını geliştirmek yerine, yurt dışı kaynaklı yazılımlara Türkçe ara yüz yazdıkları yönündeki ifadesi söz konusu görüşü destekler niteliktedir [44].

Çalışmada sunulan uygulama modeline eşdeğer işlevlere sahip ticari uygulamalar mevcut olmakla beraber, çoğunluğu yurt dışı menşeilidir. Farklı ücretlendirme politikalarıyla kullanıcıların hizmetine sunulan bu yurt dışı kaynaklı uygulamaların kuruluşa uygunluğu ve ortaya çıkartacağı maliyet, BT güvenliği için yapılan harcamaları gereksiz gören bazı idarecilere kabul ettirmek, BT güvenliğinden sorumlu her personelin karşısına çıkabilecek problemlerden biridir. Ayrıca çalışmanın konusu olan uygulama modeli BT güvenliği konusunda çok fazla bütçe ayıramayan orta ölçekli kuruluşlar için düşük maliyeti sayesinde alternatif bir önlem olarak tasarlanmıştır.

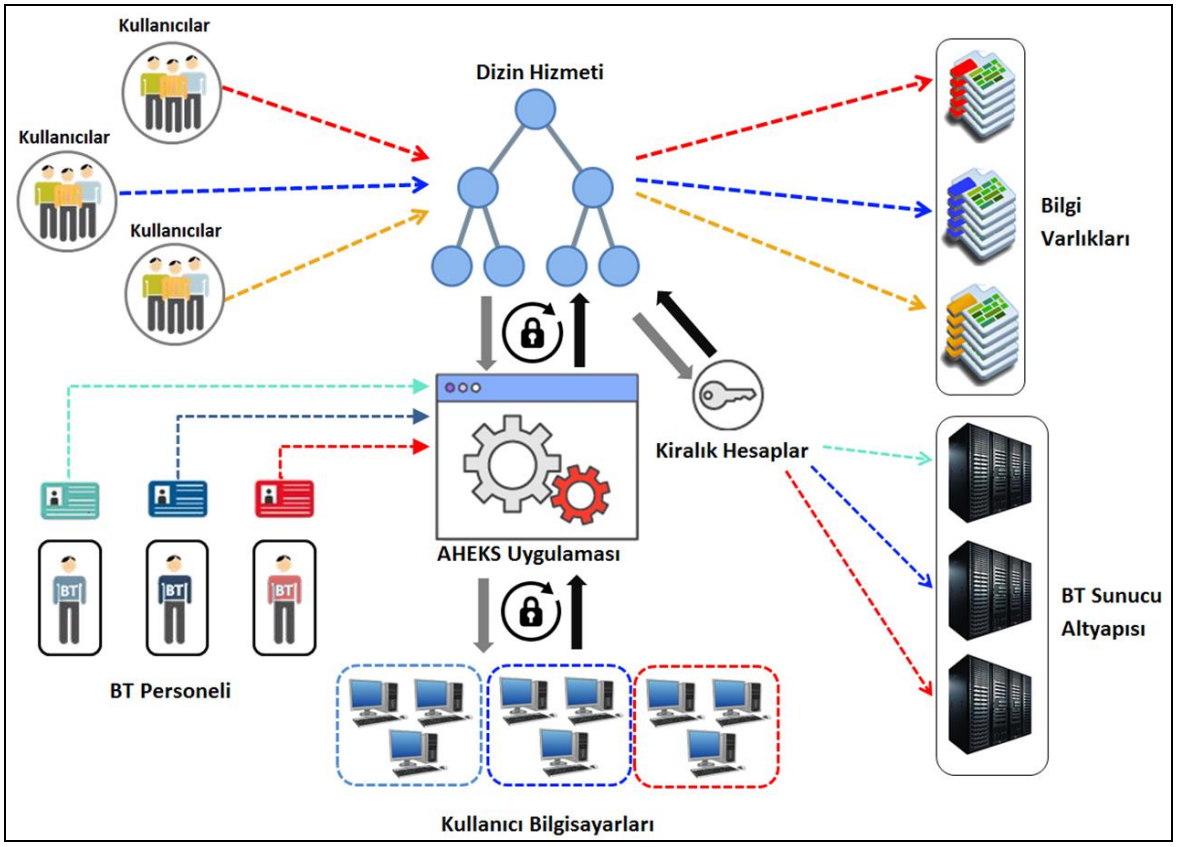
3. AYRICALIKLI HESAP ERİŞİM KONTROL SÜRECİ

Bilişim sistemlerine dâhil olan kullanıcı hesaplarının, bilgisayarların, yazıcıların ve diğer bileşenlerin belirli hiyerarşik yapı içerisinde belirli politikalar doğrultusunda yönetilmesi amacıyla dizin hizmeti uygulamaları kullanılmaktadır. Dizin hizmeti uygulamaları, dizin hizmetine dâhil edilen tüm bileşenlerin yönetilmesine imkân sağlamaktadır [1-3]. Dizin hizmeti kullanılan ve geniş kapsamlı bilişim sistemlerine sahip kuruluşlar içerisinde doğru olan BT personelinin görev dağılımını yapmaktır. Ayrıca BT personeli tarafından kullanılan ayrıcalıklı hesapların erişim yetkilerinin BT personelinin sorumlulukları çerçevesinde düzenlenmesi gerekmektedir. Bu sayede BT personelinin sorumlulukları dışındaki BT bileşenlerine yetkisiz erişimleri engellenecektir. BT personelinin bilişim sistemleri bileşenlerine erişimlerinin önemi sahip oldukları ayrıcalıklı hesaplardan kaynaklanmaktadır [20-21]. BT personeli dışında kalan kullanıcılar, kendilerine tahsis edilen kullanıcı hesapları ile dizin hizmeti uygulamaları üzerinde yapılan düzenlemeler kapsamında kurumsal bilgi varlıkları üzerinde işlem yapmaktadırlar [12-14].

Dizin hizmetindeki ayrıcalıklı hesapların parolaları ve dizin hizmetine dâhil edilmiş bilgisayarların yerel yönetici hesaplarının parolaları gerçekleştirilebilecek siber saldırılara karşı korunmalıdır. Özellikle BT personelinin sahip olduğu ayrıcalıklı hesaplar değerlendirildiğinde, arkasında saklanan değerli varlıklar nedeniyle söz konusu hesapların parolaları, her zaman saldırganların öncelikli hedefi olmaktadır [30]. AHEKS, ayrıcalıklı hesaplar için belirlenecek parolaları sıkılaştırma ve belli sürelerle değiştirme işlemini otomatik olarak gerçekleştirerek güvenliği arttırmaktadır.

Saldırganlar, illegal olarak bu parolaları aşmak maksadıyla birçok farklı yöntem ve araç geliştirmektedir. Buna karşılık olarak BT güvenlik uzmanları da karşı yöntem ve politikalar geliştirerek bu saldırılara karşı koymaya çalışmaktadırlar. Ancak saldırganların hiçbir etik ve teknik kaygısı bulunmadığından her zaman saldırılar, korunma yöntemlerinin bir adım önünde olmaktadır. Ayrıca bilinçsiz kullanıcılar, yetersiz teknik altyapı, BT güvenliğinin öneminin farkında olmayan yöneticiler ve getireceği ek maliyetler de güvenlik uzmanlarının aşması gereken sorunlar olarak karşılarına çıkmaktadır [45-49]. AHEKS, ayrıcalıklı hesap sayısını sınırlandırmak suretiyle saldırı yüzeyini azaltarak kuruluşlara BT güvenliği konusunda katkı sağlamaktadır.

Ayrıcalıklı hesapların hiçbir sınırlamaya tabi tutulmadan BT personelinin kullanımına sunulması, kuruluş içerisinde BT güvenliği sorunlarına neden olabilmektedir. BT personelinin sorumlu olduğu bilişim sistemleri dışındaki erişimlerinin engellenmesi gerekmektedir. BT altyapısı üzerindeki yetkiler, görevlendirmeler temel alınarak düzenlenmeli ve BT personeli görevlerine dayalı bir kimlik yönetimine tabi tutulmalıdır [50]. Genel olarak kimlik yönetimi süreci kavramından, kurumsal bilgi sistemleri, varlıklar ile uygulamalar üzerinde kontrol ve erişim için yüksek seviyede yetkilendirilen ayrıcalıklı kullanıcıların kontrol altına alınması anlaşılmaktadır [96]. Kimliğin yönetilmesi, kullanıcı adı ve parolalar gibi kimlik bilgileri ile dijital kimliklerin kullanım sürecidir. [51]. AHEKS, BT altyapısının mantıksal olarak bölümlenmesi ve her bölüm için yaratılan ayrıcalıklı hesapların ilgili BT personelinin kullanımıma sunulması işlevleriyle BT personelinin erişiminde kimliğe dayalı erişim kontrol sürecini devreye sokmaktadır.



Şekil 3.1 AHEKS uygulamasının örnek bir BT altyapısındaki konumu

Çalışmada sunulan AHEKS uygulama modeli, dizin hizmeti kullanılan BT altyapılarında ayrıcalıklı hesap erişim kontrol süreci sonunda BT güvenliğini arttırmayı amaçlamaktadır. Bu süreç içerisinde temel olarak amaç;

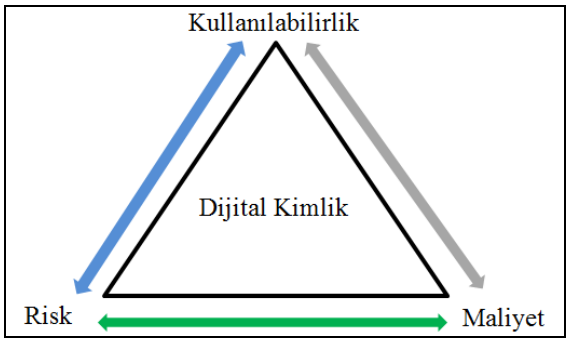
- Ayrıcalıklı hesapların sayısını sınırlamak,
- BT personeli için bir kimlik yönetim süreci sağlamak,
- BT personelinin, BT sunucu altyapısında sadece sorumlu olduğu bileşenlere erişmesini sağlamak,
- Ayrıcalıklı hesaplar ve bilgisayarların yerel yönetici hesapları için belirli sürelerde değişen, rastlantısal olarak belirlenen kuvvetli parolalar üretmektir.

AHEKS uygulaması işlevlerini yerine getirirken gömülü bir LDAP API'si sayesinde BT alt yapısındaki dizin hizmeti uygulaması ile tümleşik çalışmaktadır. AHEKS uygulaması, BT personelinin BT altyapısındaki sunuculara ve bilgisayarlara erişimlerinde, ilave bir güvenlik katmanı olarak dizin hizmeti uygulaması önünde yer almaktadır (Bkz. Şekil 3.1).

3.1. Kimlik Yönetim Süreci

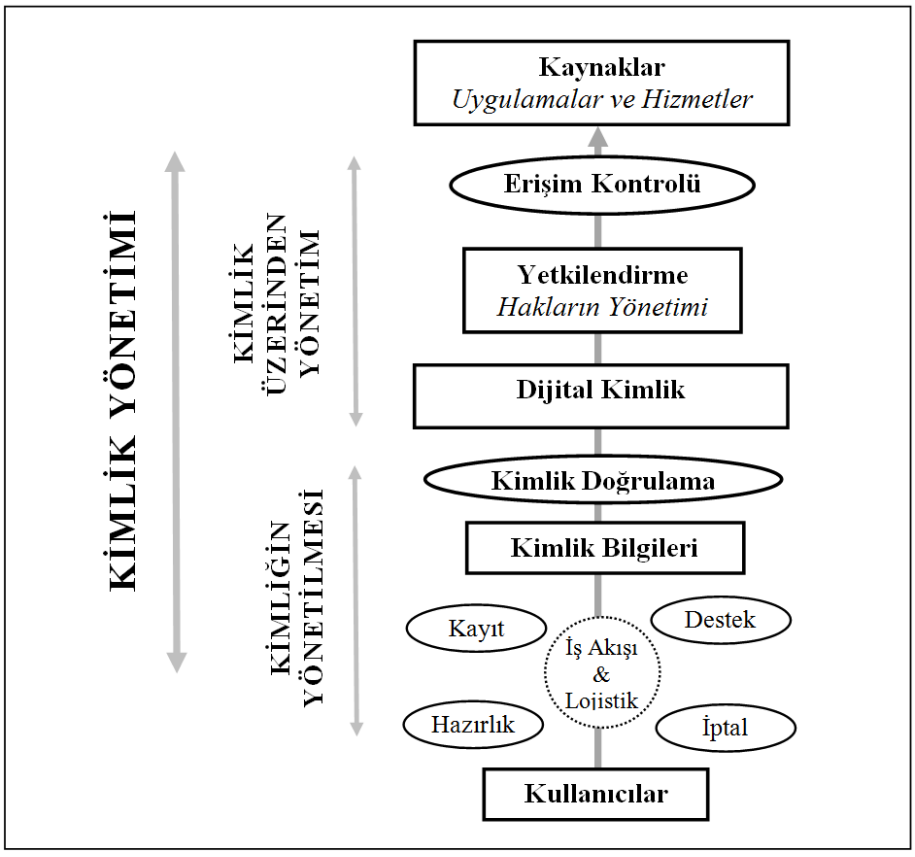
Bilişim teknolojilerinde kimlik yönetim sürecini açıklamadan önce dijital kimlik kavramının açıklanması gerekir. Dijital kimlik, özgül bir bağlamda bir varlığın bir temsilidir [52,53]. Dijital kimliğin, gerçek hayatımızdaki bilgilerimizi içeren kimlik kartı veya pasaport gibi kişisel niteliklerimizi yansıtan bir tür kimlik olduğu [54] görüşünün yanı sıra dijital kimlik ile gerçek dünyadaki kimlik arasında her zaman bir bağlantı olması gerektiğinin zorunlu olmadığını ileri süren iki farklı görüş mevcuttur [52,55]. İleri sürülen bu iki görüşün ışığında bir dijital kimlik, bir bireyin ayırt edici özelliği veya kişisel niteliklerini yansıtan dijital dünyadaki karşılığı olarak tanımlanabilir.

Kişisel nitelikler, tercihler ve çeşitli özelliklerden meydana gelen dijital kimlikler sayesinde farklı bireyler için kişileştirilmiş hizmetler sunulması mümkün kılınmaktadır. Bu özelliğin çevrim içi kullanımının yaygınlaşması, çeşitli gereksinimlerin ortaya çıkmasına neden olmuştur. Öncelikle dijital kimlik sahibi, kendisi için kişiselleştirilmiş hizmetlerden faydalanabilmek amacıyla kimliğini doğrulamak zorundadır. Ancak bir kimlik doğrulama tüm güvenlik sorunlarının çözümü değildir. Bu nedenle dijital kimliklerin yönetilmesi önemli ve gerekli bir konudur. Dijital kimlik yönetimi, sadece hizmet ve işlevsellik beklentilerini değil, aynı zamanda güvenlik ve gizlilik beklentilerini de karşılamaktadır [56]. Kimlik yönetim süreci, kullanılabilirlik, risk ve maliyet olmak üzere üç temel bileşen (Şekil 3.2) üzerinde yürütülmektedir [52].



Şekil 3.2. Dijital kimlik temel bileşenleri

Genel olarak kimlik yönetimi süreci kavramından, kurumsal bilgi sistemleri, varlıklar ile uygulamalar üzerinde kontrol ve erişim için yüksek seviyede yetkilendirilen ayrıcalıklı kullanıcıların kontrol altına alınması anlaşılmaktadır [57]. Kimlik yönetimi, kimliğin yönetilmesi ve kimlik üzerinden yönetim (Şekil 3.3) olmak üzere temel iki bileşene sahiptir. Kimliğin yönetilmesi, kullanıcı adı ve parolalar gibi kimlik bilgileri ile dijital kimliklerin kullanım sürecidir. Kimlik üzerinden yönetim ise kendi yetkileri dâhilinde belirli bir düzen içinde kaynaklara başarılı erişim ile kullanıcı kimlik ispatlama süreçlerinin bir araya getirilmesidir [51].



Şekil 3.3. Kimlik yönetim süreci iş akış bileşenleri [51]

Gelişen teknolojiye paralel olarak kurumların BT altyapılarının büyümesi ve sağladıkları çevrim içi hizmet yelpazesinin genişlemesi, bu hizmetlerden faydalanan veya yöneten kişilerin dijital kimliklerinin artmasına neden olmuştur. Farklı altyapılarda kullanılan ve sayıları artan dijital kimliklerin tutarlılığının korunması ve tehditlere karşı güvenlik çözümleri geliştirilmesi ihtiyacını da ortaya çıkarmıştır. Geniş BT altyapılarına sahip kurumlar, BT yöneticilerinin iş yükünü azaltmak, dijital kimlik yönetim maliyetlerini düşürmek, güvenliği tehdit edebilecek riskleri engellemek ve kimlik yönetim sürecinin iş akışlarına dâhil edebilmek amacıyla son on yılda kimlik yönetim sistemlerinin kullanımına önem vermektedirler [58,59].

Gerçek hayattaki kimlik ile dijital kimlikler arasından birçok benzerlik ve bunun yanı sıra farklılıklar mevcuttur. Ancak bu iki kimlik yapısını birbirinden ayıran en önemli özellik gerçek hayatta sahip olduğumuz kimlik bir tane iken dijital kimlik sayısı kullandığımız BT sistemlerine bağlı olarak birden fazla olabilmektedir [60]. Bu sayı, sıradan bir kullanıcının baş edemeyeceği kadar fazla olduğu durumlarda BT güvenliği ile ilgili sorunlara neden olabilecek yöntemlerin (*tüm parolaların aynı veya basit olması, parolaların başkalarının ulaşabileceği yerlere not edilmesi vb*.) kullanılması olasılığı artmaktadır. Bu tür güvenlik sorunlarının önüne geçmek, görev değişiklikleri ve çeşitli nedenlerle işten ayrılma gibi durumlarda ilgili kişilerin kurum içerisindeki erişim yetkilerinin düzenlenmesi konularının çözümlenmesinde kimlik yönetim süreci devreye girmektedir [58,59].

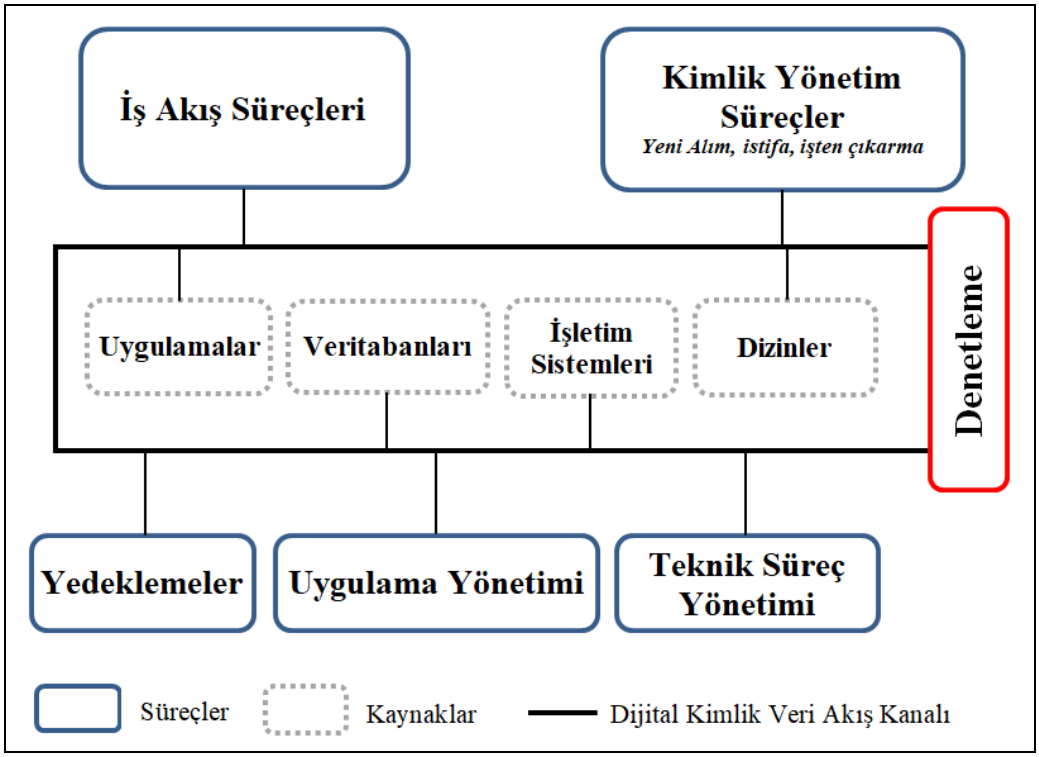
Kimlik yönetim süreci, kuruluş içerisinde dijital kimlik sahibi kullanıcıların müsaade edilen kaynaklara tabi oldukları yetki sınıflandırmaları dâhilinde erişimini, yetki sınıfları dışında kalan kaynaklara erişimlerinin engellenmesini, yetkili ve yetkisiz erişimlerin kontrol edilmesini ve en önemlisi dijital kimlik sahibi kullanıcıların yetkilerinin belirlenerek, sınıflandırılmalarını sağlamak amacıyla kullanılır [51,60-61]. Gerçekleştirilen bu işlemler BT güvenliğinin önemli bir parçasıdır ve kimlik yönetim süreci hayata geçirilirken aşağıdaki hususlara dikkat edilmesi gerekmektedir;

- Kimlik Yönetim sürecine dâhil edilecek dijital kimlikler için ekleme ve silme prosedürü belirlenmesi,
- Bir personelin BT altyapısına erişimine müsaade edilmesi ve gerekli yetkilerin verilmesi öncesinde bir onay mekanizması sürecine tabi olması,
- Meydana gelebilecek olumsuz senaryolar neticesinde sorumlunun/sorumluların tespit

edilmesi için oluşturulan her bir dijital kimliğin birbirlerinden ayrıştırılarak benzersiz olması,

- Personele verilecek erişim yetkileri, genel ve kurumsal güvenlik politikalarına uygun olması ve görevler ayrılığı ilkesine uygun olması,
- BT altyapısına erişim yetkisi verilen personele sahip olduğu erişim hakları ve güvenlik kısıtlamaları konusunda sözlü/yazılı (*tercihen yazılı*) olarak bilgilendirme yapılması,
- Sebebi ne olursa olsun, görevi değişen veya kuruluş ile ilişkisi kesilen personelin dijital kimlik bilgilerinin güncellenmesi ve yetkilerinin düzenlenmesidir [62].

Kimlik yönetim süreci uygulanan bir kuruluş yapısı içerisinde izlenmesi gereken ve önerilen iş akış şeması bir örneği Şekil 3.4'te sunulmuştur.



Şekil 3.4. Kimlik yönetim süreci iş akış şeması [63]

3.2. Dizin Hizmeti ve Basit Dizin Erişim Protokolü

Zaman içerisinde ağlar daha geniş ve karmaşık bir hale geldiler. Ağ yapıları, çok fazla sayıdaki yazıcı, uygulama, veri tabanı, kullanıcı, sunucu vb. nesneleri barındırmaya başladılar. Karmaşık ağ yapılarında kullanıcılar nesnenin ismini bilmese dahi bu nesneleri tespit etmeye, yöneticiler ise ağı idame ettirebilmek için içerikleri değiştirmeye, yeni

kaynaklar eklemeye ve eskileri çıkartmaya ihtiyaç duydular. Bu genel ihtiyaçlarla beraber yerel ağlarda ve farklı konumdaki ağlarda yer alan kaynaklar, internet bağlantıları ile ağ teknolojileri arasındaki ayrımlar ortadan kalmış, sonuç olarak dizinlerin zaman içinde daha büyük ölçekli ve karmaşık talepleri karşılaması gerekliliği ortaya çıkmıştır. Kuruluşlar tarafından ortaya konan bu ihtiyaçlar dizin hizmetini ortaya çıkartmıştır [64].

Dizin hizmetinin karmaşık ağ yapıları kullanan kuruluşlarda ihtiyaç haline gelmesi ve belli bir standart getirilmesi gerekliliği üzerine 1988 yılında Uluslararası Telekomünikasyon Birliği (*ITU*) tarafından dizin hizmetlerinde istemci/sunucu arasında iletişim için OSI referans modelinde çalışan X.500 adı verilen dizin sistemi standardı geliştirilmiştir [65,66].

Dizin sistemlerinin başlangıcı olarak kabul edebileceğimiz X.500 dizin sistemi karmaşık yapıya ve buna bağlı ağır bir işlevselliğe sahipti. Bu nedenle X.500 protokolünün kullanıldığı yapılarda dizin hizmetlerine istemci ile sunumcu arasında erişim, okuma/yazma ve yönetim işlevlerinin interaktif olarak yapılabilmesi maksadıyla sadeleştirilerek tasarlanmış LDAP adı verilen Basit Dizin Erişim Protokolü geliştirilmiştir. LDAP, X.500 dizin sistemlerinin bir alt kümesiydi ve iletişimi kolaylaştırmak veya hızlandırmak için kullanılan bir iletişim protokolü olarak ortay çıktı. Zaman içerisinde daha basit ve hızlı bir yapıya sahip olan LDAP, TCP/IP üzerinde çalışması, esnek yapısı ve üretici bağımsız bir protokol olması sayesinde farklı dizin hizmeti sağlayan uygulamalarda tek başına kullanılan ortak bir endüstri standardı haline geldi [67,68].

3.2.1. Dizin hizmeti

Dizin hizmetini tanımlamadan önce dizin terimini tanımlamak gerekir. "*Basit olarak dizin terimi, insanlar, yerler ve işler gibi nesneler hakkında bilgileri tanımlamak için kullanılır. Bir dizin, kullanıcılara bu nesnelerin aranabilir, yararlı ve tekrar kullanılabilen bir şekilde mantıksal görünümünü vermektedir"* [64].

Dizinler günlük yaşamın bir parçasıdır ve birçok kişi farkında olsun veya olmasın çok farklı dizin türlerine aşinadır. Telefon rehberleri, öğretmenlerin not defterleri, adres defterleri her gün karşımıza çıkan en bilinen örneklerdir. Bu dizinler, insanların bulmak istedikleri şeyleri düzenlemekte ve tanımlamaktadır. Örnek olarak, bir öğretmenin öğrencilerinin notlarını kaydettiği not defteri verilebilir. Not defteri içerisinde öğrencilerin

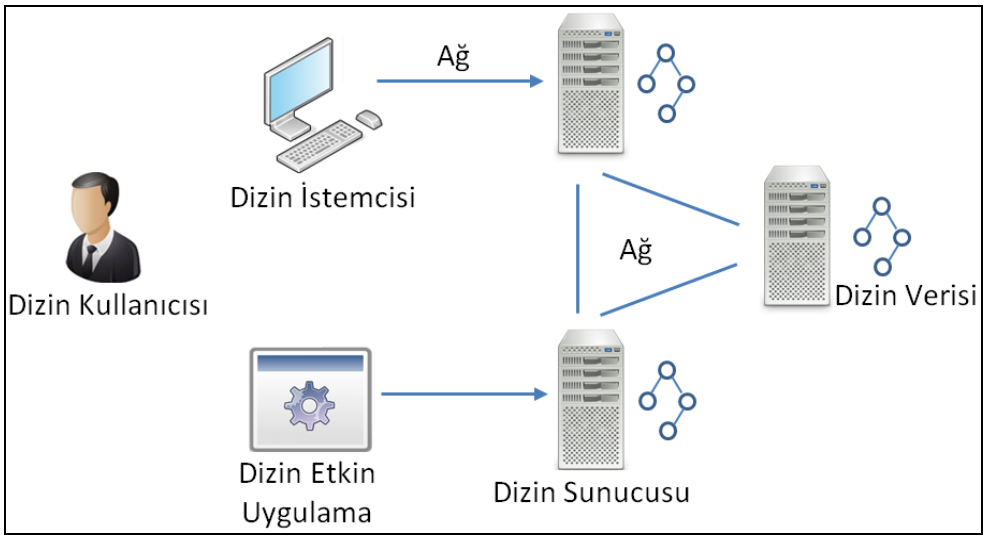
numaraları, adları, soyadları, yazılı ve sözlü notları bulmaktadır. Her öğrencinin kimlik bilgileri ile diğer tüm bilgileri eşleştirilmiştir. Bu not defteri, isimler üzerinden kolayca öğrenciye ait notlara ulaşabilmemizi sağlayan basit bir dizindir. Ancak bu dizin, isimlere dayalı olarak tek yönlü bir kullanım sağlamaktadır. Bu tür bir dizin içerisinde bir herhangi bir not bilgisinden söz konusu öğrencinin ismine ulaşmak oldukça zordur. Tek bir bileşen üzerine yoğunlaşan bu tür basit dizinlere *çevrim dışı* dizin adı verilmektedir [69].

Bilgisayar ve ağ dünyasındaki dizinler *çevrim içi* dizin olarak adlandırılmaktadır [69]. Bir işletim sistemi dizini, basit bir dizinden oldukça farklıdır. Bilgilerin saklamasının yanı sıra kullanıcıların bu bilgilere erişebilmesi için bir mekanizma sunmaktadır. Ağ dizini, ağdaki tüm nesnelerin listesini göstermek ve kullanıcıların erişimi için bir yöntem sunmaktadır. Ayrıca bir ağ dizini, ağ nesneleri ve bunların ilişkilerini bir yapı olarak görüntüleyerek kullanıcının tüm bunları kontrol etmesini sağlamaktadır [64]. Çevrim içi dizinler ile çevrim dışı dizinler arasında birçok ayırt edici fark mevcuttur. Bunlardan en temel olanları;

- Çevrim içi dizinler dinamiktir,
- Esnektir,
- Güvenlik sağlanabilir,
- Kişiselleştirilebilir [69].

Yazılım, donanım, süreçler, politikalar ve yönetimsel prosedürleri kapsayan dizindeki bilgilerin, dizin kullanıcıları için kullanılabilir hale getirilmesi *Dizin Hizmeti* olarak tanımlanmaktadır. Dizin hizmeti, bir işlemi gerçekleştirmek için birlikte çalışan karmaşık bileşenler sistemdir. Şekil 3.5'de örneği sunulan bir dizin hizmeti en az aşağıdaki bileşenleri içerir;

- Dizinde yer alan bilgiler,
- Bu bilgiyi saklayan sunucu yazılımları,
- Bilgilere erişimde kullanıcılar ve varlıklar adına hareket eden istemci yazılımları,
- Söz konusu istemci ve sunucu yazılımlarının üzerinde çalıştığı donanımlar,
- İşletim sistemleri ve aygıt sürücüleri gibi destek yazılımlar,
- Sunucuları istemcilerle, diğer sunucularla ve tüm nesnelerle bağlayan ağ altyapısı,
- Politikaların saklandığı dizine erişebilen ve güncelleyebilen politika yöneticisi,
- Dizin hizmetinin idamesini sağlayan ve izleyen prosedürler,
- Dizin hizmetini idame ettirmek ve izlemek için kullanılan yazılımlar [69].



Şekil 3.5. Dizin hizmeti bileşenleri [69]

3.2.2. Kullanım alanlarına göre dizin hizmetleri Dizin hizmetleri kullanım alanlarına ve amaçlarına göre farklılıklar gösterirler. Dizin hizmetinin farklı türleri aşağıdaki başlıklar altında incelenebilir;

Uygulamaya Özel Dizin Hizmeti: Bir uygulamayla birlikte gömülü bir şekilde gelmektedir. Bu tür dizin hizmetleri, uygulamaların bir parçası olarak görülür ve tek başına bir dizin hizmeti olarak değerlendirilmez. Örnek olarak, IBM Lotus'un isim ve adres defteri, Micrososft Exchange'in e-posta adres defteri verilebilir.

Ağ İşletim Sistemi (NOS) Tabanlı Dizin Hizmeti: Novell eDirectory (NDS), Microsoft Aktif Dizin, Sun Microsystem Ağ Bilgi Hizmeti (NIS) gibi dizin hizmeti uygulamaları örnek olarak verilebilir. Bu uygulamalar NOS'un ihtiyaçlarını karşılamak için tasarlanmışlardır.

Amaca Özel Dizin Hizmeti: Bunlar bir uygulamaya bağlı değildir. Ancak dar ve belirli bir amaç için tasarlanmış olup, genişletilebilir değildirler. Örnek olarak İnternet Alan İsim Sistemi verilebilir.

Genel Amaçlı Standartlara Dayalı Dizin Hizmeti: Bu uygulamalar, geniş bir yelpazede ihtiyaçları karşılamak için geliştirilmiştir. Örnek olarak LDAP Dizin Hizmeti ve X.500 tabanlı dizin hizmeti uygulamalarını verebilir [69].

3.2.3. Dizin hizmetinin sağladığı görevler

Nesneleri bulmak

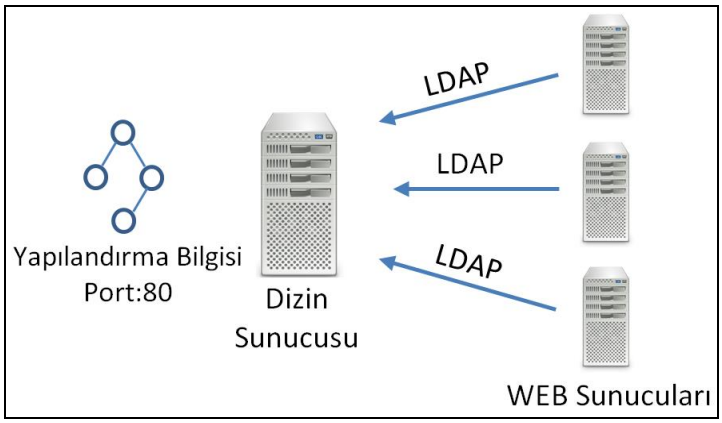
Dizinler günlük yaşantımız içerisinde genellikle bulma sorununu çözmek amacıyla kullanılmaktadır. Kütüphanede aranan bir kitabın yerini bulmak veya iletişim kurmak istediğiniz kişinin telefon numarasını bulmak bu duruma örnek verilebilir. Eğer aranan şeyin kolayca bulunması amaçlanıyorsa düzenli bir şekilde organize edilmiş dizinler kullanılmalıdır [69].

Bir nesnenin bulunması, çevrim içi dizinler içinde yerine getirilmesi gereken önemli bir görevdir. Ancak çevrim içi dizinler, bir nesnenin bulunması için, çevrim dışı dizinlere göre çok daha gelişmiş yeteneklere sahiptir. Çevrim içi dizinlerde birden fazla kritere göre bulunmak istenen nesneye ulaşılabilmektedir [69]. Örneğin bir Microsoft Exchange adres defterinde ilgili kişinin adıyla, soyadıyla, e-posta adresiyle, telefon numarasıyla vb. kriterlerden biri veya birkaçı kullanılarak arama yapılması durumunda, dizinde ilgili kişi hakkında girilmiş olan tüm bilgilere erişim sağlanabilmektedir.

Nesneleri yönetmek

Çevrim içi dizinler, çevrim dışı dizinlerden farklı olarak bilgi yönetimine ihtiyaç duymaktadırlar. Çevrim içi dizinlerin yönetilmesi gerekir ve nesneler için merkezi bir depolama imkânı sağlayan dağıtılmış bir ortamda yönetim konusu önemli bir yere sahiptir. Yönetim işi maliyetlidir ancak merkezi olarak yönetilen bir dizin esasen bu hizmetin maliyetlerini azaltmaya yardımcı olmaktadır.

Merkezi bir dizin yönetimi anlayışında, farklı uygulamaların kendi dizinlerinde tuttuğu bilgilere tek bir merkezden bir dizin hizmeti sunucusu üzerinden erişilmesi, yönetim işini oldukça kolaylaştıracak ve hızlandıracaktır. Bu sayede sunucunun uzaktan yönetimi mümkün olacak ve sunucunun yapılandırma özelliklerine bağlı olarak ağ üzerinde her yerden ulaşılabilecektir. Farklı dizin hizmeti veren sunucuların bir küme yapısı içerisinde yapılandırılması, farklı dizinlerin kendi aralarında paylaşımda bulunmalarını sağlamaktadır. Şekil 3.6'da bu yapıya bir örnek verilmiştir [69].



Şekil 3.6. Örnek bir sunucu küme yapısı

3.2.4. Dizin hizmetinin doğuşu

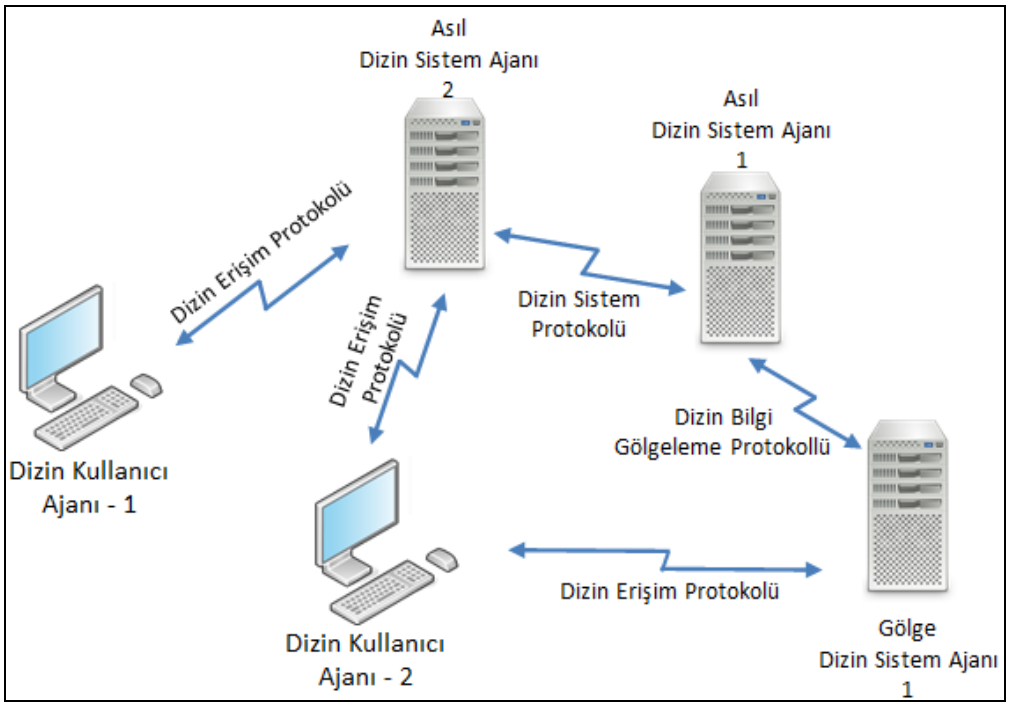
1980'lerin ortasında iki farklı standart kuruluşu birbirinden bağımsız olarak uluslararası sınırların ötesinde kuruluşlar ve sistemler için kullanılabilecek bir dizin hizmeti geliştirmek üzere çalışma başlatmışlardır. Bunlardan biri daha sonrasında adını Uluslararası Telekomünikasyon Birliği (ITU) olarak değiştirmiş olan "Uluslararası Telgraf ve Telefon Danışma Komitesi" (CCITT), kendisine üye kuruluşlar tarafından, geniş çaplı telefon rehberleri ve tutulan çok sayıdaki e-posta adreslerinin içerisinde arama yapabilmek amacıyla kullanmak üzere bir dizin yaratılması talebi üzerine çalışmalarına başlamıştır. Diğeri, Uluslararası Standardizasyon Kuruluşu (*ISO-International Organization for Standardization*), aynı zamanlarda OSI (*Open System Interconnection*) referans modeline göre çalışan ağlar ve uygulamalar için bir isim servisi (*Bir isim hizmeti ağ nesneleri hakkında bilgi sağlar-DNS buna benzer bir örnektir*) olarak hizmet verecek bir dizin hizmeti yaratma çalışmalarını yürütmekteydi [69].

Dizin hizmetleri üzerine yapılan birbirinden bağımsız bu iki çalışma nihayetinde birleştirilerek X.500 adı verilen dizin hizmetinin teknik tanımlaması ortaya çıkmıştır. İlk X.500 dizin hizmeti standardı 1988 yılının sonlarında onaylanmış ve 1990 başlarında CCITT tarafından yayınlanmıştır [69].

3.2.5. X.500 dizin hizmeti

CCITT tarafından yayınlanan teknik tanımlama, X.500 ve bu yapı içerisinde kullanılan diğer ISO standartlarından oluşan bir dizi öneriden oluşmaktadır. X.500 dizin hizmeti, bir örneğinin Şekil 3.7'de sunulduğu gibi Dizin Erişim Protokolü (*DAP- Directory Access*

Protocol), Dizin Sistem Protokolü (*DSP-Directory System Protocol*), Dizin İşlevsel Bağlama Protokolü (*DOP-Directory Operational Binding Protocol*), Dizin Kullanıcı Ajanı (*DUA-Directory User Agent*), Dizin Sistem Ajanı (*DSA-Directory System Agent*) ve Dizin Bilgi Gölgeleme Protokollerinin (*DISP- Directory Information Shadowing Protocol*) dâhil olduğu birçok protokolün birlikteliğine dayanmaktadır.



Şekil 3.7. X.500 dizin hizmeti ana bileşenleri

X.500 Dizin hizmeti modelinin gücü esnek ve eksiksiz bilgi modeline, çok yönlülüğüne ve açıklığına dayanır. X.500, herhangi bir satıcı tarafından kontrol edilmeyen, bir teknolojiye, ağ uygulamasına veya herhangi bir özel işletim sistemine bağımlılığı olmayan açık bir standarttır [69].

X.500 dizin hizmetinin ortaya çıkışından sonraki ilk yıllarda uygulamada bazı önemli kusurları bulunduğundan istenileni tam olarak verememiştir. X.500 dizin hizmeti geliştiricileri tarafından dağıtık yapılara adaptasyon için yapılan çalışmalarda, X.500 dizin hizmetinde, çoğu tam olarak tespit edilemeyen bazı önemli engellerle karşılaşılmıştır. Bu sorunlardan biride dizin hizmeti içerisindeki yararlı verinin elde edilmesi ve korunmasındaki zorluklardır. Tüm bunlara ek olarak, X.500 standartlarının karmaşıklığı ve birlikte çalışmalarının zorluğu nedeniyle, farklı X.500 uygulamalarının birlikte çalışabilirliğinin mümkün hale gelmesi uzun zaman almıştır [69].

X.500 standardı OSI ağ protokollerine dayalı çalışmak üzere tasarlanmıştır. OSI modeli tasarlanırken amaç, ileriki zamanlarda OSI modelinin geleceğin ağ protokolü olarak TCP/IP ağ modelinin yerini almasıydı. Ancak zaman içerisinde TCP/IP modeli basitliği, hızı ve düşük maliyeti gibi pek çok üstünlüğü nedeniyle tercih edilmiştir. X.500 geliştiricileri bu sorunu çözmek adına X.500 modelinin doğrudan TCP/IP üzerinden çalışmasını sağlayan bir eşleşme tanımlamışlardır. Ancak bu çözüm bile X.500'ün kökenlerinden kaynaklanan sorunlara tam olarak çözüm olmamış ve tam anlamıyla başarıya ulaşmasını engellemiştir [69].

Tüm bu olumsuzlukların dışında, bağımsız kuruluşlar kendi imkânlarıyla, hiçbir destek almadan ana bilgisayarlarını ve hizmetlerini adım adım yaymasıyla, internetin aşağıdan yukarıya doğru hızlı bir şekilde büyümesini sağlamışlardır. Buna karşılık, geniş yapıya sahip kamu hizmet sağlayıcıları düşünülerek tasarlanmış olan X.500 yukarıdan aşağıya doğru geliştirilmiştir. X.500 modelinin yukarıdan aşağıya doğru gelişimi, geçerli internet kültürüne egemen olmasını imkânsız kılmıştır [69].

3.2.6. Basit dizin erişim protokolünü

X.500 dizin erişim protokolü yani DAP büyük, karmaşık ve uygulaması zor yapısı nedeniyle çoğu uygulamada düşük performansa neden olmaktaydı. Çoğu potansiyel dizin hizmeti kullanıcısı sıradan masaüstü bilgisayarlara sahipti ve X.500 kullanımıyla beraber DAP kaynaklı yavaşlıktan etkilemişlerdi. DAP'ın neden olduğu sorunları çözmek amacıyla 1990 yılında, masaüstü bilgisayarların doğrudan TCP/IP üzerinden iletişim kurduğu ve X.500 DAP ile istemci arasında yer alan bir ara sunucu kullanımı mantığına dayanan iki farklı protokol geliştirilmiştir. Bu protokollerden biri RFC 1202 olarak tanımlanan [70] Dizin Yardım Hizmeti (DAS- Directory Assistance Service), diğeri ise RFC 1249 [71] olarak tanımlanan DIXIE'dir. Her iki protokolde başarılı olmuştur. Ancak geçiş sürecinin daha kolay olması nedeniyle X.500 dizin hizmetine erişim için istemci/istemci/sunucu mimarisi kullanan bir X.500 dizin hizmeti ara yüzü olan DIXIE tercih edilmiştir [69].

DIXIE ve DAS uygulamalarının X.500 için daha basit erişim sunmalarının ardından, İnternet Mühendisliği Görev Gücü (*IETF*) OSI dizin hizmeti çalışma grubunda yer alan Wengyik Yeong, Steve Kille, Colin Robbins ve Tim Howe tarafından tam donanımlı basit bir dizin erişim protokolü geliştirme çalışmalarına başlanmıştır. Bu LDAP için atılmış ilk adımdır. İlk LDAP nitelikleri 1997 Temmuz ayında RFC 1487 olarak tanımlandı ve

yayınlandı. Ancak LDAP'ın geniş kapsamlı kullanılan ilk modeli RFC 1777 [72] olarak tanımlanan ikinci sürüm LDAPv2'dir [69].

LDAP, ağır X.500 DAP protokolünü dört önemli alanda basitleştirmiştir;

Kodlama: Uygulamasını kolaylaştırmak amacıyla LDAP mesajlarının kodlamasında X.500 kodlama kurallarının bir alt kümesi kullanılmaktadır [69].

İşlevsellik: LDAP, DAP'ın gereksiz ve az kullanılan özelliklerinin çıkartılarak, DAP'ın işlevlerinin çoğunu çok daha düşük maliyetlerle karşılayabilmektedir. LDAP ile istemci ve sunucu uygulamaları basitleştirilmiştir [69].

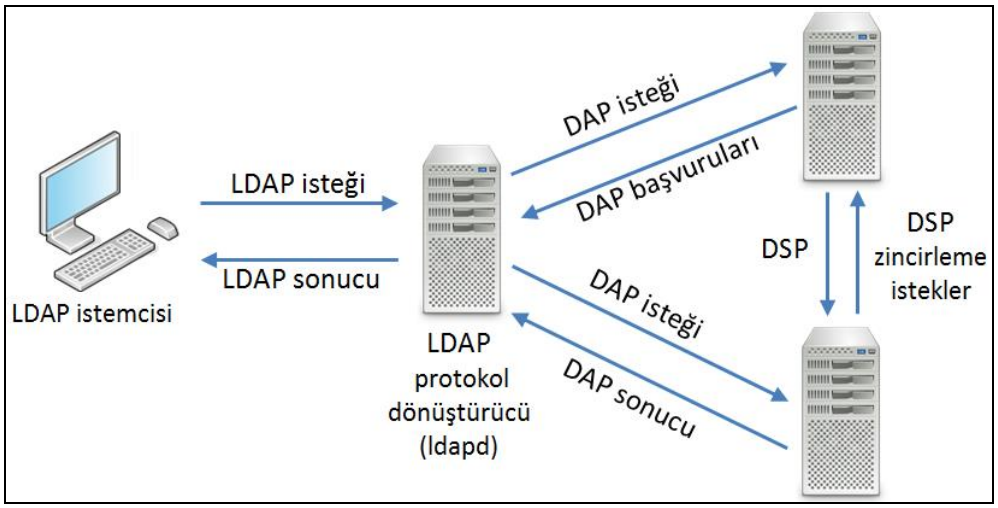
Veri Sunumu: LDAP'ta veri elemanlarının çoğunun basit metin dizeleri halinde taşınması sayesinde uygulamalar basitleştirilmiş ve performans arttırılmıştır. Verimlilik için metin dizeleri ikili kodlanmış mesajlar içinde gönderilmektedir [69].

Taşıma: Çok katmanlı olması nedeniyle ağırlaşan OSI ağ modeli yerine LDAP doğrudan TCP/IP üzerinde çalışmaktadır. Uygulama basitleştirilmiş, performansı arttırılmış ve OSI ihtiyacı ortadan kaldırılmıştır. Bu sayede LDAP dizelerinin dağıtımı basitleşmektedir [69].

Bağımsız dizin hizmeti olarak LDAP

LDAP ilk başta yalnızca X.500 tabanlı dizin hizmetlerinin ön tarafında iletişimi sağlamak amacıyla kullanılmaktaydı. İlk LDAP uygulaması Michigan Üniversitesinde geliştirilmiştir. Küçük ve hızlı olmasının yanında birçok bilgisayar platformları üzerinde çalışabiliyordu. Geliştirilen söz konusu LDAP'ın en önemli özelliği, C dili ile hazırlanan basit bir API yardımıyla, LDAP tüm istemcilere uygulanmış ve LDAP istemci uygulamasını dağıtmak için kullanılmıştır. Daha sonrasında RFC 1823 [73] olarak tanımlanan LDAPv2 istemci API'si yayınlanarak bir standart haline gelmiştir [69].

1995 yılının başlarında Michigan Üniversitesindeki LDAP geliştirme grubu tarafından, Michigan Üniversitesi hizmetleri için dizin erişim istatistikleri üzerinde yapılan incelemede X.500 dizinine gelen erişimlerinin %99'dan fazlasının LDAP üzerinden geldiği tespit edilmiştir. Çoğu X.500 dizini için geçerli olan bu istatistik bilgisinin elde edildiği ve yaygın olarak kullanılan LDAP mimarisi Şekil 3.8'de gösterilmiştir [69].

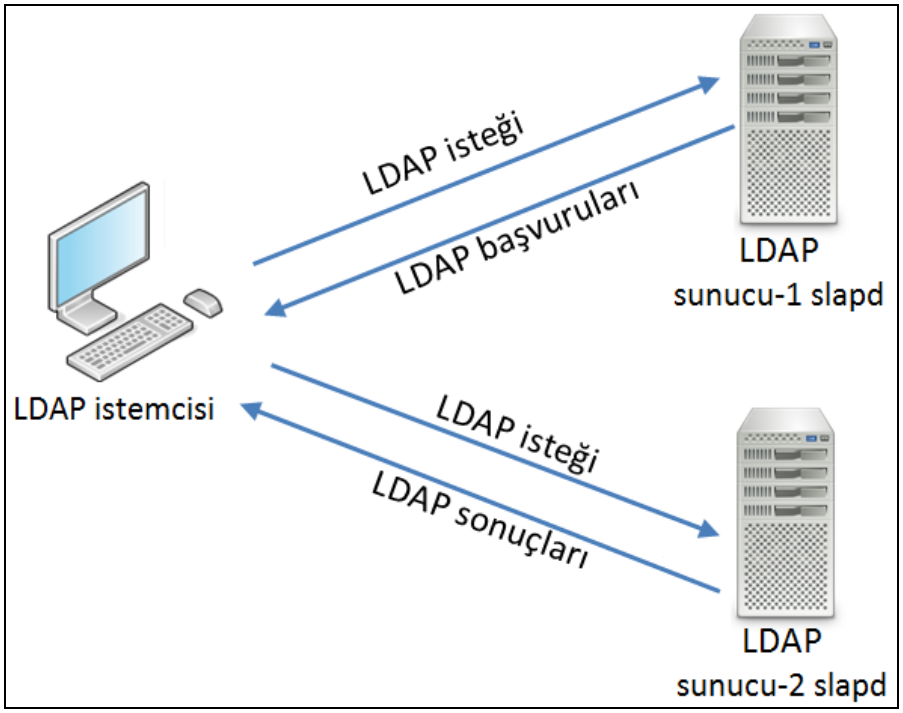


Şekil 3.8. İstatiksel incelemesi yapılan LDAP dizin sistemi mimarisi

ldapd sunucuları, DAP isteklerinin LDAP isteklerine dönüştürülmesi ve X.500 sunucularından DAP sonuçlarının LDAP sonuçları olarak dönüştürülmesi işlemini yerine getirmekteydi ve bu işlemler *ldapd* sunucularında yüksek kaynak kullanımına neden olmaktaydı. Bunun sonucu olarak X.500 dizin hizmetinin tümüne olan ihtiyaç sorgulanmaya başlanmış ve neticesinde tek başına çalışacak LDAP hizmeti kavramı doğmuştur. X.500'ün en iyi bölümlerini alan ve tek başına çalışan bu LDAP uygulamasının arka planda koşan bu yeni servisi *slapd* olarak adlandırılmıştır. *slapd'a,* ara bağlantılı mesh ağ yapı desteği bir uzantı olarak LDAPv2 protokolünde eklenmiştir. X.500 dizin hizmetinde erişim için ağır bir görevi olan bu rol, tam bir dizin hizmeti temelini oluşturacak şekilde daha kullanışlı ve basit bir rol olarak yapılandırılarak yenilenen LDAP'a aktarılmıştır. Michigan Üniversitesinin LDAP yazılımı, tüm bu yenilemelerin ardından *slapd'*da dâhil olmak üzere LDAP 3.2 sürümü ile 1995 Aralık ayında yayınlanmıştır [69]. Yenilenmiş bu LDAP sistem mimarisi Şekil 3.9'da sunulmuştur.

LDAP için kısa bir özet yapacak olursak;

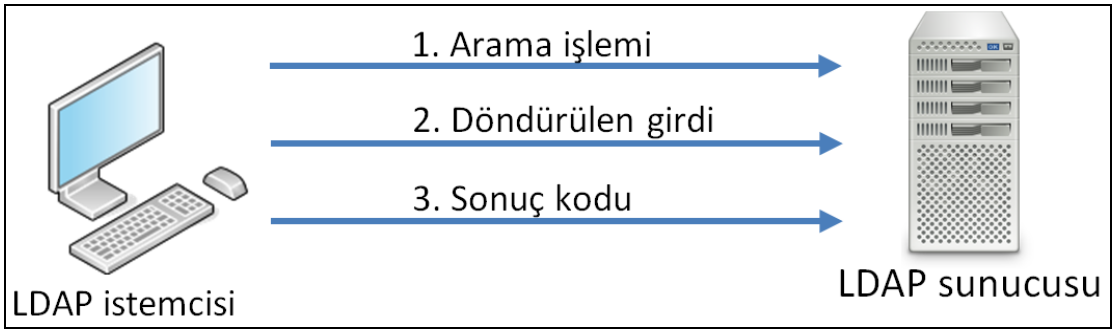
- LDAP protokolü, bir standarttır ve dizin kullanımı için bir kılavuz görevi görür,
- Dizin hizmetine erişmek için genişletilebilir dizin erişim protokolünü kullanır,
- Dizin verilerini kullanmak ve düzenlemek için bir isimlendirme modeli sunar,
- Dizin verilerine yetkisiz erişimleri engellemek için bir güvenlik modeline sahiptir,
- LDAP dizin hizmeti uygulamalarının ticari ve ücretsiz olanları mevcuttur,
- LDAP API'leri LDAP istemci uygulamalarının geliştirilmesi için kullanılmaktadır [69].



Şekil 3.9. Slapd entegrasyonu sonrası LDAP sistem mimarisi

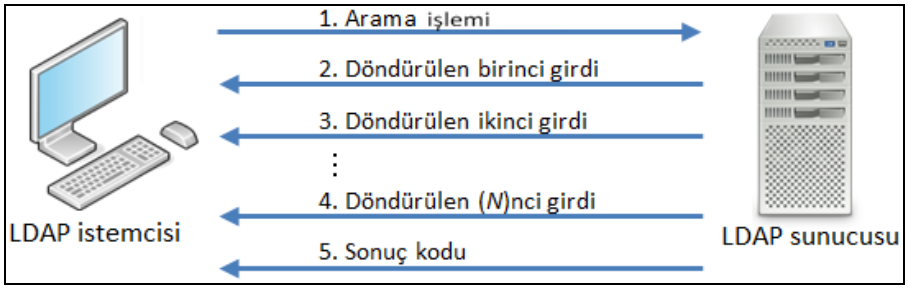
LDAP protokol işlemleri

LDAP mesaj odaklı bir protokoldür. İstemci, istek içeren bir LDAP mesajını oluşturur ve sunucuya gönderir. Sunucu isteği işler ve sonuçları içeren bir veya daha fazla LDAP mesajını istemciye geri gönderir. Örneğin bir LDAP istemcisi bir girdiyi dizinde arayacağı zaman sunucuya bir LDAP arama istek mesajı gönderir. Bu mesaj istemcide oluşturulmuş eşsiz bir mesaj kimliği içerir. Sunucu, istemci LDAP mesajını alınca veri tabanından girdiyi alır ve istemciye bir LDAP mesajında gönderir. Ayrı bir LDAP mesajıyla da sunucuya bir sonuç döndürür. Sunucudan istemciye giden tüm yanıtlar istemci tarafından oluşturulmuş orijinal mesaj kimliği ile tanımlanır. Bu etkileşim Şekil 3.10'da sunulmuştur.



Şekil 3.10. İstemci ve LDAP sunucusu arasında tek girdi transferi etkileşimi

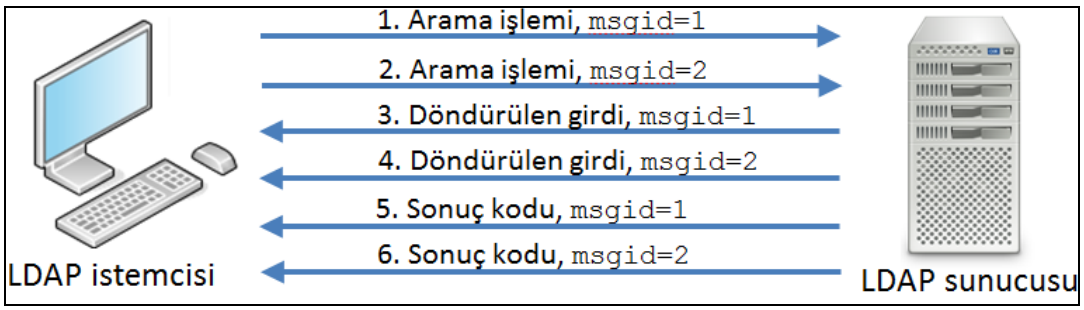
Eğer istemcinin aramaları sonucu birden fazla girdi bulunmuşsa, bu girdiler her biri için farklı olmak üzere bir dizi LDAP mesajı ile gönderilir. Her bir girdi, bir metin dizesi olarak taşınan LDAP mesajında seçkin ad (*DN- Distinguished Name*) olarak adlandırılan benzersiz bir isime sahiptir. Arama sonuçlarını içeren girdiler, arama işlemi için genel sonuç içeren bir mesaj ile sonlandırılır. Bu etkileşim Şekil 3.11'de gösterilmiştir [69].



Şekil 3.11. İstemci ve LDAP sunucusu arasında çoklu girdi transferi etkileşimi

LDAP protokolü mesaj tabanlı olduğundan, istemciye aynı anda birden fazla istek gönderme olanağı sunar. Normalde bir istemcinin aynı anda iki istek göndermesi sorun olabilir. Ancak istemcinin gönderdiği her istek için farklı olarak ürettiği mesaj kimliği sayesinde döndürülen sonuçlar mesaj kimlikleriyle etiketlenerek sıraya konulmakta ve bu sayede karmaşanın önüne geçilmektedir.

Şekil 3.12'de bir istemci aynı anda iki arama isteği gönderdiği görülmektedir. Bu durumda sunucu her iki operasyonu gerçekleştirerek istemciye sonuçları dönmektedir. Sunucu iki mesajın son sonuç kodlarını gönderir ve işlemi sonlandırır. Ancak sonuç kodlarını döndüğünde, ilk arama isteğinin sonuç kodu en son dönmektedir. Bu sayede süreç, ilk gönderilen arama isteğinin sonuç kodunun en son gönderilmesi ile sorunsuzca sonlandırmaktadır. LDAP yazılım geliştirme araçları bu işlemi otomatik olarak düzenlediklerinden geliştiricilerin ayrıca bir işlem yapmalarına gerek yoktur [69].



Şekil 3.12. İstemci tarafından gönderilen çoklu LDAP arama isteği etkileşimi

LDAP üç kategoriye ayırabileceğimiz dokuz temel protokol işlemine sahiptir.

Sorgulama İşlemleri: Arama ve karşılaştırma işlemleri, dizine sorgu isteklerinin gönderilmesi sağlamaktadır.

Kimlik doğrulama ve kontrol işlemleri: Bağlantı kurma işlemi bir istemcinin kimlik ve kimlik doğrulama bilgilerini sayesinde dizin üzerinde kimliğini tanımlamasını sağlamaktadır. Bağlantı kesme işlemi, istemcinin oturumunu sonlandırmasını sağlamaktadır. Bırakma işlemi ise istemcinin bir operasyonun daha önce talep ettiği sonuçları ile artık ilgilenmediğini belirtmesini sağlamaktadır [69].

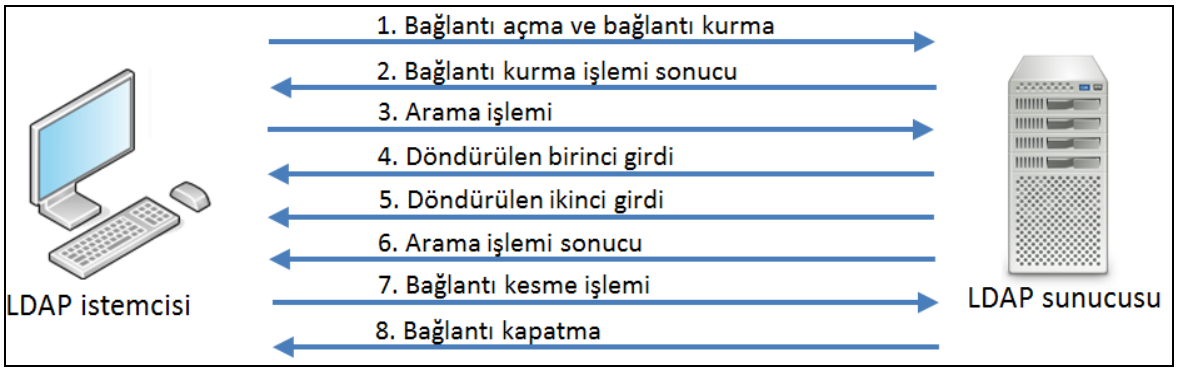
Güncelleme İşlemleri: Ekleme, silme, değiştirme ve seçkin ad değiştirme işlemleri sayesinde dizin içerisinde yer alan bilgilerin güncellenmesine müsaade etmektedir[69].

LDAP sahip olduğu dokuz temel protokol işlevinin yanında LDAPv3 tasarımı ile beraber üç kategoride ele alabileceğemiz (*LDAP uzatılmış işlemler, LDAP kontrolleri, Basit kimlik doğrulama ve güvenlik katmanı*) genişletilebilirlik özelliğini de kazanmıştır [25].

LDAP işleyişi

Şekil 3.13'de sunulmuş olan tipik LDAP istemci/sunucu işleyişi için örnek bir senaryonun uygulama adımları aşağıda açıklanmıştır.

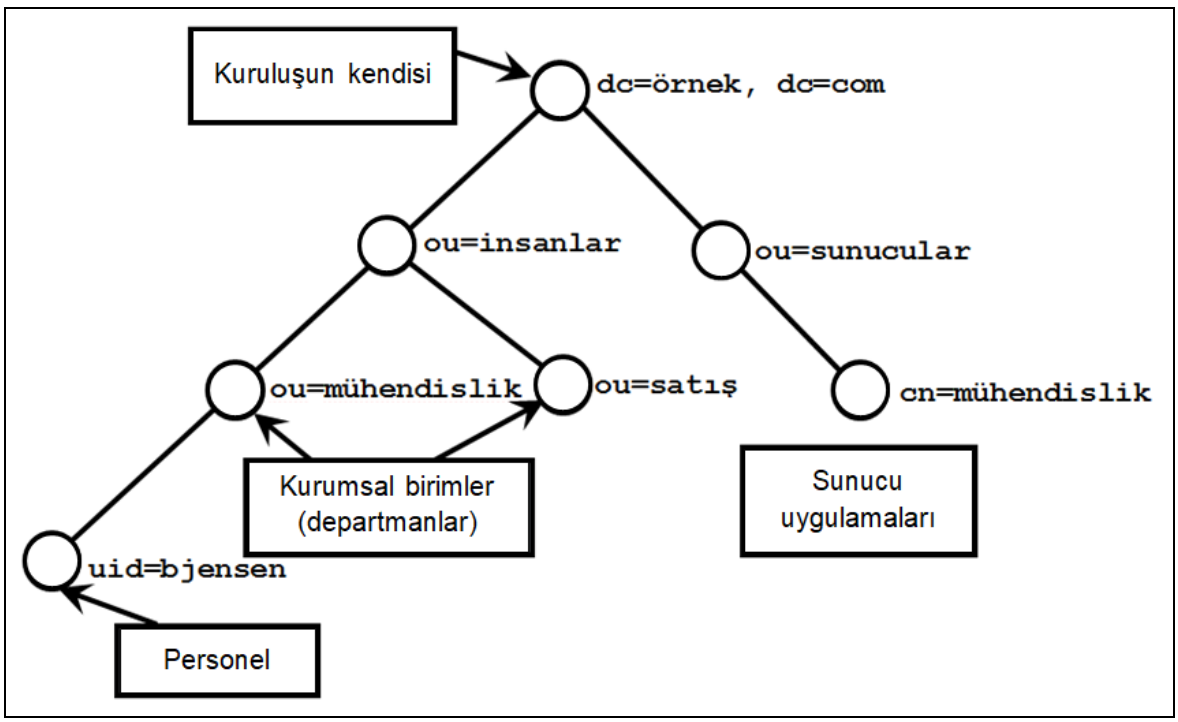
İstemci, LDAP sunucusuna TCP bağlantı açar ve bir bağlantı kurma işlemi talep eder. Bu bağlantı kurma işlemi, kimlik doğrulaması talebinde bulunan istemcinin kimlik doğrulmasında kullanılan kimlik doğrulama bilgilerinin dizin girdi adını içermektedir. Kimlik doğrulama bilgileri basit parolalar veya sayısal sertifikalarda olabilmektedir. Ardından dizin, istemcinin bağlantı kurmasına izin vermek için parolasını veya sayısal sertifikasını kontrol eder ve doğru ise bu bilgileri onaylar. Başarılı doğrulamanın ardından dizin, istemciye başarılı sonucunu döner. İstemci, başarılı kimlik doğrulama işleminin ardından arama isteğini gönderir. Sunucu, iki eşleşen girdi ile sonuçlanan bu isteği işler ve bir sonuç mesajı gönderir. Sonucu alan istemci, sunucu ile arasındaki bağlantıyı sonlandırmak için bir bağlantı kesme isteği gönderir ve sunucu bağlantıyı sonlandırır [69].



Şekil 3.13. Normal bir LDAP mesaj alışverişi

LDAP girdileri nitelikleri ve değerleri

Dizin içerisindeki bir nesne hakkındaki bilgi yığınını ifade eden temel bilgi birimi, girdi olarak tanımlanır. Girdiler çoğunlukla bir kişiye ait bilgiler gibi gerçek dünyadaki nesleri açıklamaktadır. Ancak bu bir zorunluluk değildir. Tipik bir dizin tarafından sunulan örgütsel yapıda, insanlara, departmanlara, sunuculara, yazıcılara ve diğer gerçek dünya nesnelerine karşılık gelen binlerce girdi olabilir [69]. Şekil 3.14'de gerçek dünyadaki nesnelere karşılık gelen, tipik bir dizin örgütsel yapısının bir bölümü sunulmaktadır.



Şekil 3.14. Tipik dizin yapısından bir bölüm

Her bir dizin girdisi bir seçkin ada sahiptir. Şekil 3.14'de DN *dc=example, dc=com* olan bir örgütsel yapı gösterilmiştir. Bir girdi, her biri belirli bir nesne özelliğini tanımlayan bir dizi nitelikten meydana gelmiştir. Her bir nitelik, bir türe ve bir veya daha fazla değere sahiptir. Buradaki tür terimi, gerçek verilerden meydana gelen nitelik ve değer içerisinde yeralan bilgiyi tanımlar. Bir kişiye ait ad, soyad, telefon numarası ve e-posta adresi niteliklerini tanımlayan girdi Şekil 3.15'de sunulmuştur [69].

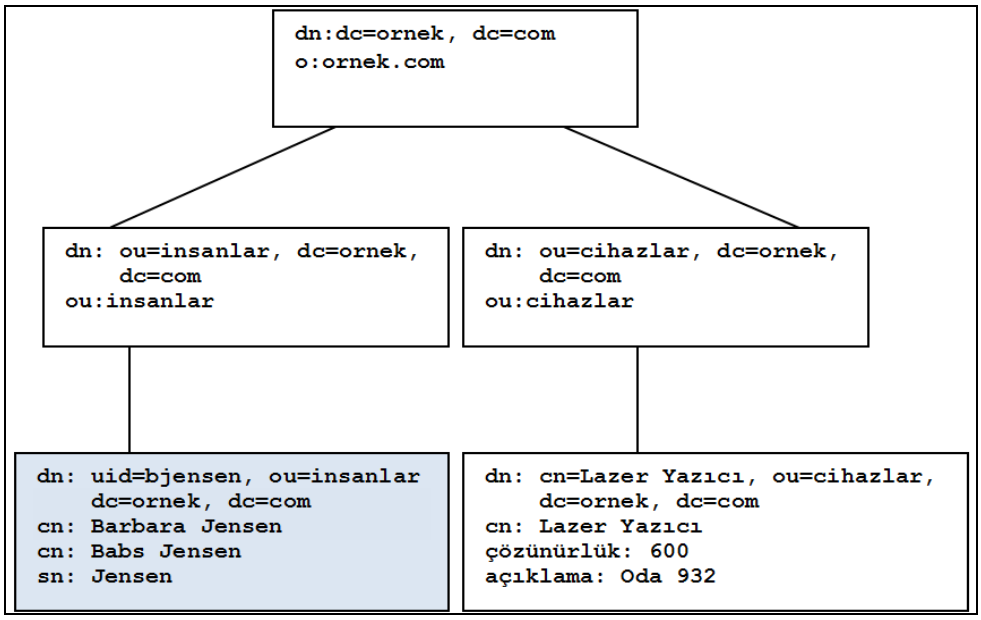
Nitelik Türü	Nitelik değerleri
cn:	Barbara Jensen Babs Jensen
sn:	Jensen
Telefon Numarası:	+1 408 555 1212
e-posta:	babs@ornek.com

Şekil 3.15. Bir dizin girdisinin sunduğu nitelikler, türler ve değerler

LDAP isimlendirme modeli

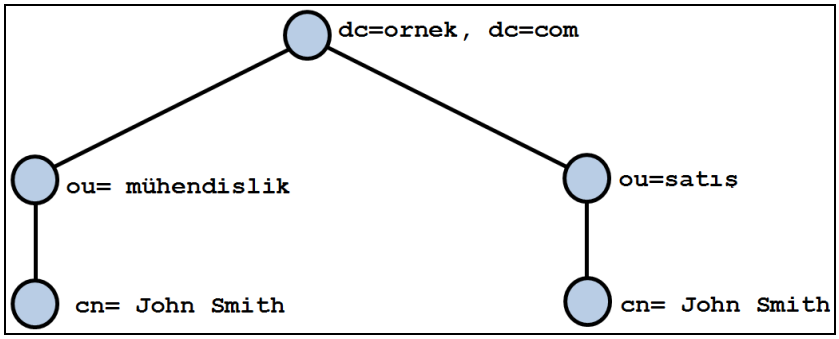
LDAP isimlendirme modeli, başvurulan ve düzenlenen verileri tanımlar. Başka bir deyişle, özgün yapı taşları dışında kalan ve oluşturulabilen dizin girdisi yapı türlerini tanımlamaktadır. Bu süreçte, mantıksal yapı içerisindeki girdiler düzenlenir ve sonrasında isimlendirme modeli yapı içerisinde başvurulan herhangi belirli dizin girdisini belirtir. Yönetilmesi kolay olan bir yöntemle, esneklik sağlayan LDAP isimlendirme modeli, dizin içerisine verilerin yerleştirilmesini sağlamaktadır. Örneğin kuruluş içerisinde yer alan tüm çalışanları tanımlayan girdileri tutmak için oluşturulan bir havuz yaratılabilir. Veya kuruluş şubelerinin coğrafik konumları yansıtacak bir şekilde bir dizin oluşturulabilir.

LDAP isimlendire modelinde girdiler, ağaç yapısının tersine göre düzenlenmektedir. İncelendiğinde *dc=ornek, dc=com, ou=insanlar* ve *ou=cihazlar* girdisi tüm verileri/nitelikleri ve içerisinde yer aldıkları alt düğümleri içerdiği görülmektedir. Şekil 3.16'da *uid=bjensen, ou=insanlar, dc=ornek, dc=com* işaretlenmiş alandaki dizin girdisinin adıdır. Dizin girdisi adı soldan sağa doğru okunduğunda ağaç yapısı içerisinde aşağıdan yukarı doğru oluşturulduğu görülmektedir [69].



Şekil 3.16. Tipik bir LDAP dizin bölümü

Dizin içerisindeki bir girdiye başvurmak için kesinliğin sağlanması gerekir ve bu nedenle isimlendirme modeli, herhangi bir girdiye eşsiz bir isim verilmesine ihtiyaç duyar. LDAP içerisinde, girdinin seçkin adı, en soldaki bileşeni *Göreceli Seçkin Ad* (*RDN- Relative Distinguished Name*) olarak adlandırılır. Doğrudan ortak bir kapsayıcı paylaşan bir dizi girdilerde her bir RDN eşsiz olmalıdır. Bu kural, yinelemeli olarak tek bir dizin ağacına uygulandığında hiçbir girdinin DN ile aynı olmamasını sağlar. Aynı ada sahip iki girdi eklenmeye çalışıldığında, dizin hizmeti ikinci girdinin eklenmesi girişimini engelleyecektir. Linux ve Windows dosya sistemlerinde aynı klasör içerisine mevcut bir dosyanın adı ile aynı isimde başka türdeş bir dosya yaratılmaya çalışıldığında bu girişimin reddedilmesi örnek verilebilir. RDN'ler, doğrudan ortak bir kapsayıcı paylaştıkları zaman eşsiz olmaları gerekmektedir. Şekil 3.17'de iki farklı alt ağaç içerisinde yer alan ve aynı olan *cn=John Smith* RDN'i görülmektedir ve bu yapı bahsedilen kurala uygundur [69].

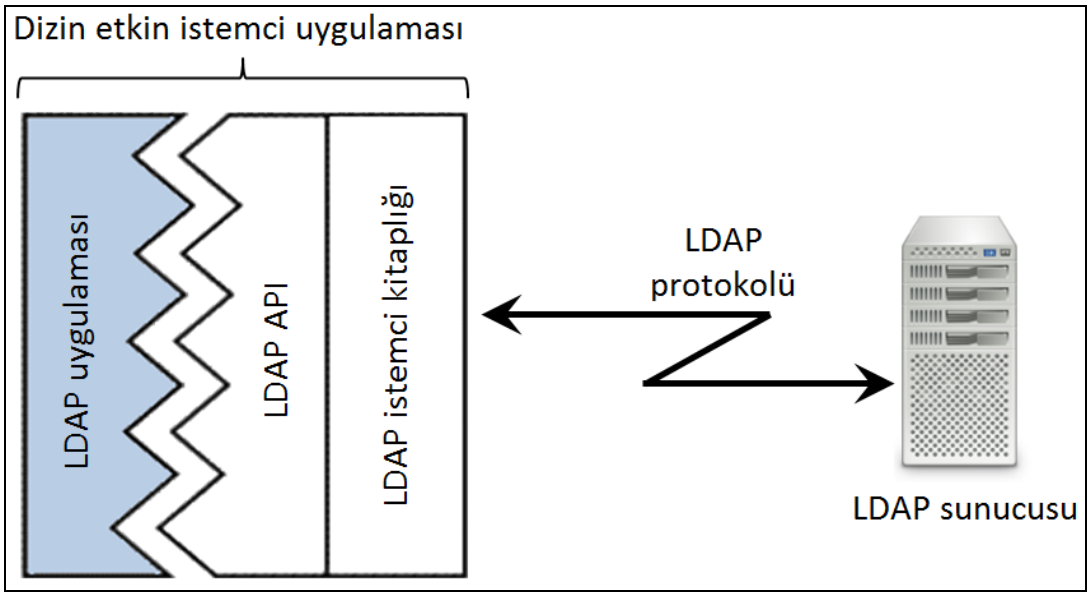


Şekil 3.17. Farklı kapsayıcılar içerisinde yer alan aynı göreceli seçkin adlar

LDAP API

Dizin etkin uygulamaların çok daha hızlı geliştirilmesi amacıyla dizin erişimlerinde ve güncellemelerde kullanılmak üzere standart bir API geliştirilmiştir. Bu maksatla Michigan Üniversitesindeki orijinal LDAP dağıtımına, bir C programlama kitaplığı ve birkaç örnek istemci programı dâhil edilmiştir. İleriki dönemlerde LDAP protokolünün yaygınlaşmasına paralel olarak LDAP uyumlu dizin etkin uygulamaların geliştirildiği farklı yazılım geliştirme araçlarının (*SDK*) sayısı artmış ve geliştiriciler tarafından kullanılmaya başlanmıştır [69].

Bunlardan biride C programlama dili SDK'larıdır ve günümüzde yaygın olarak kullanılan C++ programlama dili de bu SDK'lar üzerinde geliştirilebilmektedir. LDAP API'si, LDAP istemci kitaplığı için ortak bir ara yüz sunmaktadır. Şekil 3.18'de LDAP API'sinin dizin etkin uygulamalardaki konumu gösterilmiştir.



Şekil 3.18. Bir LDAP API'sinin dizin etkin uygulamalardaki konumu

LDAP C API bir dizi çekirdek fonksiyonu tanımlar. Çizelge 3.1'de temel LDAP C API fonksiyonları sunulmuştur. Bu API'ler dizin için asenkron bir ara yüz sağlar. Yani bu fonksiyonlar sunucuda bir protokol işlemini başlatmak için kullanılır ve sonrasında *ldap_result()* fonksiyonu ile başlatılmış olan işlemin sonuçları alınmaktadır. Bu yetenek sayesinde bir istemci çoklu protokol istekleri veya diğer işleri aynı anda gerçekleştirmektedir [69].

Çizelge 3.1. Temel LDAP C API fonksiyonları

Fonksiyon	Açıklama
`ldap_search()`	Dizin girdileri için arama yapar.
`ldap_compare()`	Girdinin içerdiği belirlenmiş bir nitelik değerini test eder.
`ldap_bind()`	Dizin Hizmeti için kimlik doğrulaması yapar.
`ldap_unbind()`	Bir LDAP oturumunu sonlandırır.
`ldap_modify()`	Mevcut bir dizin girdisinde değişiklik yapılmasını sağlar.
`ldap_add()`	Yeni bir dizin girdisi ekler.
`ldap_delete()`	Mevcut bir dizin girdisini siler.
`ldap_rename()`	Mevcut bir dizin girdisinin adını değiştirir.
`ldap_result()`	Bir önceki işlemin sonuçlarını alır.

3.2.7. Aktif dizin

Aktif Dizin, Microsoft ağ işletim sistemidir (*NOS-Network Operating System*). Başlangıçta Windows 2000 üzerine inşa edilmiştir. Günümüze kadar farklı sürümleri geliştirilerek gelmiştir ve dünya üzerinde kullanılan en yaygın ağ işletim sistemidir. Aktif Dizin yetkililere, küresel olarak dağıtılmış olabilecek kurumsal çaptaki bilgileri tek merkezden etkin olarak yönetmesini sağlar [74].

Microsoft'un ilk tümleşik ağ işletim sistemi (*NOS*) ortamı Windows NT 3.0, Lan Manager protokolleri ve OS/2 işletim sisteminin bir çok özelliği birleştirilerek, ilk olarak 1990 yılında yayınlamıştır. Windows NT 3.0, Aktif dizinin 1997 yılında ilk deneme sürümü yayınlanana kadar kullanılmıştır. Windows NT, kullanıcı, grup ve bilgisayar sayılarını 40.000 nesne ile sınırlamaktaydı ve bu sınırlama, büyük kuruluşlara uygun değildi. Son kullanıcılara NOS hizmeti sağlayan dağıtık yapıdaki etki alanı denetleyicilerinin veri replikasyonu, düşük bant genişliğine sahip bağlantılar nedeniyle uzun süreli gecikmelere ve kötü performanslara neden oldu. Microsoft bu sorunlar nedeniyle daha ölçeklenebilir ve

esnek olması için ağ işletim sisteminin tasarımında köklü bir değişiklik gerektiğini karar verdi. Bu nedenle, çözüm için LDAP tabanlı dizin hizmetlerine yönelmiştir [74]. Sonraki dönemde, aktif dizin için LDAP çözümlerine yönelim ve diğer güncelleştirmeler aşağıdaki yenilikleri getirmiştir.

Kopyalayarak Çoğaltma (Replikasyon) ve güven izleme: Aktif dizin, Windows Yönetim Araçları (*Windows Management Instrumentation-WMI*) sayesinde etki alanı denetleyicilerinin dizin bilgilerini kopyalayarak çoğaltma işlemlerini başarıyla tamamlayıp tamamlamadığını ve güven ilişkilerinin doğru işleyip işlemediğini gözlemleyebilmektedir.

Basitleştirilmiş kullanıcı ve ağ kaynağı yönetimi: Aktif dizin kullanımıyla beraber kimlik bilgileri ve diğer güvenlik ayarlarının kontrolünü kolaylaştıracak hiyerarşik yapılar oluşturuldu. Bu sayede, kullanıcıların rahatlıkla ağ kaynaklarına ulaşmaları sağlanmıştır.

Dizin birleştirme: LDAP tabanlı ara yüzler yardımıyla, eşitleme desteği kullanılabilmekte ve uygulamalarda özel dizin birleştirme ihtiyaçları karşılanabilmektedir.

Dizin etkin uygulamalar ve alt yapı: Aktif dizin özellikleri, uygulamalar ve ağ nesnelerinin düzenlenmesini ve yönetimini basitleştirmiştir.

Basit ölçekleme: Aktif dizin, her bir etki alanında milyonlarca nesneyi ölçeklendirmektedir. Dizin içerisindeki yapılandırma ve güncel yenileme teknikleri performansı arttırmaktadır.

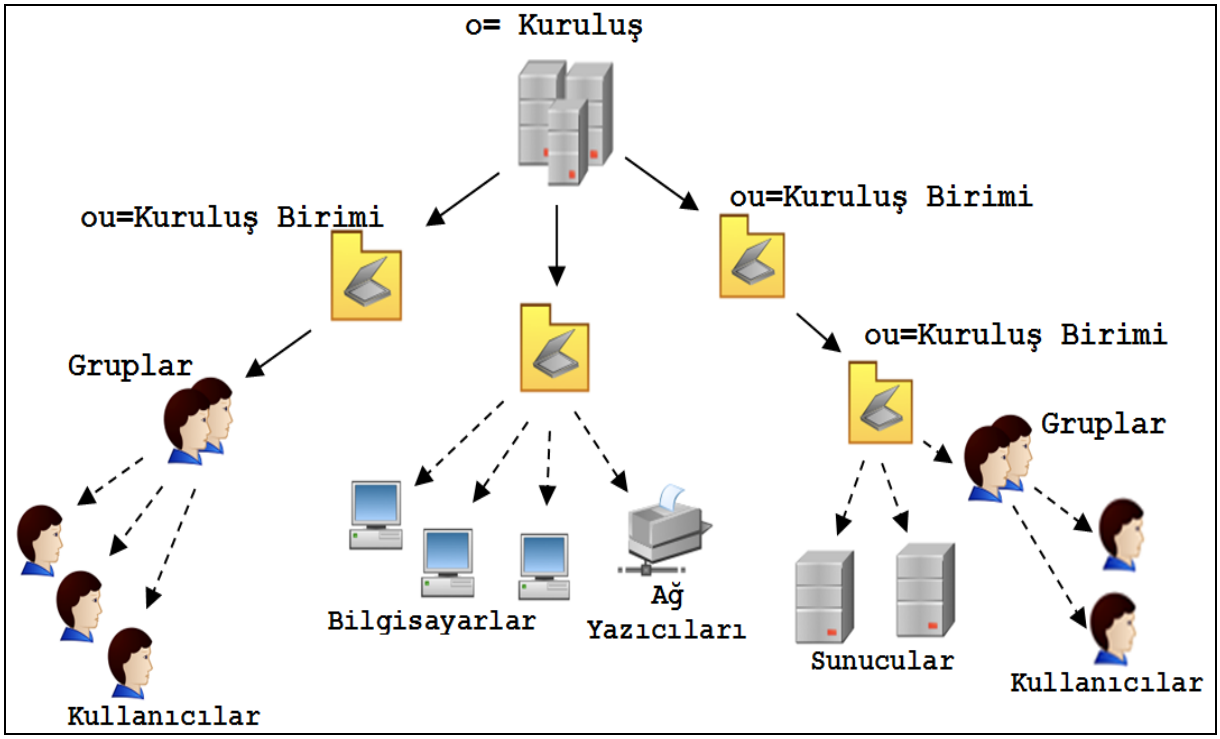
İnternet standartlarına uyumluluk: Aktif dizin, internet standartları ile uyumlu olarak LDAP tabanlı bir erişim sistemi ve DNS tabanlı bir isim alanı kullanmaktadır.

Yaygın geliştirme ortamı: Aktif dizin, nesne tabanlı ara yüz sağlayan Aktif Dizin Hizmet Ara Yüzü (*Active Directory Service Interfaces-ADSI*) sayesinde yaygın bir geliştirme ortamına sahiptir. ADSI, yazılım geliştiriciler ve yöneticiler için Microsoft Visual Basic, Java, C veya Visual C++ gibi yüksek düzeyli programla dili araçları ile farklılıklara takılmadan dizin etkin uygulamaların geliştirilmesini kolaylaştırmaktadır.

Esnek, güvenli kimlik doğrulama ve yetkilendirme: Aktif Dizin, Kerberos V5 protokolü, Güvenli Yuva Katmanı sürüm 3 (*SSLv3*) ve X.509 sürüm 3 sertifikalarını kullanan Taşıma Katmanı Güvenliği (*TLS*) gibi birden çok kimlik doğrulama yöntemini desteklemektedir.

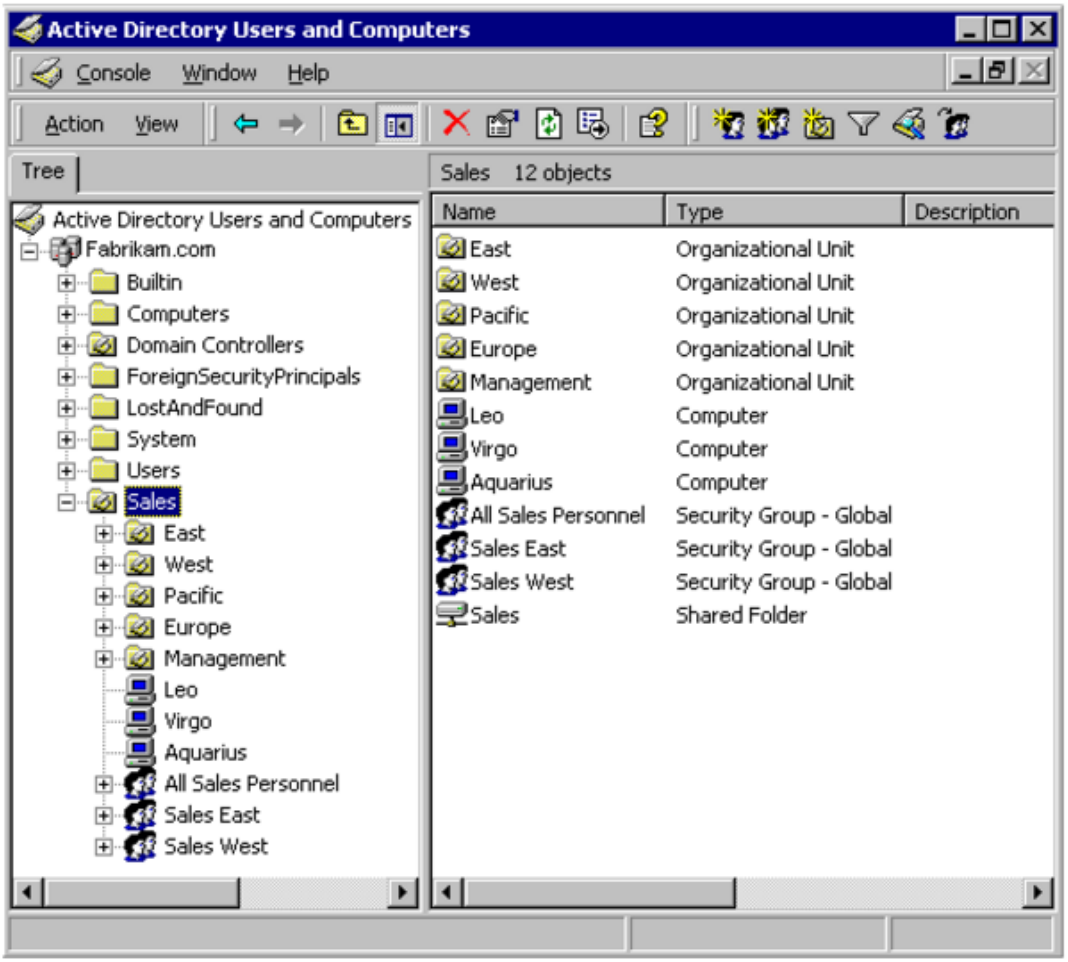
Mesaj kuyruğu (MSMQ-Message Queuing) dağıtım listeleri: Aktif dizinde barındırılan dağıtım listelerine ileti gönderilmesini sağlamaktadır [75].

Aktif Dizin içerisinde depolanan veriler, kullanıcılara bir dosya sistemine benzer bir şekilde hiyerarşik şekilde sunulmaktadır. Her bir girdi bir nesneyi ifade eder. Yapısal seviyede, kapsayıcı ve kapsayıcı olmayan olarak iki tür nesne mevcuttur. Kapsayıcı olmayan nesneler yaprak düğümler (*leaf node*) olarak adlandırılmaktadır. Bir veya daha fazla kapsayıcı, kök bir kapsayıcıdan hiyerarşik bir şekilde dallara ayrılmaktadır. Her bir kapsayıcı yaprak düğümleri veya diğer kapsayıcıları içermektedir. Ancak yaprak düğümler nesne içermemektedir. Bu hiyerarşik yapı modeli Şekil 3.19'da sunulmuştur [74]. Ayrıca Şekil 3.20'de hiyerarşik yapının bir kısmının görüldüğü grafik ara yüzü sunulmuştur.



Şekil 3.19. Aktif dizin hiyerarşik bir nesne yapısı örneği

Aktif dizinde bulunan hiyerarşik yollar, bir nesneye ulaşmak için eşsiz olarak verilmesi gereken ve bir önceki bölümde ayrıntılı olarak açıklanmış olan seçkin adları kullanmaktadır. Seçkin adlar, dizin içerisindeki herhangi bir nesneyi işaret eden bir araç olarak LDAP standardında tanımlanmıştır. Seçkin adlar, LDAP standartlarında aktif dizin nesnelerini gösteren söz dizimi ve kurallar olarak tanımlanır. Seçkin adlar içerisinde aktif dizin tarafından yaygın olarak kullanılan nitelik türleri Çizelge 3.2'de sunulmuştur [74].



Şekil 3.20. Hiyerarşik yapının bir kısmının görüldüğü grafik ara yüzü [76]

Çizelge 3.2. En yaygın kullanılan nitelik türleri

Seçkin Ad Anahtarları	Nitelik
CN	Ortak ad
L	Yer Adı
ST	Eyalet veya Bölge Adı
O	Kuruluş adı
OU	Kuruluş Birimi Adı
C	Ülke Adı
STREET	Açık Adres
DC	Etki alanı Bileşeni
UID	Kullanıcı Kimliği

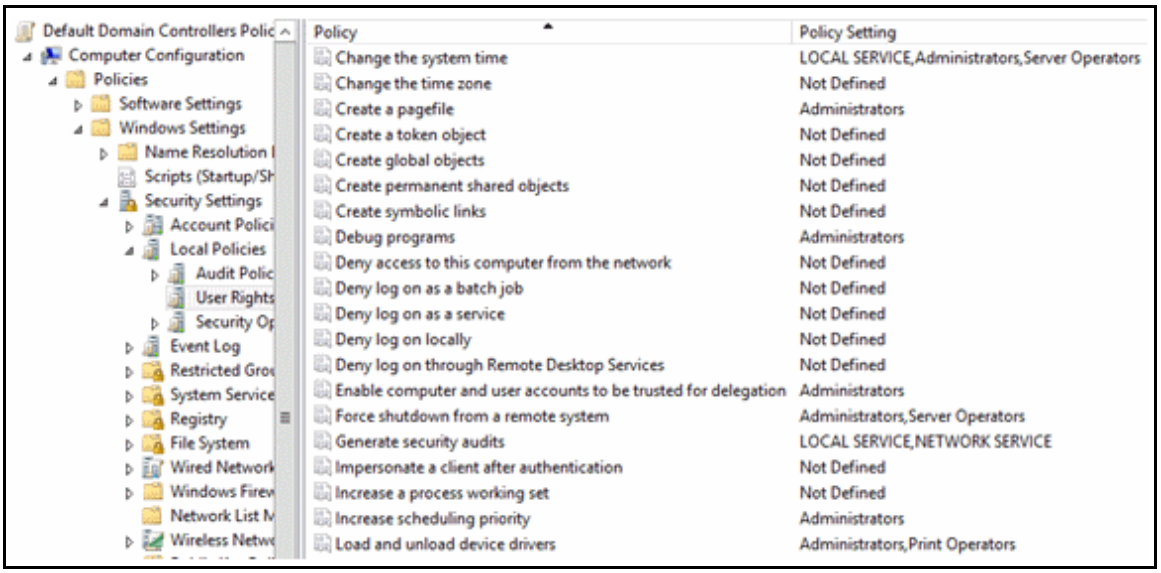
Uygulama modelinin pilot çalışmaları aktif dizin üzerinde yapılmıştır. Uygulama modeli, aktif dizin API'lerinin kullanıldığı dizin etkin bir uygulamadır. Geliştirilirken ASP.Net programlama dili kullanılmıştır. Uygulama modeli, LDAP protokollerine göre uyarlanan her dizin hizmetinde kullanılmak üzere tasarlanması sayesinde aktif dizin uygulamasına bağımlılık yaratmamaktadır. Uygulama modeli, LDAP uyumlu her türlü dizin hizmeti ile tümleşik olarak kullanılabilmektedir. Bunun için sadece ilgili dizin hizmeti uygulamasına ait API kitaplıklarının yazılım geliştirme aracına (*Software Development Kit-SDK*) aktarılarak uygulama kodlarında kullanılması yeterli olmaktadır.

3.2.8. Aktif dizin uygulamalarındaki ayrıcalıklı hesapların yetenekleri

Dizin hizmeti ve özellikle Microsoft aktif dizin uygulaması içerisindeki ayrıcalıklı hesap olarak tanımlanan, genellikle BT personeli tarafından kullanılan hesapların yetkilerinin ne kadar fazla olduğu ve saldırganların eline geçtiği kötü bir senaryo sonucunda BT altyapısının kontrolünün saldırganların eline geçebileceği hususu önceki bölümlerde açıklanmıştı. Bu bölüm içerisinde Microsoft aktif dizin uygulaması tarafından kullanılan ayrıcalıklı hesapların yetkileri daha yakından incelenmiştir.

Aktif dizinde yer alan "*Ayrıcalıklı*" olarak tanımlanan hesaplar, söz konusu etki alanı içerisindeki tüm nesne ve kaynaklarda her türlü eylemi gerçekleştirmek üzere güçlü haklar, imtiyazlar ve izinlere sahip olarak yapılandırılmıştır [17]. Bu hesaplara sahip olacak kişilerin tüm aktif dizin ağaç yapısını kontrol edebilecekleri düşünüldüğünde, hesapları kullanacak kişilerin yüksek güvenirliğe sahip kişi/kişiler olması ve sürekli olarak izlenmesi gerekmektedir [77]. Söz konusu hesapların ayrıcalıklarını kavramak adına öncelikle imtiyaz, haklar ve izin terimlerinin karşılıkları anlaşılmalıdır.

Hak ve imtiyazlar, sistem geneline bakıldığında aynı anlamdadır ve kullanıcılar, hizmetler, bilgisayarlar ile gruplar gibi nesneler üzerinde güvenlik ilkeleri doğrultusunda verilen yetkileri ifade etmektedir. Bu yetkiler aktif dizinde haklar veya kullanıcı hakları olarak da ifade edilmektedir. Aktif dizinde güvenlik ilkeleri seçeneğinden ayarlanan bu yetkilerin ayarlandığı ara yüzün ekran görüntüsü örnek olarak Şekil 3.21'de sunulmuştur. Şekil 3.21'de sunulduğu üzere, kullanıcı hesabı tarafından gerçekleştirilmesi uygun görülen eylemler (*sistem saatini değiştirmek, paylaşım nesneleri oluşturmak, ağ erişimine müsaade etmek gibi*) tanımlanarak, verilmek istenilen kullanıcı hakları yapılandırılmaktadır [17].



Şekil 3.21. Aktif dizin kullanıcı hakları yapılandırma bölümü ekran görüntüsü

İzinler, kayıt defteri, dosya sistemi, hizmetler ve aktif dizin nesneleri gibi güvenliği ön planda olan nesneler için uygulanan erişim kontrolünü ifade etmektedir. Aktif dizindeki güvenilir nesneler, izinli veya yasaklı olmak üzere bir güvenlik ilkesi girdisine sahiptir. Bu nesneler üzerinde gerçekleştirilecek eylemler (*okuma, yazma, silme gibi*) bu güvenlik ilkesi girdilerine bağlıdır [17].

Aktif dizin tasarımı itibariyle kullanıcı hakları ve izinler için en az yapılandırmaya ihtiyaç duyacak şekilde tasarlanmıştır. Normal kullanıcı hesapları, varsayılan güvenlik ilkeleri sayesinde sisteme zarar verebilecek bir eylemi gerçekleştirecek kadar yetkiye sahip değildir. Ancak aktif dizin uygulaması kullanılan BT altyapılarının kontrol, bakım ve idamesi ile görevli kullanıcılar normal kullanıcı hesaplarını kullanmamaktadır. Bu nedenle sistemde tümleşik olarak dâhil edilmiş ayrıcalıklı hesap grupları mevcuttur. Bunlar kurumsal yönetici hesap grupları (*Enterprise Admins*), etki alanı yönetici hesap grupları (*Domain Admins*) ve yerleşik yönetici hesapları (*Built-in Administrators*) olmak üzere üç kategoride incelenmektedir. Ayrıca bu kullanıcılara nazaran yetkileri daha kısıtlı olan şema yönetici hesapları (*Schema Admins),* ele geçirildiği takdirde sisteme zarar verebilecek kadar yetkiye sahiptir [17].

Kurumsal yönetici hesap grupları (*Enterprise Admins*), dizin yapısı içerisinde en yetkili kullanıcı grubudur ve bu gruba dâhil bir hesap tüm nesneler üzerinde tam yetkilidir. Bunun yanı sıra aktif dizin uygulama sunucusunun yerel yönetici hesabı bu grubun doğal bir üyesidir. Ayrıca bu grupta yer alan bir hesap, sisteme dâhil olan tüm bilgisayar ve

sunuculardа aynı yetkilere sahiptir [17]. Aktif Dizin uygulama sunucusunun yerel yönetici hesabının bu grubun doğal üyesi olması beraberinde güvenlik zafiyetlerini de getirmektedir. Varsayılan parolası değiştirilmeyen veya kurulum sırasında basit bir parola verilerek geçiştirilmesi durumunda bu hesaplar çok büyük sorunlara neden olabilir. Microsoft, bu hesaplar için güçlü bir parola verilmesini ve varsayılan yönetici hesabı adının (*Administrator*) mutlaka değiştirilmesini tavsiye etmektedir [78].

Etki alanı yönetici hesap grupları (*Domain Admins*), daha önceki bölümlerde açıklanmış olan ve aktif dizin içerisindeki tanımlanan kuruluş (*organization–o*) kök yapısı altında bulunan tüm nesneler üzerinde tam yetkiye sahiptir. Kök yapısı altındaki tüm bilgisayar ve sunucularda yerel yönetici grubunun doğal bir üyesidir.

Yerleşik yönetici hesapları (*Built-in Administrators*) varsayılan olarak, aktif dizin içerisindeki bilgisayar ve sunucular üzerinde tam yetkiye sahiptir. Ancak aktif dizin uygulaması üzerinde yetkileri bulunmamaktadır [17].

3.3. Parola Kullanımı ve Parola Saldırıları

Parolalar BT güvenliği açısında önemli bir role sahiptir. Kaynakların koruması adına düşük teknolojili bir çözüm sunarak, kimliği doğrulanmamış veya yetkisiz erişime teşebbüs eden kişileri ve hizmetleri engeller. Kullanılan parolalar ve korudukları bilgilerin çeşitliliği düşünüldüğünde, parolaların önemi netleşmektedir [79]. Örneğin; Twitter, Facebook, Linkedin gibi sosyal ağlar parolasız ve herhangi bir kimlik doğrulaması olmadan kullanılsa, herhangi bir kişi tüm özel bilgilerinize rahatlıkla erişebilecek ve bilgilerinizi istediği gibi maniple edebilecektir [80]. Bu durumun büyük veya küçük, özel ve kamu kuruluşları için geçerli olduğu düşünüldüğünde, bu kuruluşların uğrayabileceği zarar çok daha iyi anlaşılmaktadır.

Parolalar günümüzde akıllı telefonlarda, tabletlerde, bilgisayarlarda ve gündelik yaşantımızda birçok alanda çok sık kullandığımız önemli ve basit bir güvenlik çözümüdür. Çalışmamızın konusu gereği incelediğimiz parolalar, bilgisayarlar ve bilgisayar sistemlerinde kullanılanlar olacaktır. Parolalar, bir bilgisayarda veya bilgisayar sistemleri içerisinde depolanan bilgileri korumak ve kaynaklara yetkisiz erişimi engellemek

maksadıyla kullanılan en son savunma hattını oluşturmaktadır. Bazı durumlarda alınan tüm güvenlik önemlerine rağmen yegâne savunma hattı olmaktadırlar [80].

AHEKS uygulama modeli, yerel yönetici hesaplarının ve dizin hizmetindeki ayrıcalıklı yönetici hesaplarının parolalarına karşı bilinçli veya bilinçsiz tehditlerin önüne geçmek üzere BT güvenlik uzmanlarına destek olması amacıyla geliştirilmiştir.

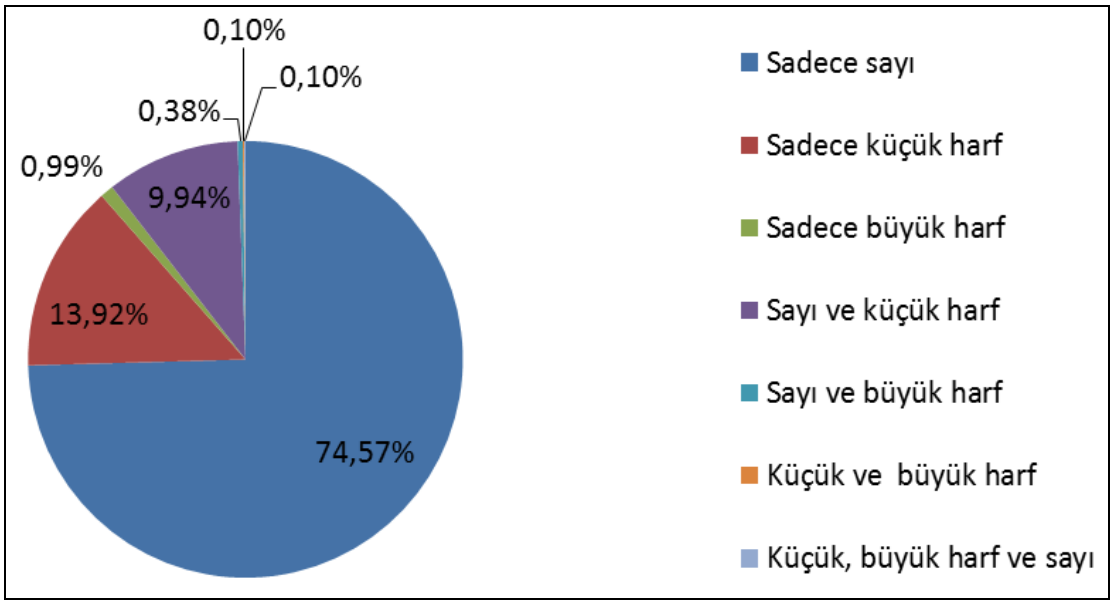
3.3.1. Parola kullanımında yapılan hatalar

Parola, kullanıcıların bir bilgisayarda oturum açmak, dosyalara, programlara ve diğer kaynaklara erişmelerini sağlamak için kullandıkları karakter dizisidir. Parolalar, kişileri yetkili olmadıkları sürece bilgisayara erişmemelerini sağlamak için kullanılmaktadır [81,82]. Parola, doğası gereği kişisel bir bilgidir. Bu bilgiyi elinde bulunduran kişiye, parola ile korunan değerlere erişim müsaadesi verilmiş demektir. Yani değerli varlıklarımıza erişmek için kullanılacak olan parolanın, aksi bir tedbir alınmadığı müddetçe ne olacağına kullanacak kişi karar vermektedir. Bu durumda değerli varlıklarımızı güvenerek teslim ettiğimiz kişinin parola seçiminde gösterdiği duyarlılık kadar varlıklarımıza koruma sağlamış oluruz. Ancak insanın olduğu her alanda olduğu gibi bu durumda hatalara açıktır [83].

Genel parola kullanım hataları

Güçlü bir parola, tahmin edilmesi kolay olmayan ya da deneme yanılma yolu ile ele geçirilmesi oldukça zor olan karakter dizileri olarak tanımlanabilir [84]. Sağlam ve dayanıklı bir parola oluşturmak maksadıyla yapılan ilk hamle seçilecek parolanın uzunluğu yani karakter sayısını artırmaktır. Bu düşünce ile hareket edilerek oluşturulan parolaların, gerçekten sağlamlık açısında daha az karakterden oluşan parolalara nazaran daha güçlü olduğu söylenebilir. Karakter sayısının artması entropi (*farklı bir sözcük üretebilme ihtimali*) değerini yükselten en önemli faktörlerden biridir ve güçlü bir parola oluşturmak için kullanılan yöntemlerden biri olarak kabul edilmektedir [85]. Ancak karakter sayısını fazla olması güçlü bir parola oluşturmak için tek kıstas değildir. Genel olarak güvenlik ve kullanılabilirlik dengesi ideal bir parola için gerekli şartlara sahip olduğu kabul edildiğinde 8 karakterden oluşan bir parolanın uzunluk açısından asgari yeterliliği karşıladığı konusunda genel bir görüş birliği mevcuttur [86,87].

Rakam, küçük harf, büyük harf, özel karakterler bir parolada ne kadar fazla kullanılırsa, yani karakter türlerinin çeşitliliği ne kadar fazla olursa entropi oranı o kadar artmaktadır [87]. Bir veri tabanında toplanan parolalar üzerinde yapılan bir araştırmaya göre parola oluşturulurken kullanılan karakter çeşitliliği kullanım oranı Şekil 3.22 ‘de sunulmuştur.



Şekil 3.22. Parola oluşturulurken kullanılan karakter çeşitliliği oranları [86]

Dayanıklı bir parola, sözlüklerde bulunamayacak şekilde bir anlam ifade etmeyen, rastgele karakterlerden oluşan ve uzunluğu yeterli olacak şekilde oluşturulmalıdır. Aşağıda sıralanan ölçütler, dayanıklı bir parola oluşturmak için gerekli temel ölçütlerdir.

- Karakter sayısı az olan parolaların, karakter sayısı fazla olan parolalara göre daha kolay elde edilmesi nedeniyle parolalar daha uzun oluşturulmalıdır (*Ortak düşünce en az sekiz karakter olması*),
- Parolalar büyük harf, küçük harf, rakam ve özel karakterlerden oluşturulmalıdır. Ardışık veya tekrarlanan kombinasyonlar ("12345678," "55555555," "abcdefg" vb.) veya klavyede yan yana duran harflerden oluşmamalıdır,
- Parola, kullanan kişi tarafından hatırlanması kolay, fakat başkalarının tahmin etmesi zor olmalıdır,
- Kullanıcı hesabınızın adı yakınlarınızı adı veya doğum tarihleri olamamalıdır,
- Parola, farklı bir dilde olsa dahi sözlüklerde bulunabilecek, anlam ifade eden bir kelime (parola, password vb.) veya kelimenin tersten yazılışı (alorap, drowssap vb.) olmamalıdır,

- Parolalar, ortak kullanılan veya bilinmeyen bir bilgisayarda kullanılmamalıdır,
- Parola, statüsü ne olursa olsun kimse ile paylaşılmamalıdır,
- Parolalar düzenli olarak değiştirilmelidir. Değiştirme zaman aralığı, parolanın koruduğu içeriğin önemine göre kısaltılmalıdır,
- Hatırlanabilir olmalıdır. Güçlü bir parola, hafızada kalıcılığı az veya her defasında bir nota bakılarak hatırlanabilecek şekilde oluşturulmamalıdır. Nimonik (*mnemonic*) ifadeler ile hatırlaması kolay parolalar seçilmelidir [87,88].
- Parolalar, normal posta veya elektronik posta yoluyla gönderilmemelidir [89].

İnternet üzerinde yapılacak kısa bir araştırma sonucunda en kötü ve en yaygın parolalarla ilgili birçok anket, makale ve araştırmaya ulaşılabilir [90-94]. Tabi yapılan bu araştırmalar genellikle yurt dışı kaynaklı olması nedeniyle listedeki parolalar ve belirtilen hatalı kullanıcı davranışları temel olarak benzerlik gösterse de bazı farklılıklar içermektedir. Bu kapsamda ülkemizde görülen ve sıklıkla rastlanan parola oluşturulurken yapılan hatalar ve örnekleri Çizelge 3.3'de sıralanmıştır.

Çizelge 3.3. Hatalı parola oluşturma davranış örnekleri

Parola Oluşturma Davranışı	**Örnek**
Taraftarı olunan spor kulübü ve kuruluş tarihi	*besiktas1903*
Kendisini veya yakınlarının isimleri ve doğum tarihleri	*ahmet1982*
Çok fazla parola olması nedeniyle basit parola kullanımı	*123456*
Doğum yeri ve plaka kodu	adana01
Sevilen sporcu isimleri ve forma numaraları	Quaresma77
Kullandığımız cep telefonu numarası	*5998887766*
Çocuklarının adı ve doğum tarihlerinin son haneleri	*ahmetmehmet9699*
Seçilen bir sözcük ile son hanelerindeki rakamların değiştirilmesi	parola01, parola02, parola03, parola04, parola05, …
Klavyede sıralanan ilk sıradaki harfler	qwerty - fgğiod
Hesap adı ile aynı olacak şekilde parola kullanımı	ahmet.mehmet@gazi.edu.tr *parola :* ahmetmehmet

Parola oluşturulurken yapılan hatalar dışında ayrıca parola kullanım davranışlarında da bazı hatalar yapılmaktadır. Kullanıcılar tarafından genellikle bu tür hatalar alışkanlık haline getirilmiştir [87]. Bu nedenle, parola ile korudukları sosyal ağ hesapları, çevrim içi

bankacılık hesapları, bulut depolama hesapları, iş yerlerinde kullanılan kullanıcı hesapları vb. hesapların herhangi birinin ele geçirilmesi sonucu tüm diğer hesaplar, saldırganlar tarafından kullanıcının parola verirken göstermiş olduğu davranış anlaşıldığı için ele geçirilme tehlikesi altındadır. Bu nedenle işletim sistemleri, sosyal ağlar ve çevrim içi bankacılık uygulamalarında bu hizmetleri sağlayanlar tarafından kullanıcıların parolalarını güçlendirmek için bazı tedbirler (*parola uzunluğu, karakter çeşitliliği, isim ve doğum tarihinin kullanımının engellenmesi, parolanın belli aralıklarla değiştirilmeye zorlanması, geçmiş parolaların kullanımının engellenmesi vb.*) alınmaktadır [95]. Ancak bu tedbirler bile bazı kullanıcıları parolalarını düzeltmeleri için motive edememekte ve Çizelge 3.4'de bazı örnekleri verilmiş olan hataları tekrarlamaya devam etmektedirler [83,96].

Çizelge 3.4. Hatalı parola kullanım davranışı örnekleri

Davranış Türü
Kişisel işlemlerde kullanılan (*çevrim içi bankacılık işlemleri parolaları, sosyal ağ hesaplarının parolaları vb.)* parolaların iş yerlerinde kullanılması
Doğum tarihi, aile bireylerinin isimleri, hobiler, spor takımları gibi sosyal ağlar üzerinden elde edilebilecek alışkanlıkların parolalarda kullanılması
Parolalardaki sadece tek bir harfin, rakamın veya karakterin değiştirilerek kullanılması
Bilgisayarların varsayılan parolalarının değiştirilmemesi (*Windows XP işletim sistemlerinde "administrator" parolası varsayılan olarak boş gelir*)
Parola bilgilerini içeren dokümanları bilgisayarda tutulması
Parola bilgilerini içeren yazılı dokümanların bilgisayarların yanında tutulması
Kullanılan parolaların iş arkadaşlarıyla paylaşılması
Aynı parolaların dönüşümlü olarak farklı hesaplarda kullanılması

BT personeli tarafından yapılan parola kullanım hataları

Parola kullanımında hataları sadece sıradan kullanıcılar yapmamaktadır. Tüm tehditlerin ve her hangi bir ihlal durumunda ortaya çıkabilecek zararların farkında olan, bilinçli kullanıcı olarak gördüğümüz ve meydana gelecek zararlardan doğrudan sorumlu tutulacak BT personelinin parola kullanımı konusunda hiç hata yapmadığını iddia etmek yanıltıcı ve

hayalperest bir düşünce olacaktır. BT personelinin parola kullanımı konusunda yapacağı yanlışlar, her ne kadar sıradan bir kullanıcının yapacağı hatalara oranla çok daha az olsa da, ortaya çıkacak zarar çok daha fazla olacağından titizlikle ele alınması ve kontrol altında tutulması gereken bir problem olarak karşımıza çıkmaktadır.

İş yoğunluğu, manevi tatminsizlik, umursamazlık, bilgi noksanlığı, aidiyet duygusunda noksanlık, teknik altyapı yetersizliği, kullanılan teknik altyapı hakkında bilgi sahibi olmamak gibi nedenlerden ötürü BT personelinin bu konu hakkında yeterli duyarlılığa sahip olmadığı görülebilmektedir. Bilişim sistemlerinin 24 saat çalışır durumda olmasını sağlamakla yükümlü olan BT personeli, arıza durumunda en kısa sürede arızaya müdahale etmelidir. Bu nedenle BT personelinin çalışma saatleri diğer çalışanlara nazaran farklılıklar gösterebilmektedir. Bazı durumlarda arızayı ilk fark eden çalışan, sorumlu BT personeline ulaşarak konu hakkında bilgi verir. Arızanın boyutlarına göre sorumlu BT personelinin cihazların başından müdahale etmesi gerekebilir ve böyle bir senaryoda yapılması gereken doğru harekette bu olmalıdır. Ancak bazı durumlarda BT personeli, doğru olanı yapmaktansa kolay ve zahmetsiz olanı yapmayı tercih ederek, BT sistemleri üzerinde ayrıcalıklı haklara sahip kullanıcı hesabına ait parolayı, kendisine ilk ulaşan kişiye vererek arızayı çözmesini talep edebilmektedir. Kendisine verilen sorumluluktan kaçınarak yapmış olduğu bu hareket, tüm BT altyapısının bilinçli veya bilinçsiz olarak çok büyük zararlara uğramasına neden olabilmektedir.

Teknolojinin ilerlemesi ve bilgisayarların lüks harcamalardan çok bir ihtiyaç olduğu günümüzde, kuruluşlarda kullanılan bilgisayar sayıları yüzleri hatta binleri bulmaktadır. BT personeli, çözüm için ayrıca bir tedbir alınmamışsa, bilgisayarların yerel yönetici hesaplarını tek tek değiştirmek zorundadır. Bu çok fazla iş yükü getirmekte, bu nedenle çok sayıda bilgisayar bulunan yapılarda ihmal edilebilmektedir. Bir defa değiştirilen yerel yönetici hesap parolası tekrar değiştirilmemekte ve uzun süre aynı parola ile kalabilmektedir. Veya belli dönemlerle, bir uygulama yardımıyla değiştirilse bile tüm bilgisayarların yerel yönetici hesaplarına aynı parolalar verilmektedir. Daha vahim olanı ise, bilgisayarlara ilk yükleme esnasında verilen parolaların hiç değiştirilmeden kullanılmasıdır. Bu senaryoların üçünde de verilen parola ne kadar güçlü olursa olsun, yerel yönetici hesapları için tüm bilgisayarlarda aynı parola kullanılması, bir bilgisayarın yerel yönetici hesap parolasının ele geçirilmesi durumunda tüm bilgisayarların ele geçirilme ihtimalini ortaya çıkmaktadır [87,97].

Parola kullanım hataları genellikle sıradan kullanıcı olarak tanımladığımız kişiler tarafından yapılıyor olsa da, BT personeli tarafından aynı hataların yapıldığı da görülmektedir. Birçok sistemi kontrol eden BT personeli, her birine ayrı parola vermektense, hatırlaması kolay olması nedeniyle tek bir parola ile tüm sistemleri yönetme yoluna gidebilir. Veya kullandığı parolaların tahmin edilebilir olması tüm sistemi tehdit eden diğer bir unsurdur. Özellikle yerel yönetici hesabı parolası ile dizin hizmeti uygulaması içerisinde kullanmış olduğu ayrıcalıklı yönetici hesap parolası aynı olması en önemli ihmallerden biridir.

Uzak masaüstü bağlantıları kullanılarak yapılan erişimler sırasında bağlantı sonlandırılmadan önce mutlaka oturum kapatılmalıdır. Oturum kapatılmadan bağlantı sonlandırılması durumunda, uzak sistem üzerinde ki oturum açık kalacak ve bu nedenle kullanılan parola bilgisi bellekte durmaya devam edecektir. Bir şekilde uzak sistemin komut satırına erişebilen bir saldırgan tarafından kullanılacak araç ve yöntemlerle ile bellekteki parola bilgisini almak oldukça basittir. Aynı etki alanı içerisindeki tüm bileşenler üzerinde yetkisi olan bir kullanıcı hesabı ile oturum açıldığı andan, oturumun sonlandırıldığı zamana kadar parola bilgisi bellekte kalmaya devam eder. Bu nedenle özellikle ayrıcalıklı hesaplar ile yapılacak işlemlerin ardından oturum kapatılarak söz konusu sistemden çıkış yapılması gerekmektedir.

AHEKS uygulama modeli, her bilgisayar için farklı olacak şekilde ve her kullanım sonrası değiştirilmek suretiyle yerel yönetici hesaplarına ait parolaları güncelleyerek ve dizin hizmeti içerisindeki ayrıcalıklı hesapların parola yönetimini mümkün kılarak bu sorunların ortadan kaldırılmasını sağlamaktadır.

3.3.2. Parola saldırıları

Parola saldırısı, bilişim sistemleri üzerinde kullanılan hesaplara ait parolaların saldırganlar tarafından illegal olarak ele geçirilme çabasıdır [98]. Kullanılan yöntemlere, araçlara ve hedef sistemin yapısına göre farklılıklar gösterebilmektedir [99]. Saldırganlar tarafından elde edilen parolalar, hedef bilişim sistemini ele geçirerek sisteme zarar vermek veya değerli verileri elde etmek için kullanılırlar. Saldırganların amaçlarına ulaşabilmek için elde ettikleri parolaların hedef bilişim sistemleri üzerinde yeterli yetkilere sahip olması gerekir. Yetkisiz bir kullanıcı hesabına ait parola elde edildiği durumlarda saldırganlar,

yetkilerini arttırabilmek amacıyla *hak yükseltme* adı verilen yöntemi kullanarak amaçlarına ulaşmaya çalışırlar [79,100].

Yatay ve Dikey Hak Yükseltme

Hak yükseltme saldırısı, sahip olduğu erişim haklarını kullanarak bir saldırgan tarafından normalin dışındaki erişim haklarının elde edilmesidir. Hak yükseltme saldırıları tüm ağı ele geçirmek için kullanılabileceği gibi erişimi kısıtlanmış verilere ve kaynaklara erişim içinde kullanılabilir [101].

Hak yükseltme saldırıları temel olarak iki başlık altında toplanmaktadır;

- Dikey Hak Yükseltme
- Yatay Hak Yükseltme

Dikey hak yükseltme, sahip olunandan daha yüksek yetki veya erişim seviyesinin elde edilmesidir. Bu ek yetki veya erişim hakları, başlangıçta olduğundan çok daha fazla kaynağa erişilmesini sağlar. Örneğin; kullanıcı grubunda bulunan sınırlı haklara sahip bir kullanıcının yönetici grubuna eklenmesi ile yönetici haklarının elde edilmesi [102,103].

Özellikle dizin hizmetindeki etki alanı yöneticileri grubuna üye bir hesabın ele geçirilmesi durumunda günlük kayıtların saklandığı sunucuları, elektronik posta sunucuları veya veri tabanı sunucuları gibi hayati önem taşıyan sunuculara tam erişim hakkı saldırgan tarafından ele geçirilecektir. Kısaca tüm veri ve uygulamaların kontrolünü saldırgan elde edecektir. Saldırgan kontrolü ele geçirmesinin ardından hizmet dışı bırakma saldırılarıyla tüm ağı etkisiz kılabilir. Saldırgan, müşteri bilgileri, çalışanların kayıtları, kuruluşa ait ticari sırlar gibi verilere erişebilir ve bunları farklı amaçlar için kullanabilir. Saldırganın bu hassas verilere erişmek için kök veya yönetici seviyesindeki hesapları elde etmesi gerekli değildir. Bu buna yetkili bir kullanıcının hesabını elde etmesi yeterlidir [101].

Yönetici hesaplarının ele geçirilmesi saldırgana diğer kullanıcı hesaplarını, müşteri hesaplarını veya oluşturabileceği sahte hesaplarla kuruluş içerisinde faaliyetlerde bulunarak kuruluşa maddi ve manevi olarak çok büyük zararlar verebilir.

Yatay hak yükseltme, bir hesabın/servisin benzer veya aynı erişim haklarına sahip hesabı ele geçirmesi sonucu erişimi olmayan içerikte işlem yapmasını sağlamasıdır [103,104]. Örneğin; kullanıcı grubuna dâhil bir hesaba sahip saldırgan tarafından kullanıcı grubunda bulunan başka bir kullanıcının hesabının ele geçirilmesi sonucu normalde erişimi olmayan mağdura ait elektronik posta hesabının ele geçirilmesi.

Bunların dışında bu konu içerisinde ele alınması gereken bir konuda hak düşürme saldırısıdır. İlk bakışta mantıksız gelebilecek bu işlem bir saldırı türü olarak kötü niyetli kişilerce kullanılmaktadır. Örneğin; kurum içerisinde üst yönetimde bulunan bir kullanıcı, önemli verilerin tutulduğu ve işlendiği bir uygulamaya girdi yapma yetkisine sahip sıradan bir çalışanın hesabını kullanılarak söz konusu uygulamadaki verileri çıkarları doğrultusunda değiştirebilir.

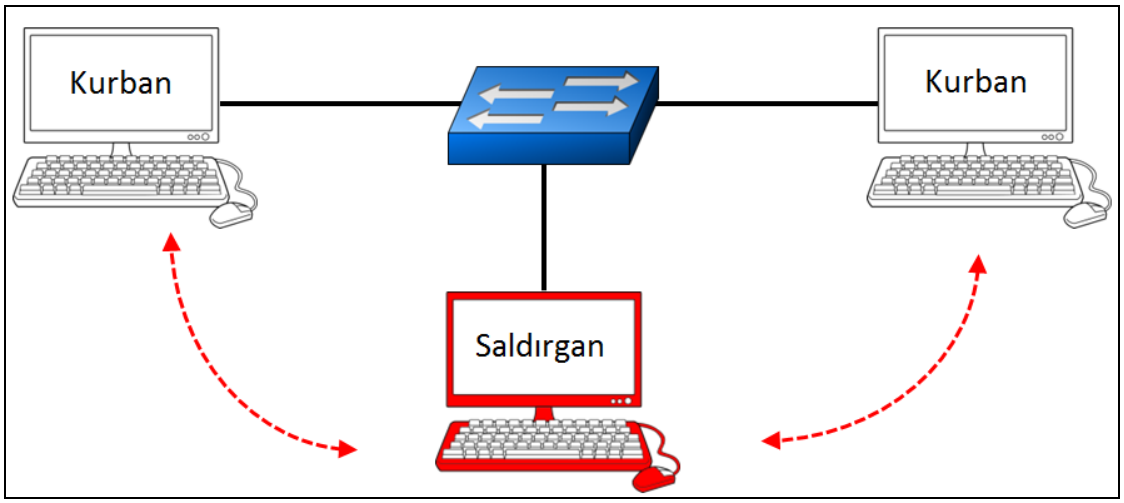
Parola saldırı yöntemleri

Parola elde etmek için yapılacak saldırılar, uygulama metotlarına göre dört temel türde incelenmektedir [105,106].

- Pasif Çevrimiçi Saldırılar
- Aktif Çevrimiçi Saldırılar
- Çevrimdışı Saldırılar
- Teknik Yöntemler Kullanılmayan Saldırılar

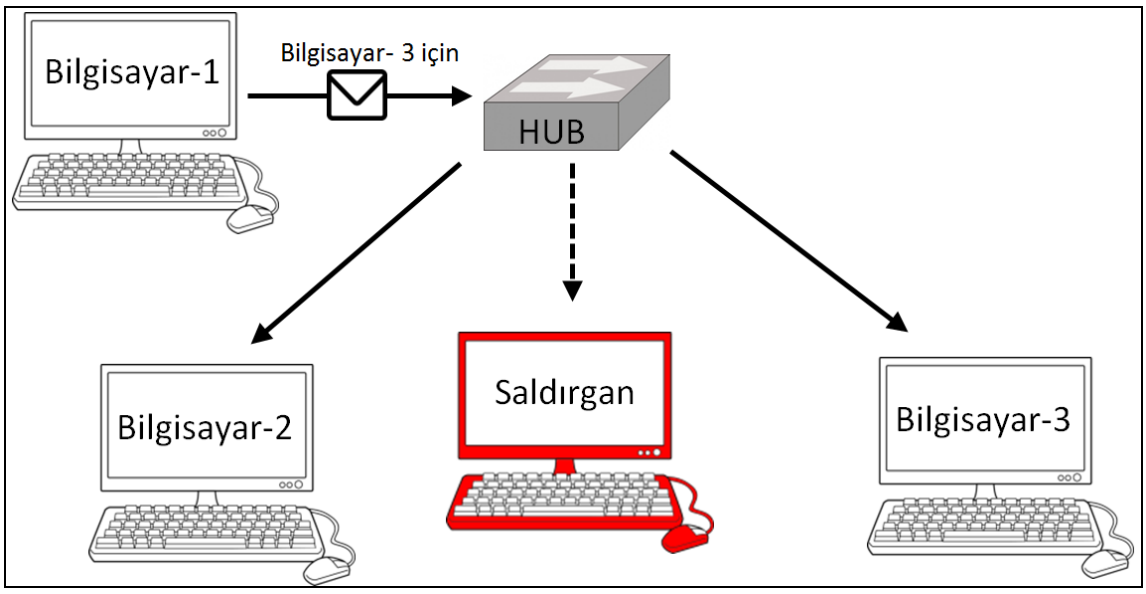
Pasif çevrimiçi saldırılar

Bu saldırılar, aynı yerel ağda bulunan saldırgan tarafından ağ trafiğinin maniple edilmesi ile yapılmaktadır. Bu saldırı metodu iki şekilde yapılmaktadır. İlki Şekil 3.23'de temsili olarak gösterilmiş olan *Ortadaki Adam* (Man-in-the-Middle-MITM) olarak adlandırılan saldırı türüdür. Saldırgan, yerel ağdaki tüm trafiğin üzerinden akmasını sağlayacak, içeriği değiştiriliş paketleri tüm ağa yayınlar. İçeriği değiştirilmiş paketlerden zehirlenen kurbanın gönderdiği paketler saldırgan üzerinden geçmeye başlar. Aynı zamanda saldırgan kendisine gelen kurbana ait paketleri dinler ve tekrar içeriğini değiştirerek kendisini hedefe kurban olarak tanıtır ve gelen sonuçların üzerinden geçmesinin sağlar. Trafiğin üzerinden akmasını sağlayan saldırgan, akan trafikte parola bilgisini tespit etmeye çalışır [106].



Şekil 3.23. Ortadaki adam saldırısı yöntemi temsili

İkinci saldırı yöntemi, ağ trafiğini koklama/dinleme (Sniffing) olarak adlandırılan yöntemdir. Temsili olarak Şekil 3.24'de gösterilmiş olan bu saldırı yönteminde saldırgan ve hedefler aynı yerel ağ içerisinde olması gerekmektedir. Ancak saldırının etkili olabilmesi için sistemde göbek (hub) [107] adı verilen ağ cihazları olmalıdır. Bu ağ cihazı hedefe göndereceği paketleri tüm ağ cihazlarına gönderir, paketin sahibi paketi alır ve diğer ağ cihazları paketi reddeder. Ancak saldırgan bu paketleri reddetmez ve toplar. Daha sonra toplanan paketler içerisinde parola bulmak için tarama yapar. Bant genişliğini dolduran ve güvenlik açısından yeterli olmayan göbek (hub) ağ cihazları artık kullanılmamaktadır. Bu iki saldırı yönteminde Cain & Abel, ettercap, Arpspoof, Ngrep, Wireshark, karma, Tcpdump, Dsniff, SSLStrip gibi araçlar kullanılmaktadır [106,108].



Şekil 3.24. Ağ trafiği dinleme saldırı yöntemi temsili

Aktif çevrimiçi saldırılar

Bu saldırı yönteminde, yerel ağ veya internet üzerindeki herhangi bir hedefe, farklı araç ve yöntemler kullanılarak parola giriş ekranlarında üzerinden parola tahminleri denenerek sisteme sızmaya çalışılmaktadır. Aktif çevrim içi saldırılar için Kaba Kuvvet Saldırısı (*Brute Force Attack*)ve Sözlük Saldırısı (*Dictionary Attack*) olarak sıralanabilir.

Kaba Kuvvet Saldırıları

Parola tahminlerinin girilerek, parolanın bulunmaya çalışıldığı yöntemlerdir. Çok basit bir yöntem olmasının yanı sıra çok etkilidir. Eğer kullanılan parola zayıf ve tahmin edilebilir bir parola ise bu saldırı türü ile kolayca bulunulabilir. Ancak zaman, bu saldırı türünde kısıtlayıcı bir etkendir ve yeterli zamana ihtiyaç vardır [108,109]. Güçlü bir parola kullanıldığı takdirde, parolayı bulmak bu saldırı türü ile yıllar sürmektedir. Günümüzde bu saldırı mantığını kullanan otomatikleştirilmiş araçlar kullanılmaktadır. Bu araçlar başarılı olana kadar parolaları tahmin etmeye çalışmaktadır. Otomatikleştirilmiş araçlar, etkisini sadece zayıf ve basit parolalar üzerinde göstermektedir [105].

Sözlük Saldırıları

Saldırganın elinde belli kıstaslara göre oluşturulmuş kelime listesi (*wordlist*) adı verilen dosyalar bulunmaktadır. Bu kelime listeleri, hedef için özel olarak hazırlanmış (*örneğin sosyal ağlardan elde edilen bilgilerle*) veya genel olarak hazırlanmış (*örneğin Türkçe kelimelerin bulunduğu bir dosya*) olabilir. Sözlük saldırılarında kelime listeleri çeşitli araçlarla (*hydra, medusa, ncrack, xhyra vb.*) beraber kullanılarak hedef sistem üzerinde denemeler yapılarak parola tespit edilmektedir [87]. Şekil 3.25'de basit bir kelime listesinin içeriği gösterilmiş olup, Şekil 3.26'da hydra aracı ile bu kelime listesi kullanılarak yapılan bir saldırı sonucu görülebilmektedir. Bu saldırı türü çevrim içi kullanılabileceği gibi çevrim dışı olarak da kullanılabilir.

```
root@kali:~# cat passwordfile.txt
password
Password
password1
Password1
Password123
```

Şekil 3.25. Basit bir kelime listesi içeriği [105]

```
root@kali:~# hydra -L userlist.txt -P passwordfile.txt 192.168.20.10 pop3
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes

Hydra (http://www.thc.org/thc-hydra) starting at 2015-01-12 15:29:26
[DATA] 16 tasks, 1 server, 24 login tries (l:4/p:6), ~1 try per task
[DATA] attacking service pop3 on port 110
[110][pop3] host: 192.168.20.10   login: georgia   password: password❶
[STATUS] attack finished for 192.168.20.10 (waiting for children to finish)
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-01-12 15:29:48
```

Şekil 3.26. Hydra saldırıcı aracı ile yapılan bir sözlük saldırısı sonucu [105]

Çevrimdışı saldırılar

Bu saldırı yönteminde parolaların depolandığı bilişim sistemlerine erişilerek, parolalar elde edilmeye çalışılmaktadır. Depolanan parolalar düz metin, şifreli veya ileri bölümlerde ayrıntılı olarak açıklanacak olan kriptogarfik özet (*hash*) halinde tutulmaktadır [80]. Elde edilen parolaların düz metin hali dışındaki halleri çeşitli saldırı teknikleri kullanılarak çözümlemeye çalışılmaktadır. Gökkuşağı Tablosu Saldırısı (*Rainbow Attack*) ve Özet ile Geçiş (Pass The *Hash*) saldırısı olarak sırlanabilir. Özet ile Geçiş (*Pass The Hash*) [108] saldırı tekniği sadece Windows işletim sistemlerinde kullanılmaktadır [105]. Çevrim dışı saldırılar genellikle kriptogarfik özet (hash) halinde tutulan parolalar için gerçekleştirilmektedir.

Özet (Hash)

Özet *(Hash)* [110], karakterlerden oluşan bir girdi dizesinin, genellikle daha kısa, eşsiz ve sabit uzunlukta dönüştürülmüş şeklidir. Yani boyutuna bakılmaksızın herhangi bir veri, bir özet algoritmalarından biri kullanılarak, sabit boyuta sahip harf ve sayılardan oluşan tek yönlü bir özet üretir. Bu alfa-sayısal özet, veri girdisinin parmak izi gibidir. Veri de yapılacak en ufak değişiklik bile özetin değişmesine neden olur [111].

Özet algoritmaları şifreleme algoritması değildir. Şifreleme algoritmaları, bir anahtara bağlı olarak veriyi şifreler ve şifreli veri uygun anahtar kullanılarak deşifre edilir. Ancak Özet algoritmaları, tek yönlüdür ve aynı algoritma metodu kullanılarak asıl verinin elde edilmemesi maksadıyla tasarlanmışlardır. Yaygın olarak kullanılan bazı özet algoritmaları ve özellikleri Çizelge 3.5'de sunulmuştur [112,113].

Çizelge 3.5. Bazı özet algoritmaları özellikleri

Algoritma	Mesaj Boyutu (bit)	Blok Boyutu (bit)	Kelime Boyutu (bit)	Mesaj Özet Boyutu (bit)
SHA-1	$< 2^{64}$	512	32	160
SHA-256	$< 2^{64}$	512	32	256
SHA-384	$< 2^{128}$	1024	64	384
SHA-512	$< 2^{128}$	1024	64	512
MD5	$< 2^{64}$	512	32	128

Çizelge 3.5'deki algoritmalara ilave olarak NT ve NTLM algoritmaları da kullanılarak "Gazi Üniversitesi" kelimelerinin elde edilen özet bilgileri Çizelge 3.6'da sunulmuştur.

Çizelge 3.6 ve Çizelge 3.7. karşılaştırıldığında, Çizelge 3.7'deki aynı girdinin sadece ikinci kelimesinin ilk harfinin küçük olarak yazıldığını buna rağmen özetlerin tamamen farklı olduğu görülmektedir.

Çizelge 3.6. "Gazi Üniversitesi" olarak yapılan girdinin farklı özet algoritmaları ile elde edilen özet bilgisi

Girdi	Algoritma	Özeti
Gazi Üniversitesi	SHA-1	`7c3f744e8a56d8edf52a543c04619439aaad3012`
	SHA-256	`980601c6840e35df492f687eb01558b4cbc08cad3fb8332b7b01502bd60628af`
	SHA-384	`562b00a183422830e33c08d08ea7d891a58b7834e67bf4c92b6263ff2d879722284fad6459695e50d310dc157d316720`
	SHA-512	`f19411c203f1660c71ff28c2fd565169109461fec1bd9b8b611ab4dfe98e5c51fb7545c530a7d0cdc97c8e2bc10f903c29f659d080a2c43238116b12ad9053db`
	MD5	`2eb9957b4fda06c0b4fee127f212dd85`
	LM	`f9d5f28413f5caa76e102f4293e1a653`
	NTLM	`03092f1e8c6999a857c5366465659224`

Çizelge 3.7. “Gazi üniversitesi” olarak yapılan girdinin farklı özet algoritmaları ile elde edilen özet bilgisi

Girdi	Algoritma	Özeti
Gazi üniversitesi	SHA-1	201f35ac589b6493e48c75053aabbba740b9f271
	SHA-256	7365e13e4c4e9ac2e81c976c0535b831cb19e6c0ecdd4c843e8f7a0719146f8b
	SHA-384	2072fa30c5948c21f4df4b7eaf3208d800332ac1b234674453f460588920b9a5130c209197b20368829435c10decbfb3
	SHA-512	622db3f13f08f02d354fd31c3a925338ab1177c7ce59489a41a1f9be794ca86e2b7c52a64879fa1bcd1c21988f67056c5005103b8f50875a908b01edd52b8731
	MD5	d8425490267980c57ff09350f48a715c
	LM	afb1d12b0c8ee47d6e102f4293e1a653
	NTLM	d68358f7f20fd781d2626cc416e18a02

Gökkuşağı Tablosu Saldırısı (Rainbow Attack)

Özet halleri elde edilen parolaların düz metin olarak tespit edilmesini sağlayan yöntemdir. Oluşturulan kelime listelerinin uygun algoritmalar ile özetleri çıkarılarak gökkuşağı tablosuna girilir. Daha sonra kurbandan elde edilmiş olan parola özetleri ile gökkuşağı tablosuna girilenler karşılaştırılarak parolanın düz metin hali elde edilmeye çalışılır. Şekil 3.27’de *The Powerful RainbowCrack* aracı kullanılarak gerçekleştirilen bir gökkuşağı saldırısından elde edilen parolalar gösterilmektedir [114].

-::TYPE	-::HASH	-::PASS	-::STATUS	-::TIME	-::SUBMITED
md5	7e89bcc6151b24992a255cd665d4aa16		waiting	0:0:46	2006-11-11 10:45:31
md5	0696eeaff05bf2105b0bcf6d93ac73a0		waiting	0:0:47	2006-11-11 10:45:30
md5	c32cf089d464d3ed1a3af347ae208188		processing3	0:25:6	2006-11-11 10:21:11
md5	c6fe5851aff10a64e8a52e82b323304f		processing3	0:46:29	2006-11-11 09:59:48
md5	a79c879d28c5c8a4707d52bbaa57607f	12050	cracked	0:45:41	2006-11-11 09:51:43
md5	a79e1c64d27737e3f959a6a56b41c650		processing3	0:57:18	2006-11-11 09:48:59
md5	2ef5b8b0eee93568a1126bb923664057		processing3	0:57:36	2006-11-11 09:48:41
md5	e53cc072934b25e45dc273c6c342556d		processing3	0:58:7	2006-11-11 09:48:10
md5	d38ad0e58c9525343f492161b87400a1	htmldb	cracked	0:58:23	2006-11-11 09:44:01
md5	d926dbaeb7fac97612ec219f7f172610		processing3	1:4:30	2006-11-11 09:41:47
md5	fcf2483ced17683085849877134fd50c		processing3	1:6:32	2006-11-11 09:39:45
md5	377a8f80271a6f920df0e4aa84d1029a	bombi	cracked	0:43:12	2006-11-11 09:38:26
md5	85d95e2ad51bfcd5d6d352486fbe2769	pupsi	cracked	1:8:2	2006-11-11 09:28:25
md5	96bc2c727049b5dce27bd8b9e8b264bf		processing3	1:19:6	2006-11-11 09:27:11
md5	8aa12bbde69504ba86b942726b4d7623		notfound	1:18:15	2006-11-11 09:02:54
md5	5ce1d809749963448767622e0ca8169f	28264451	cracked	0:48:15	2006-11-11 09:02:35

Şekil 3.27. The powerful rainbowcrack aracıyla gerçekleştirilen örnek saldırı sonucu [114]

Özet ile Geçiş (Pass The Hash) saldırısı

Pass the Hash saldırı tekniği ilk defa 1997 yılında Paul Ashton tarafından "NT Pass The Hash" istismarı olarak duyuruldu [115-117]. Bu saldırı yöntemi kullanılarak yapılan saldırılar günümüzde halen kullanılmaktadır. Parolaların özet halinde saklanması, Windows'un sunulan bir özelliği olması nedeniyle bu saldırılar Windows işletim sistemlerini tehdit etmeye devam etmektedir [118].

Bazı işletim sistemlerinde, bir parolaya ait özet ile parolanın açık metin hali birbirinin muadilidir ve parolanın yerine özeti kullanılabilmektedir. Saldırganlar, sisteminize ait parolanın özetini ele geçirirse parolaya ihtiyaç olmadan sisteminize erişmektedir. Bu saldırı yöntemine Özet ile Geçiş (Pass The Hash) saldırısı adı verilmektedir. Genellikle Windows işletim sistemlerine karşı kullanılmaktadır [116]. Bunun yanı sıra bazı web uygulamalarında ve Kerberos kullanan Linux sistemlere karşı da kullanılmaktadır. Linux işletim sistemleri parola bilgisini, Windows işletim sistemlerinden farklı bir yöntemle etc/shadow dosyası altında saklar ve bu nedenle özet ile geçiş saldırısı tüm Linux işletim sistemlerine karşı kullanılamamaktadır. Bu saldırı tekniği için hasdump, fgdump, John The Ripper, Cain&Abel gibi araçlar kullanılır [105]. Hashdump saldırı aracı ile bir Windows işletim sisteminden elde edilen parola bilgileri şekil 3.28'de sunulmuştur.

```
meterpreter > hashdump
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
georgia:1003:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:df40c521ef762bb7b9767e30ff112a3c:938ce7d211ea733373bcfc3e6fbb3641:::
```

Şekil 3.28. Windows işletim sisteminden hashdump ile elde edilen parola bilgileri [105]

Teknik olmayan saldırılar

Bu saldırı yöntemi daha çok insani ilişkileri ve zaafları kullanarak karşı tarafın doğrudan parolasını öğrenmek veya farkında olmadan çeşitli yöntemlerle kendisi tarafından saldırgana verilmesini sağlamayı amaçlamaktadır. Kurbanı parolasını girerken izlemek, telefon veya sahte e-postalar aracılığıyla parolasını saldırganın yönlendireceği alanlara girmeye ikna etmek, çöplerde parola yazılı veya parolanın tahmin edilmesini sağlayacak atıkları aramak gibi tamamen beşeri zaaflara dayanan bir saldırı yöntemidir. Basit olmasına rağmen oldukça etkili bir yöntemdir [119,120].

4. METOD VE MATERYAL

Dizin yapısına dâhil bilgisayarlara ait parolaları korumak, ayrıcalıklı hesapları kontrol etmek, siber saldırılardan korunmak ve BT güvenlik prosedürlerine uyumluluğu sağlamak maksadıyla farklı birçok ticari uygulama çözümleri kullanılmaktadır. Bu çalışmada geliştirilen AHEKS, bu uygulamalarla eş değer işlevlere sahiptir. AHEKS, eş değer işlevlere sahip uygulamaların sahip olduğu ayrıcalıklı hesap yönetimi temel işlevine ilave olarak sunduğu yerel yönetici hesapları yönetimi ve diğer hizmetler sayesinde kuruluşların tüm ihtiyaçlarına cevap verebilecek yetenektedir.

Eşdeğer uygulamalar ile AHEKS sistemi arasındaki karşılaştırmalar Çizelge 4.1'de sunulmuştur. Söz konusu uygulamalar incelendiğinde, farklı birçok ek özelliğe sahip olduğu görülmektedir. Ancak AHEKS sisteminin de diğer uygulamalarla farklılıklar gösteren ve kuruluşun ihtiyaç durumuna göre avantaj sağlayacak yönleri bulunmaktadır.

Eş değer işlevlere sahip uygulamalar incelendiğinde, temel BT güvenlik ihtiyaçlarından biri olan dizin hizmeti için ayrıcalıklı hesap erişim kontrolü özelliğine sahip olduğu görülmektedir. Ancak bazılarında diğer bir BT güvenlik sorunu olan yerel yönetici hesaplarının parola kontrolünü sağlayacak özellikler bulunmamakta veya ayrıca alınacak lisanslar ile bu özellikler eklenmektedir.

Tahmin edilebilir veya basit bir parola kullanıldığı takdirde *Sözlük Saldırıları* ya da *Kaba Kuvvet Saldırıları* gibi saldırı yöntemleri ile yerel yönetici hesaplarına ait parolalar ele geçirilebilmektedir. Güçlü ve tahmin edilmesi zor parolalar kullanıldığı durumlarda bile *Özet ile Geçiş (Pass The Hash) Saldırı* ile yerel yönetici hesap parolaları ele geçirilebilmektedir [116,121]. Dizin yapısında bir bilgisayarın yerel yönetici hesabının ele geçirilmesi tüm sistemin saldırganlar tarafından ele geçirilmesine neden olabileceğinden yerel yönetici hesaplarına ait parolaların yönetimi ihmal edilmemelidir [105].

Parola saldırılarının tartışıldığı Bölüm 3 içerisinde açıklanan, saldırı yöntemleri incelendiğinde, bu iki işlevin birbirinden ayrı olarak düşünülemeyeceği anlaşılmaktadır. Bu yapı incelendiğinde AHEKS uygulamasının bu özelliği ile öne çıktığı değerlendirilmektedir. Bunun yanı sıra eşdeğer işlevlere sahip uygulamaların raporlama ve işlemlerin kayıt altına alınması konusunda daha fazla özelliğe sahip olduğu görülmektedir.

Eşdeğer işlevlere sahip uygulamaların yanı sıra Çizelge 4.1'de yer alan ve yerel yönetici hesaplarının yönetimi ile ilgili sorunu çözmek amacıyla Microsoft tarafından *Local Administrator Password Solution* aracı geliştirilmiş [122] ve Mayıs 2015'te yayımlanmıştır. Bu araç, sadece Windows işletim sistemine sahip ve Microsoft'a ait bir dizin hizmeti uygulaması olan *Aktif Dizin* içerindeki bilgisayarların yerel yönetici hesaplarının parolalarını kontrol ve yönetimini sağlamaktadır.

Ayrıcalıklı hesapların hiçbir sınırlamaya tabi tutulmadan BT personelinin kullanımına sunulması kuruluş içerisinde BT güvenliği sorunlarına neden olabilmektedir. BT personelinin sorumlu olduğu bilişim sistemleri bileşenleri dışındaki erişimleri engellenmelidir [50]. BT altyapısı üzerindeki yetkiler, görevlendirmeler temel alınarak düzenlenmeli ve BT personeli görevlerine dayalı bir kimlik yönetimine tabi tutulmalıdır. AHEKS ve eş değer işlevlere sahip diğer uygulamaların temel görevlerinden biride bunu sağlamaktır.

Çizelge 4.1'de yer alan uygulamalar incelendiğinde menşeinin yurt dışı olduğu ve ücretli ticari yazılımlar olduğu görülmektedir. AHEKS ayrıca bir maliyet gerektirmemesi ve yerli bir uygulama olması nedeniyle diğerlerine göre avantaj sağlamaktadır.

AHEKS, yerel yönetici hesaplarının ve dizin hizmeti ayrıcalıklı hesaplarının yönetimini bir bütün halinde sunması sayesinde diğer uygulamalardan ayrılmaktadır. Esnek yapısı, kuruluşa özel olarak şekillendirilebilmesi, maliyet gerektirmemesi, sade olması ve gereksiz ayrıntıdan uzak temel BT güvenlik ihtiyaçlarına yönelik modüllere sahip olması uygulama modelinin öne çıkan özellikleridir. Ayrıca uygulamadan faydalanacak personelin sisteme dâhil edilmesi aşamasında güçlü bir onay mekanizmasına sahip olması AHEKS'i daha güvenli hale getirmiştir. Maliyet gerektirmemesi, gereksiz ayrıntılardan arındırılmış olması ve temel BT güvenlik ihtiyaçlarının ön planda tutulması AHEKS ile diğer uygulamalar arasında önemli bir fark yaratmaktadır. Ancak kuruluşların eşdeğer işlevlere sahip uygulamalar ile AHEKS arasında yapacağı seçim öncesinde ihtiyaçların ön planda olduğu bir değerlendirmede bulunmaları gereksiz maliyetlerin ve kullanılmayacak özelliklerin yaratacağı karmaşayı engelleyecektir.

Çizelge 4.1. Uygulama karşılaştırma çizelgesi

Uygulama Adı	Menşei	Dizin Hizmeti Ayrıcalık Hesap Erişim Kontrolü	Yerel Yönetici Hesapları Parola Kontrolü	Sistem İçi Onay Mekanizması	Maliyet	Kimlik Dayalı Erişim Kontrolü	Diğer
CyberArk: Privileged Account Security Solution	ABD	+	+*	Kısmen	Ücretli	+	▪ Tek seferlik ayrıcalık tanıma seçeneği, ▪ Farklı uygulamalar için uygulamaya dayalı yetkilendirme seçeneği , ▪ Mobil erişim desteği, ▪ Farklı tehdit algılama sistemlerine uyumluluk.
https://www.cyberark.com/products/privileged-account-security-solution/							
CA Technologies: Privileged Access Manager Server Control	ABD	+	-	Kısmen	Ücretli	+	▪ Acil durumlar için ayrıcalıklı hesap erişimi, ▪ Ayrıcalıklı kullanıcı hesapları tespit mekanizması, ▪ Farklı modüller için birleştirilmiş ara yüz.
https://www.ca.com/us/products/ca-privileged-access-manager-server-control.html							
ManageEngine: Privileged Password Manager for Enterprises	ABD	+	-	Kısmen	Ücretli	+	▪ Paylaşılan yönetimsel parola yönetimi, ▪ Merkezi parola kasası, ▪ Uzak oturum açma imkânı, ▪ Ayrıcalıklı oturum video kaydı, ▪ İki etkenli kimlik doğrulama, ▪ Mobil erişim desteği.
https://www.manageengine.com/products/passwordmanagerpro/							
Thycotic: Privileged Account Management	ABD	+	+	Kısmen	Ücretli	+	▪ İki faktörlü kimlik doğrulama ▪ IP kontrollü erişim ▪ Mobil erişim desteği ▪ Ayrıcalıklı oturum video kaydı
http://thycotic.com/products/secret-server/							
Lieberman Software: Enterprise Random Password Manager	ABD	+	+*	Kısmen	Ücretli	Kısmen	▪ Ayrıcalıklı oturum video kaydı, ▪ Farklı uygulamalar için uygulamaya dayalı yetkilendirme seçeneği.
http://www.liebsoft.com/Enterprise_Random_Password_Manager/							
IBM: Security Privileged Identity Manager	ABD	+	-	Kısmen	Ücretli	+	▪ Ayrıcalıklı hesap işlemlerini ve kimlik doğrulama adımlarını kaydeder. ▪ Ayrıcalıklı hesaplarını kullanımı için süre sınırlaması
http://www-03.ibm.com/software /products/tr/pim							
Oracle: Privileged Account Manager	ABD	+	-	+	Ücretli	+	▪ Farklı etki alanı desteği ▪ Linux ve Unix sistemlerde kullanılır. ▪ Farklı uygulamalar için uygulamaya dayalı yetkilendirme seçeneği ▪ Ayrıcalıklı oturum video kaydı
http://www.oracle.com/technetwork/middleware/id-mgmt/overview/opam-homepage-1697430.html							

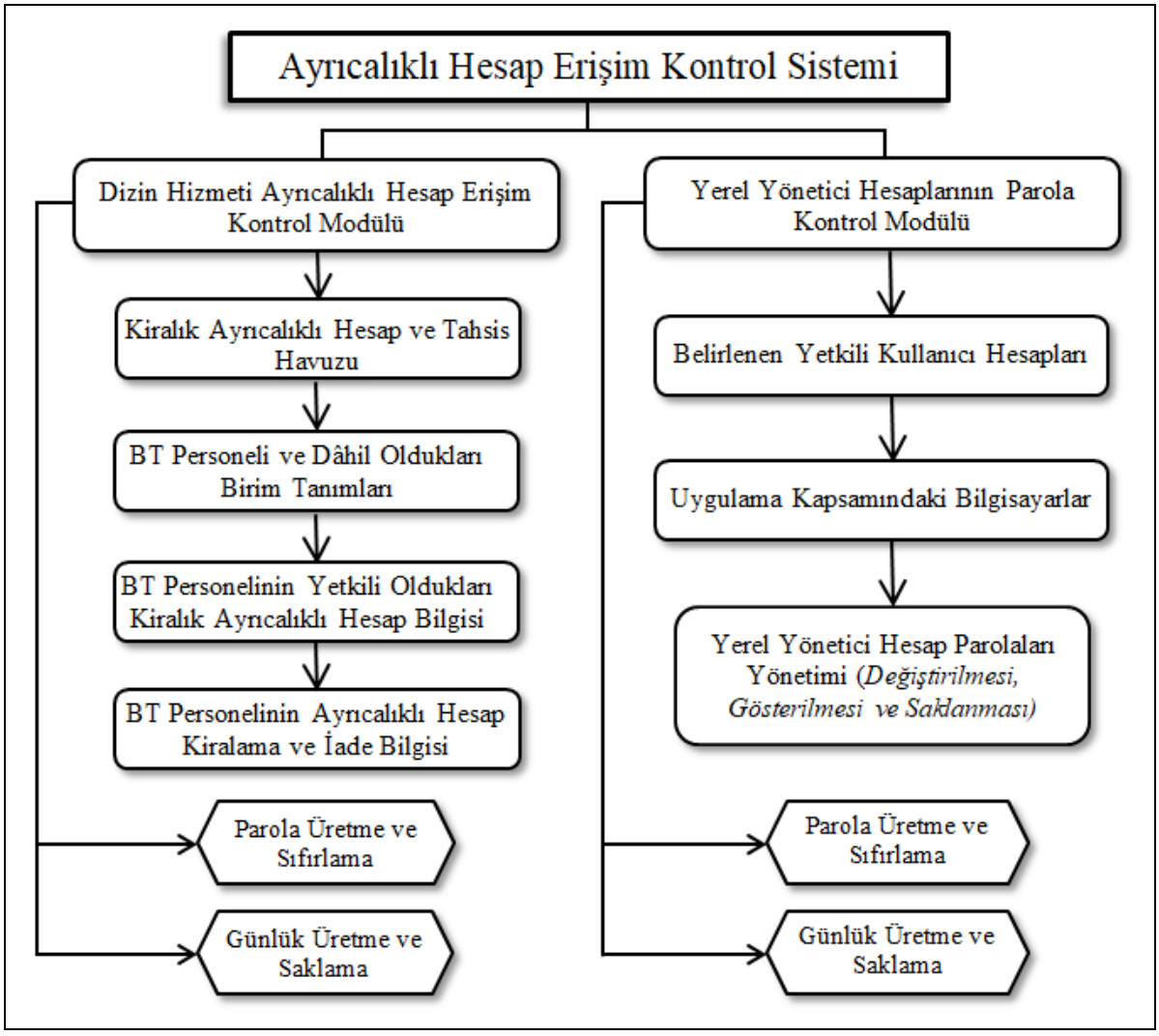
Çizelge 4.1. (devam) Uygulama karşılaştırma çizelgesi

Uygulama Adı	Menşei	Dizin Hizmeti Ayrıcalık Hesap Erişim Kontrolü	Yerel Yönetici Hesapları Parola Kontrolü	Sistem İçi Onay Mekanizması	Maliyet	Kimlik Dayalı Erişim Kontrolü	Diğer
Quest: Identity and Access Management Solutions	ABD	+	-	+	Ücretli	+	▪ Farklı etki alanı desteği ▪ Rapor üretme ▪ Çok faktörlü kimlik doğrulama ▪ Uzak oturum açma imkânı ▪ Rapor üretme
https://www.quest.com/solutions/identity-and-access-management							
Beyondtrust: The PowerBroker Privileged Access Management Platform	ABD	+	+	Kısmen	Ücretli	+	▪ Gerçek zamanlı oturum izleme, ▪ Şifre, kullanıcı ve hesap davranış analizi, ▪ Bütünleşik ayrıcalıklı tehdit analizi, ▪ Ayrıcalıklı hesapların tespit edilmesi.
https://www.beyondtrust.com/solutions							
Centrify :Privileged Identity Management	ABD	+	+	+	Ücretli	+	▪ Dinamik ayrıcalıklı hesap yönetimi, ▪ Süreye dayalı ayrıcalık tanımları, ▪ İşlemler için kullanıcıların kendi hesaplarının kullanımı
https://www.centrify.com/products/server-suite/privilege-management/							
Local Administrator Password Solution	ABD	-	+	-	Ücretsiz	-	▪ Microsoft tarafından "Pass The Hash" olarak bilinen saldırılara karşı geliştirilmiş ve sadece Windows işletim sistemlerinde kullanılan bir uygulama
https://technet.microsoft.com/en-us/library/security/3062591.aspx							

* *ilave lisans gerektirmektedir.*

5. AYRICALIKLI HESAP ERİŞİM KONTROL SİSTEMİ UYGULAMA MODELİ

Dizin hizmetindeki ayrıcalıklı hesapların parolaları ve aynı ağ içerisinde yer alan bilgisayarların yerel yönetici hesaplarının parolalarına gerçekleştirilebilecek saldırıları engellemek, kurumsal olarak bilişim teknolojilerinin kullanımında kimlik yönetimini sağlıklı bir şekilde yürütebilmek maksadıyla *Ayrıcalıklı Hesapların Erişim Kontrol Sistemi* (AHEKS) modeli geliştirilmiştir. Geliştirilen model, *Dizin Hizmeti Ayrıcalıklı Hesap Erişim Kontrol Modülü* ve *Yerel Yönetici Hesaplarının Parola Kontrol Modülü* olarak iki temel bileşenden meydana gelmektedir (Şekil 5.1) ve mekanizmanın tam anlamıyla görevini yerine getirebilmesi bu iki modülün bir arada çalışması ile mümkün olmaktadır.

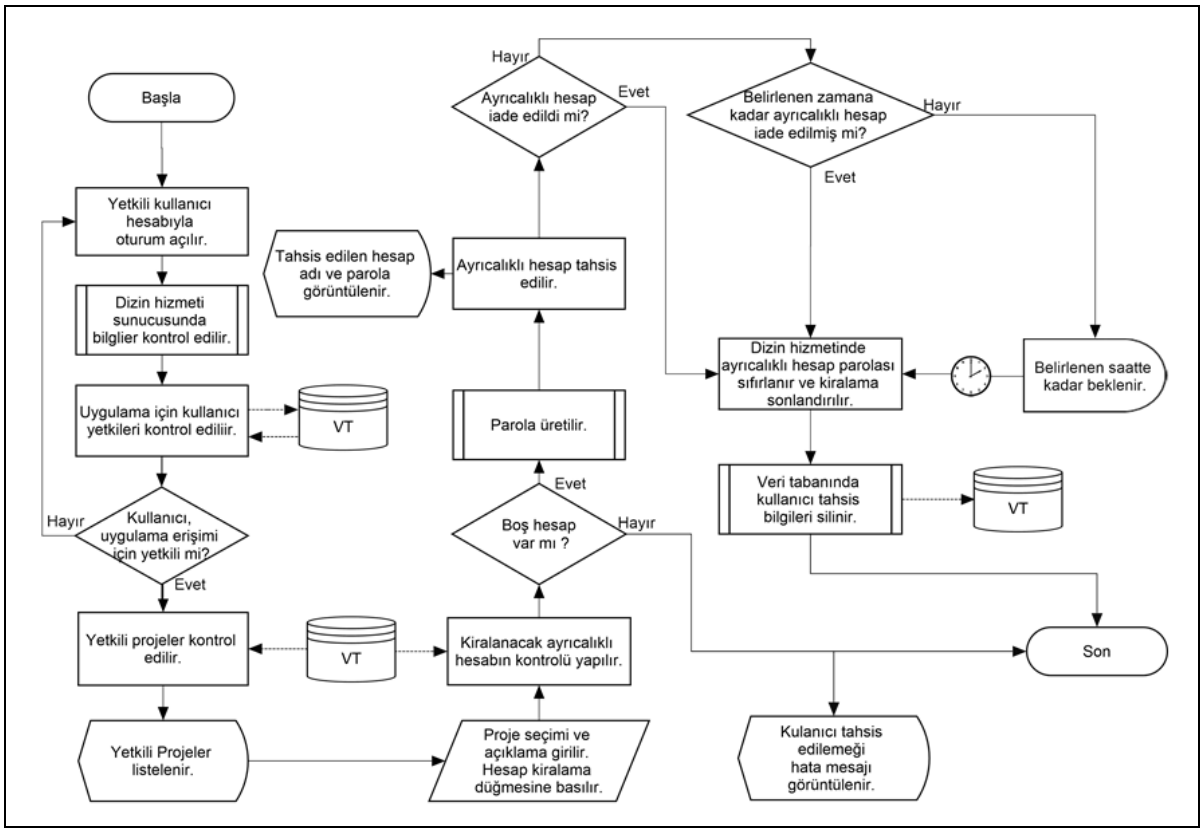


Şekil 5.1. Ayrıcalıklı hesap erişim kontrol sistemi uygulama model şeması

AHEKS'in ilk ana modülü, dizin hizmeti içerisindeki ayrıcalıklı hesap güvenliğini ve yönetimini sağlayan *Dizin Hizmeti Ayrıcalıklı Hesap Erişim Kontrol* modülüdür. Bu ana modül altı alt işlevi barındırmaktadır. İkinci ana modül, dizin ağaç yapısında aynı etki alanındaki bilgisayarların yerel yönetici hesaplarına ait parolaların güvenlik ve yönetimini sağlayan *Yerel Yönetici Hesaplarına Ait Parola Kontrol* modülüdür. İkinci ana modül, altı alt işlevden meydana gelmektedir (Şekil 5.1). Ayrıca arka planda tüm sistemin kullandığı, farklı işlevler için farklı tablolar barındıran, günlük kayıtların tutulduğu ve BT altyapısı içerisinde ağ güvenlik cihazlarıyla korunan güvenli bir alana konumlandırılmış AHEKS'e ait veri tabanı yer almaktadır.

5.1. Dizin Hizmeti Ayrıcalıklı Hesap Erişim Kontrol Modülü

Dizin hizmeti ayrıcalıklı hesap erişim kontrol modülü, dizin hizmetinde bulunan ayrıcalıklı hesap sayısının düşürülmesi ve bu hesapların sadece ihtiyaç halinde yetki verilen kişilerce kiralanması işlevini yerine getirmektedir (Şekil 5.2). Bu modül sayesinde ayrıcalıklı hesap kiralayan bir kullanıcı, yetkililer tarafından belirlenen kriterler doğrultusunda hareket etmek zorunda kalmaktadır.

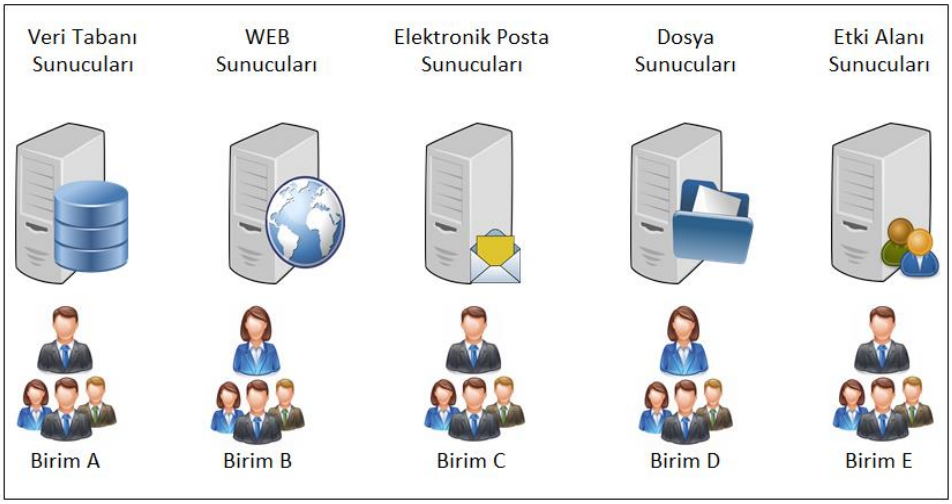


Şekil 5.2. Dizin hizmeti ayrıcalıklı hesap erişim kontrol modülü temel iş akışı

Dizin hizmeti ayrıcalıklı hesap erişim kontrol modülünü oluşturan altı alt modül, ana modülün temel yapı taşlarıdır. Bu alt modüller, kurumsal yapının organizasyon biçimine göre arttırılabilir veya ufak değişiklikler yapılabilir. Ancak bu modülün doğru çalışması temel altı alt modüllün varlığına bağlıdır. Birinin bile eksiltilmesi hedeflenen amacı tehlikeye sokacaktır.

5.1.1. Kiralanacak ayrıcalıklı hesaplar ve hesap gruplarının oluşturulması

Bu modülün işlevini yerine getirmesi için öncelikle Şekil 5.3'de örneği verildiği gibi her bir BT personelinin sorumlu olduğu projeler ve birim liderleri belirlenmelidir. Daha sonra BT personelinin kiralayacağı ayrıcalıklı hesaplar ve tahsis havuzu oluşturulmalıdır. Burada proje terimi ile anlatılmak istenen, web sunucuları, yazıcı sunucuları, etki alanı kontrol sunucuları elektronik posta sunucuları, dosya sunucuları veri tabanı sunucuları vb. sunucularda yapılacak işlemlerdir.



Şekil 5.3. Örnek proje sorumluluk dağılımı

BT personelinin sorumlu olduğu projeye göre her birim için dizin yapısında farklı bir kullanıcı grubu oluşturulur. Oluşturulan gruplara, örnek olarak Şekil 5.4'de gösterildiği şekilde projelerle ilişkili uygun bir isimlendirme yapılır.

Dizin hizmetinde her proje için farklı olacak şekilde kullanıcı gruplarının oluşturulmasının ardından ilgili birim için yeterli sayıda kiralanacak hesaplar oluşturulur. Oluşturulan hesapların sayısı, birimdeki personel sayısına veya ilgili projede eş zamanlı çalışacak personel sayısına göre belirlenmelidir.

Dizin yapısında oluşturulan kullanıcı gruplarının ve kiralanacak hesapların, hangi projeler için yetkilendirildiği bilgisi veri tabanında *kullanıcı grupları→sorumlu birim→proje tanımı* bilgilerinin eşleştirmesi maksadıyla Çizelge 5.1'de sunulduğu şekilde veri tabanı içerisinde bunu tanımlayacak bir tablo oluşturulmaktadır

Grup Adı	Açıklama	Kiralanacak Hesaplar
VTYNTGRP	Veri Tabanında İşlem Yapmaya Yetkili Grup	Vtynthsp01
		Vtynthsp02
		Vtynthsp03
WEBYNTGRP	WEB Sunucularında İşlem Yapmaya Yetkili Grup	Webynthsp01
		Webynthsp02
		Webynthsp03
EPOSYNTGRP	E-Posta Sunucularında İşlem Yapmaya Yetkili Grup	Epstynthsp01
		Epstynthsp02
		Epstynthsp03
DOSYNTGRP	Dosya Sunucularında İşlem Yapmaya Yetkili Grup	Dosynthsp01
		Dosynthsp02
		Dosynthsp03
EAYNTGRP	Etki Alanı Sunucularında İşlem Yapmaya Yetkili Grup	Eaynthsp01
		Eaynthsp02
		Eaynthsp03

Şekil 5.4. Örnek dizin hizmeti kullanıcı grupları ve kiralanacak hesaplar

Çizelge 5.1. Örnek kullanıcı grupları, proje tanımları ve sorumlu birim eşleştirme tablosu

Sorumlu	Birim	Açıklama
VTYNTGRP	Birim A	Veri tabanında işlem yapmaya yetkili grup
WEBYNTGRP	Birim B	WEB sunucularında işlem yapmaya yetkili grup
EPOSYNTGRP	Birim C	E-Posta sunucularında işlem yapmaya yetkili grup
DOSYNTGRP	Birim D	Dosya sunucularında işlem yapmaya yetkili grup
EAYNTGRP	Birim E	Etki Alanı sunucularında işlem yapmaya yetkili grup

Dizin yapısında oluşturulmuş olan kullanıcı gruplarının ilgili proje kapsamında yetkilendirme yapılmalıdır. Yetkilendirme işlemleri, oluşturulan kullanıcı gruplarının sorumlu olduğu proje kapsamındaki sunucularda yerel yönetici grubuna (*Administrators*) eklenerek yapılmaktadır. Burada dikkat edilmesi gereken ve diğer projelerden farklı olarak, veri tabanında işlem yapmaya yetkili kullanıcı grubu ek olarak veri tabanı uygulamasının yönetici hesapları grubuna da dâhil edilmektedir. Bunun nedeni veri tabanı uygulamasına oturum açma işlemi için kiralık hesapların kullanılmasını sağlamaktır.

Dizin yapısında ve sunucularda yukarıda belirtilen işlemlerin yapılmasının ardından BT personeline ait etki alanı yöneticisi yetkilerine sahip hesapların yetkileri alınarak, BT birimlerinde görevli olmayan normal bir personele ait hesaplarla aynı yetkilere çekilmelidir. Bu sayede BT personeli, görevlerini yerine getirirken yönetici haklarına sahip bir hesaba ihtiyaç duyduğu durumlarda AHEKS'i kullanması sağlanmaktadır.

5.1.2. Kiralık ayrıcalıklı hesap ve tahsis havuzu ile BT personelinin ilişkilendirme işlemleri

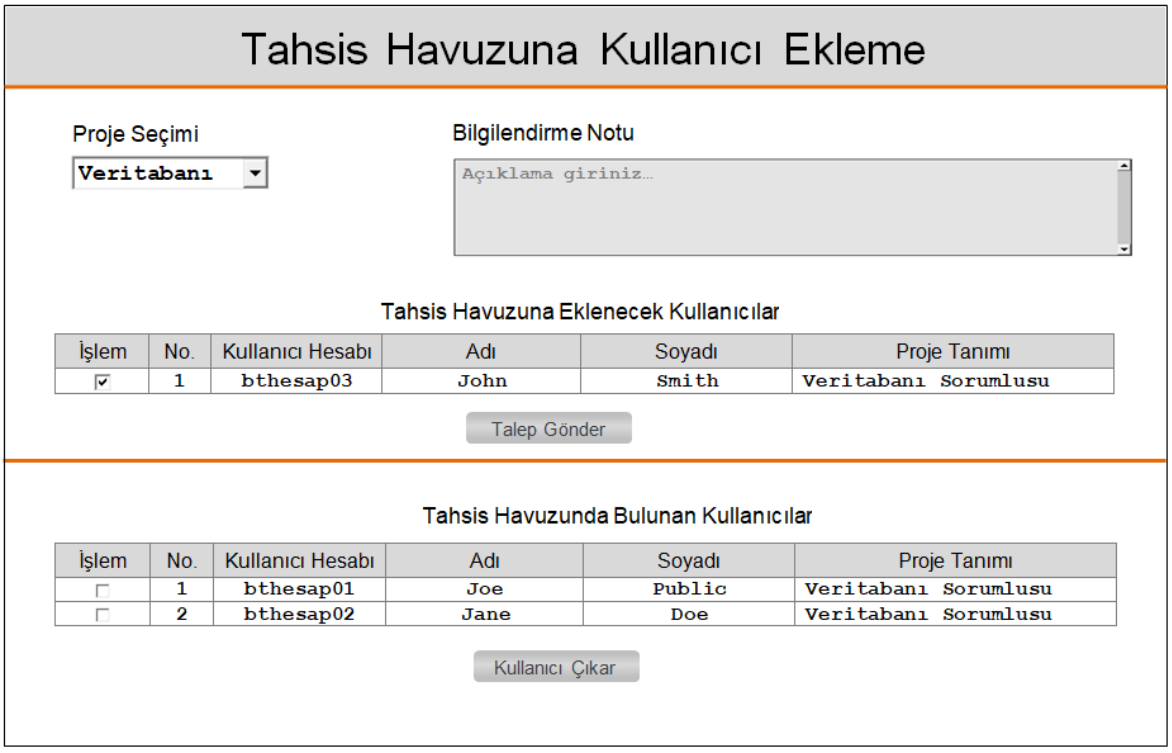
BT personelinin *dizin hizmeti ayrıcalıklı hesap erişim kontrol* modülünden faydalanabilmesi için sisteme dâhil edilmelidir. Kullanıcı dâhil etme yetkisi, belirlenen kullanıcıya/kullanıcılara verilebileceği gibi daha önce farklı projeler için oluşturulmuş birim liderlerine de verilebilir. Bu sorumluluğun birim liderlerine verilmesi ayrıcalıklı hesapları kullanacak kişilerin tespitini ve takibini daha güvenilir kılacaktır. Sisteme dâhil edilecek kullanıcı için ilk talep birim lideri tarafından yapılır. Birim liderinin kimler için talepte bulunabileceği ve hangi personelden sorumlu olduğu bilgileri, AHEKS'e ait veri tabanı üzerinde oluşturulacak ve örnek bilgilerle Çizelge 5.2'de sunulan, benzer değerlerin saklandığı bir tabloda tutulur. Yeni katılan bir personelin modülü kullanabilmesi için birim personelinin ve sorumlu liderinin bilgilerinin ilişkilendirildiği tabloya eklenmelidir.

Tahsis havuzuna eklenecek BT personeli için birim lideri tarafından BT güvenliğinden sorumlu yöneticiye *tahsis havuzuna kullanıcı ekleme* ara yüzü üzerinden talep gönderilmektedir. Talep sadece birim liderinin AHEKS veri tabanında Çizelge 5.2'de gösterildiği gibi lideri olduğu birimde görevli BT personeli için gerçekleştirilmektedir.

Çizelge 5.2. Veri tabanı örnek kullanıcı hesapları ilişkilendirme tablosu

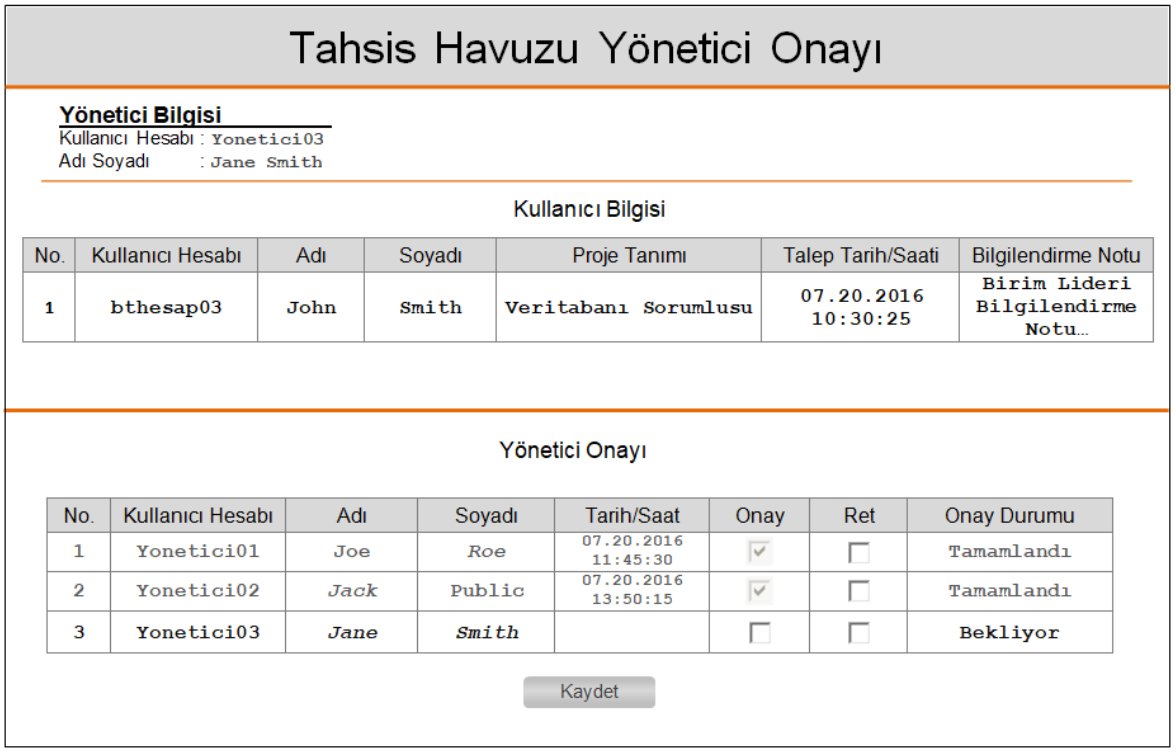
ID	Sorumlu	Birim	Açıklama	Hesap1	Hesap1	Hesap3
1	brmAkul01	A	Birim A Lideri	brmAkul02	brmAkul03	brmAkul04
2	brmBkul01	B	Birim B Lideri	brmBkul02	brmBkul03	brmBkul04
3	brmCkul01	C	Birim C Lideri	brmCkul02	brmCkul03	brmCkul04
4	brmDkul01	D	Birim D Lideri	brmDkul02	brmDkul03	brmDkul04
5	brmEkul01	E	Birim E Lideri	brmEkul02	brmEkul03	brmEkul04

Birim lideri, Şekil 5.5'te ekran görüntüsü sunulan *Tahsis havuzuna kullanıcı ekleme* arayüzünden birim lideri talep işlemi yaparak üç aşamalı onay mekanizmasını başlatır. Bu modül, birim liderinin sorumlu olduğu birim personeli için talep gönderecek şekilde yapılandırılmıştır. Talep için onay verecek üç yönetici (*sayı kuruluşun yapısına göre değişiklik gösterebilir*) daha önceden tespit edilmelidir. Birim lideri tahsis havuzuna dâhil edilmesini talep ettiği kullanıcı için bilgilendirme amaçlı bölüme talebin gerekçesi ve ilgili personel hakkında kısa bir açıklama notu ekleyerek onay verecek yetkilileri bilgilendirir.



Şekil 5.5. Tahsis havuzuna kullanıcı ekleme ara yüzü ekran görüntüsü

Birim liderinin talep gönder düğmesine basmasının ardından onay mekanizmasındaki ilk onaylayacak yöneticiye bilgilendirme amaçlı olarak içeriğinde onay bekleyen personel bilgileri ve birim liderinin bilgilendirme notu bulunan bir elektronik posta iletilmektedir. Onay verecek yöneticilerin oturum açtıkları tahsis havuzu yönetici onayı arayüzünde, onay işlemiyle ilgili temel bilgiler ve onay işleminin hangi aşamada olduğunu gösteren bir tablo mevcuttur (Şekil 5.6). Üçlü onay mekanizması tamamlandığı zaman, son onayın tarihi arayüzde yer alan tabloya yazılarak tahsis havuzuna ekleme işlemi tamamlanmaktadır.



Şekil 5.6. Tahsis havuzu yönetici onayı arayüzü ekran görüntüsü

Onay işlemleri arayüzde yer alan tablodaki sıralamaya göre ilerlemektedir. Her yönetici onayının ardından bir sonraki yöneticiye bilgilendirme için bir e-posta gönderilmektedir. Tablodaki onay kutucuğu, sırası gelmeyen yönetici için pasif durumdadır ve sırası gelmeden aktif duruma geçmeyecektir. Bu sayede yöneticiler kendisine sıra gelmeden onay işlemini gerçekleştiremeyecektir. Tahsis havuzu yönetici onayı arayüzünde bulunan üçlü onay mekanizmasındaki bilgilerin aynısı veri tabanında bir tabloda da tutulmaktadır. Üçlü onay mekanizmasının tamamlanmasının ardından söz konusu BT personeli, birim lideri tarafından görevlendirildiği proje/projeler için AHEKS'e oturum açarak ayrıcalıklı hesap kiralama arayüzü vasıtasıyla ayrıcalıklı hesap kiralayabilecektir.

Tahsis havuzuna dâhil edilen BT personelinin herhangi bir nedenle (iş akdinin feshedilmesi, farklı görevlendirme, başka birime atama, istifa vb.) bulunduğu görevden ayrılması durumunda sistem dışına çıkartma işlemi birim lideri tarafından gerçekleştirilmektedir. BT personelinin sisteme dâhil edilmesi bir onay mekanizmasına bağlı olmasına karşın, sistemden çıkarılması birim liderinin sorumluluğundadır.

Birim lideri, Şekil 5.5'te görülen *tahsis havuzunda bulunan kullanıcılar* tablosunda, sorumlu olduğu birim de görevli havuzdan çıkarılacak personelin bulunduğu satırın ilk sütunundaki onay kutucuğunu işaretler ve çıkar düğmesine basarak kullanıcının tahsis havuzu dışına çıkartılmasını sağlar. Özellikle hoş olmayan bir nedenle yaşanabilecek bir işten çıkarma durumunda, işten çıkarılacak BT personelinden önce birim liderine haber verilerek söz konusu personelin sistem dışına çıkarılması sistemi intikam amaçlı yapılabilecek olası bir saldırıdan koruyacaktır.

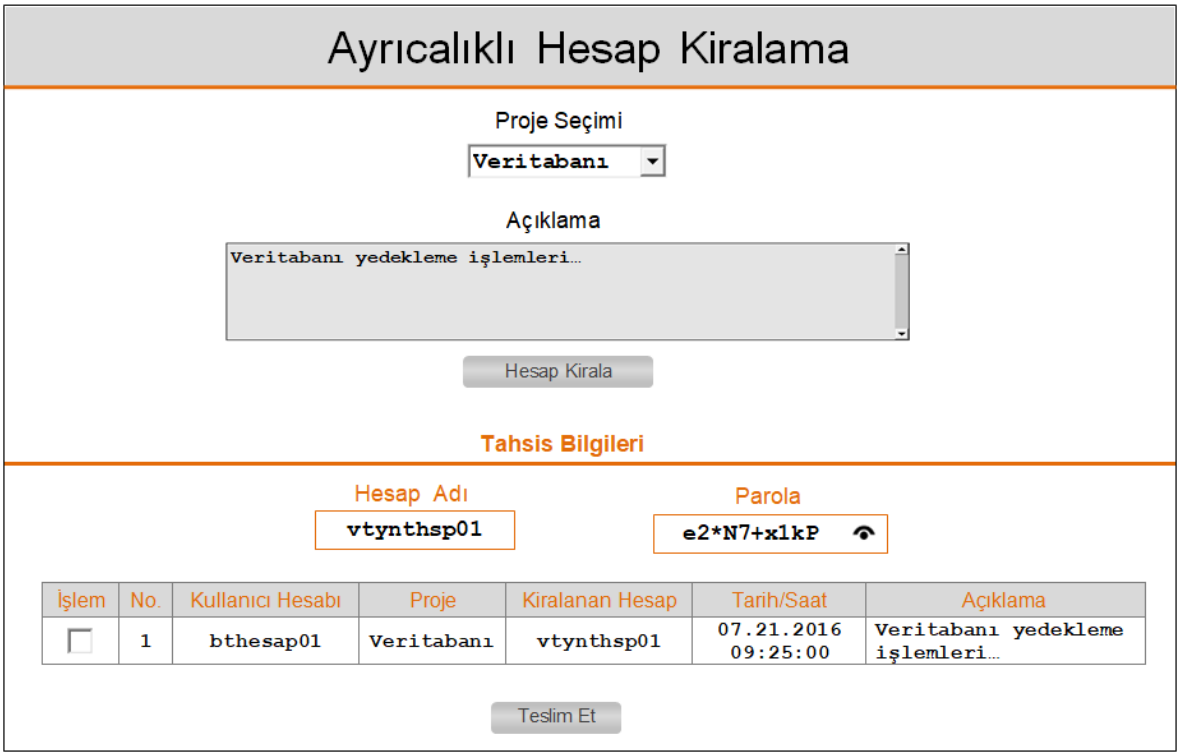
5.1.3. Tahsis havuzundan ayrıcalıklı hesap kiralama

BT personeli, tahsis havuzuna dâhil edilmesinin ardından sorumlu olduğu proje için ayrıcalıklı hesap kiralayabilecektir. *Dizin hizmeti ayrıcalıklı hesap erişim kontrol modülü* uygulama arayüzünde BT personeli oturum açmak için dizin hizmetindeki kendi hesabını kullanmaktadır. Oturum açma bilgileri, dizin hizmeti üzerinden doğrulanmaktadır. Ayrıcalıklı hesabı kiralamak için *ayrıcalıklı hesap kiralama* arayüzünden sırasıyla proje seçimi yapılır, açıklama bölümüne hesap kiralama gerekçesi girilir ve kiralanan hesap bilgisi görmek için *hesap kirala* düğmesine basılarak işlem tamamlanmaktadır.

Hesap kiralama işleminin tamamlanmasının ardından Şekil 5.7'de sunulduğu şekilde BT personelinin hesap adı, kiralanan hesabın adı, yetkili olduğu proje, kiralama başlangıç tarihi ve açıklama ara yüzde gösterilmektedir. Bu bilgilerin aynısı veri tabanında, tahsis havuzundan ayrıcalıklı hesap kiralanma işlemleri için oluşturulmuş olan tabloya yazılır.

Dizin hizmeti ayrıcalıklı hesap erişim kontrol modülü, daha önce oluşturulmuş olan ayrıcalıklı kiralık hesaplardan hangisinin tahsis edileceğini veri tabanındaki bu tabloya bakarak tespit etmektedir. Tablodaki kiralama başlangıç tarihi sütununu kontrol eder, eğer bu sütun doluysa bir sonraki ayrıcalıklı kiralık hesabı tahsis eder. Tüm ayrıcalıklı kiralık hesaplar kullanılıyorsa, hesap tahsis işlemini gerçekleştiremeyeceği bilgisini ara yüz

ekranında gösterir. Bu bilgilendirme mesajının yanı sıra hesapları kimlerin kiraladığı bilgisi ara yüz üzerindeki tahsis bilgileri bölümünde görüntülenmektedir.



Şekil 5.7. Tahsis havuzundan ayrıcalıklı hesap kiralama arayüzü ekran görüntüsü

BT personeli, kiraladığı ayrıcalıklı hesabı, arayüzdeki *teslim et* düğmesine basarak iade eder. İade işlemi gerçekleştiğinde veri tabanındaki tahsis havuzu ayrıcalıklı hesap kiralama tablosundaki söz konusu satırda BT personelinin hesap adı, kiralanan hesabın adı, yetkili olduğu proje, kiralama başlangıç tarihi ve açıklama sütunları içeriği silinir. Bir sonraki kiralama işlemine kadar bu sütunlar boş kalacaktır. Bir sonraki kiralama işlemi esnasında kiralama başlangıç tarihi boş olan ilk hesap tahsis edilmektedir.

5.1.4. Kiralık hesaplar için üretilen parolanın özellikleri ve yenilenmesi

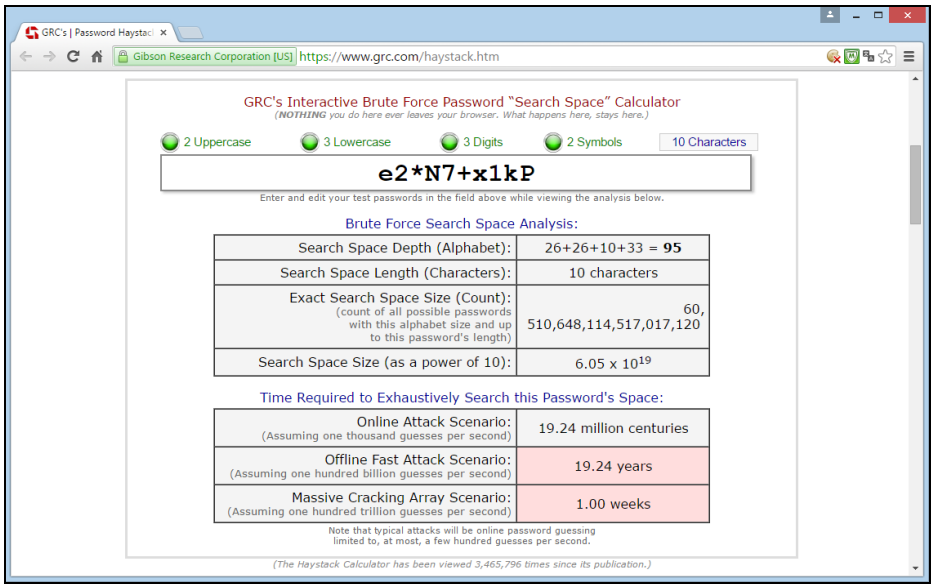
BT personeli, tahsis havuzundan kiralama işlemini tamamladığında, ara yüz ekranında kendisine tahsis edilen ayrıcalıklı hesabı ve buna ait parolayı görmektedir. Üretilen tüm parolalar, 10 karakterden oluşur ve rakam, BÜYÜK/küçük harf ve özel karakterler içermektedir. Tahsis edilen hesaba ait parolalar oluşturulurken uygulamanın derlendiği yazılım diline ait bir parola üretme kod parçası kullanılmaktadır (Örnek Şekil 5.8).

```
static string CreateRandomPassword(int passwordLength)
{
   string allowedChars =
    "abcdefghijkmnopqrstuvwxyzABCDEFGHJKLMNOPQRSTUVWXYZ0123456789.?@!#%+-*%";
   char[] chars = new char[passwordLength];
   Random rd = new Random();
   for (int i = 0; i < passwordLength; i++)
   {
        chars[i] = allowedChars[rd.Next(0,allowedChars.Length)];
   }
   return new string(chars);
}
static void TestRandomPassword()
{
   Console.WriteLine("Testing for generation of random passwords");
   for (int i = 0; i < 6; i++)
   {
   Console.WriteLine("Password {0}={1}",i,CreateRandomPassword(10));
   Thread.Sleep(2000);
   }
   Console.ReadLine();
}
```

Şekil 5.8. Rastgele parola üretmek için kullanılabilecek örnek C# kod parçacığı [123]

Üretilen parola, okunduğunda anlam ifade etmeyen, 10 karakterden oluşan ve parola karmaşıklık ilkesine uygun şekilde üretilmektedir. 10 karakterden oluşan bu parola içerisinde rakamlar, Türkçe karakterler içermeyen BÜYÜK/küçük harfler ve özel karakter bulunmaktadır. Parolayı üreten kod parçacığı parolada istenilen tür ve sayıda karakterin kullanılmasını sağlayacaktır.

Üretilen parolaların sağlamlığını ölçmek amacıyla üretilen örnek bir parola (*örnek parola "e2*N7+x1kP"*) https://www.grc.com/haystack.htm internet sayfasında bulunan uygulama tarafından *Brute Force* saldırılarına karşı test edilmiştir. Alınan test sonuçlarının ekran görüntüsü Şekil 5.9'da, bu sonuçların açıklamaları Çizelge 5.3'te görülmektedir.



Şekil 5.9. Örnek parola için kombinasyon ve saldırı süreleri sonuçları

Örnek parolanın test sonuçları incelendiğinde, saniyede 100 trilyon tahmin yapıldığı varsayılan olağanüstü hızlı bir *Brute Force* saldırı senaryosunda bir haftada çözülebileceği sonucu elde edilmiştir. Bu sonuçlara bakıldığında üretilen parolanın ne kadar kuvvetli olduğu görülmektedir. Ayrıca bu sonuçlara göre üretilen parolaların, ilk bölümlerde bahsedilen parola saldırıları yöntemleri tarafından tahmin edilebilmesi neredeyse imkânsızdır.

Çizelge 5.3. Üretilen örnek parola için kombinasyonlar ve saldırı süreleri

Parola Kombinasyonu	
Arama Uzayı Derinliği	Toplam 95 Karakter (*26 Küçük Harf + 26 Büyük Harf +10 Rakam + 33 Özel Karakter*)
Arama Uzayı Uzunluğu	10 Karakter
Tam Arama Uzayı Boyutu	60.510.648.114.517.017.120 (*Uzunluğu ve kullanılan karakter ile oluşturulabilecek olası parola sayısı*)
Arama Uzayı Boyutu	6,05 X 10^{19} *(10'nun kuvveti olarak)*
Tarama Süresi	
Çevrim İçi Saldırı Senaryosu	19.240.000 Asır (*Saniyede 1.000 tahmin yapıldığı varsayıldığında*)
Çevrim Dışı Hızlı Saldırı Senaryosu	19,24 Yıl (*Saniyede 100 milyar tahmin yapıldığı varsayıldığında*)
Çevrim Dışı Hızlı Saldırı Senaryosu	19,24 Yıl (*Saniyede 100 milyar tahmin yapıldığı varsayıldığında*)
Olağanüstü Hızlı Saldırı Senaryosu	1 Hafta (*Saniyede 100 trilyon tahmin yapıldığı varsayıldığında*)

Parolalar, her ayrıcalıklı hesap kiralama işleminde, hesabın iadesinde, arayüzden çıkış yapıldığında ve zamanlanmış bir görev yardımıyla günün belirli bir saatinde yenilenmektedir. Kiralanan ayrıcalıklı hesabın iadesinin unutulması veya bilerek iade edilmediği durumlar için ise bu hesapların uzun süre kullanımını engellemek maksadıyla uygulama içerisinde zamanlanmış bir görev yardımıyla günün belirli bir saatinde yenilenmektedir. Bu şartlar altında gün içerisinde söz konusu kiralık hesap hiç kullanılmamış olsa bile en az bir kere yenilenmekte ve bu sayede üretilen bu karmaşık parolayı çözmek için saldırganlara en fazla 24 saat süre tanımaktadır. Üretilen parolanın

sağlamlığı ve süre kısıtlaması bulunması, saldırganların parolayı bulmalarını engelleyecektir. Dizin hizmetindeki parola yenileme işlemi, uygulama geliştirilirken kullanılan yazılım dili için hazırlanmış, dizin hizmeti uygulamasına ait bir uygulama programlama arayüzü (*Application Programming Interface-API*) ile gerçekleştirilmektedir.

Kurumsal bir ağın güvenliği için tasarlanan AHEKS *dizin hizmeti ayrıcalıklı hesap erişim kontrol* modülü için, dizin hizmetinde ayrıcalıklı haklara sahip hesap ve bu hesaplara ait parolaların güvenliğini sağlamak birinci önceliğe sahiptir. Bu nedenle üretilen hiçbir parola bir veri tabanına veya başka bir depolama alanında tutulmamakta ve sadece bellekte geçici olarak tutulmaktadır. Bu nedenle uygulama ara yüzünden tarayıcı kapatılarak çıkıldığında, kiraladığımız hesap için parola hala geçerliliğini koruyacaktır. Ancak ara yüz yardımıyla bu parolayı tekrar görmek mümkün olmamaktadır. Uygulama ara yüzüne tekrar giriş yapıldığında tahsis havuzunda söz konusu kiralık ayrıcalıklı hesabın aynı kullanıcıya tahsis edildiği görülmektedir. Ancak ara yüzde parolanın olması gereken alan boş olarak gelecektir. Tekrar parolayı görmek için hesabın iade edilip tekrar alınması gerekmektedir.

5.1.5. Dizin hizmeti ayrıcalıklı hesap erişim kontrol modülü günlük kayıt işlemi

AHEKS Veri tabanında, dizin hizmeti ayrıcalıklı hesap erişim kontrol modülü çalışma döngüsü içerisinde yapılan işlemler için kullanılan tablolara ek olarak günlük kayıtların tutulması amacıyla salt okunur olarak bir tablo bulunmaktadır. Gerçekleştirilen işlemler, öncesinde günlük kayıtların tutulduğu bu tabloya salt okunur olarak yazılmaktadır. Günlük kayıtların tutulduğu tabloda;

- Modüle giriş yapan kullanıcı hesaplarının bilgileri,
- Kiralanan ayrıcalıklı hesap bilgileri,
- Dizin hizmetinde kullanıcı hesapları ile ilişkilendirilen ad ve soyadı bilgileri,
- Üçlü onay mekanizması işlem bilgileri

bulunmaktadır.

Tüm işlemlerin günlük kayıtları, tarih/saat bilgileri, hesap bilgileri gibi önemli bilgilerin tutulduğu bu tabloda hiçbir şekilde kiralanan ayrıcalıklı hesap için üretilen parolaya ait bir bilgi bulunmamaktadır. Geçerliliğini yitirse bile bir parolaya ait bilginin bu tablo üzerinde tutulması güvenli olmayacaktır.

5.2. Yerel Yönetici Hesaplarına Ait Parola Kontrolü

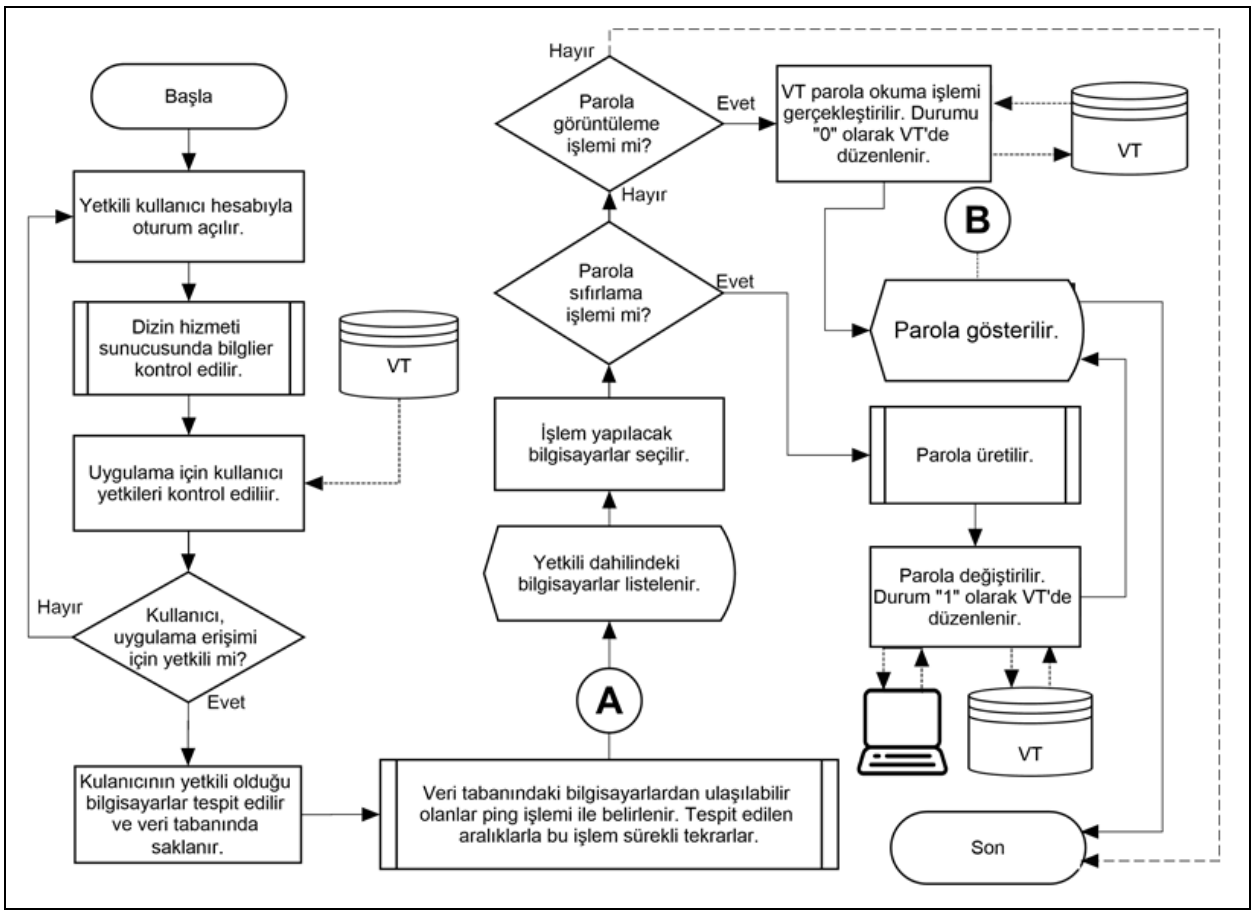
AHEKS de diğer modül "*Yerel Yönetici Hesaplarına Ait Parola Kontrol*" modülüdür. Yerine getirdiği işlev itibariyle çok önemli bir güvenlik zafiyetini ortadan kaldırmaktadır. Bu modül, kuruluş içerisinde dizin yapısına dâhil tüm bilgisayarların yerel yönetici hesaplarına ait parolaların, merkezi ve otomatik olarak yönetilmesini sağlamaktadır. Bu modül sayesinde dizin yapısına dâhil olan tüm bilgisayarların yerel yönetici hesaplarına ait parolalar, her bilgisayar için farklı olarak üretilen bir parola ile değiştirilmektedir. Ayrıca yerel yönetici hesabına zayıf parola verilmesini, uzun süre aynı parolanın kullanılmasını, tüm bilgisayarlarda aynı parolanın kullanılmasını engelleyerek çok önemli bir güvenlik açığını kapatmaktadır.

Dizin yapısına dahil olan tüm bilgisayarların yerel yönetici hesaplarına ait parolaları, dizin hizmeti ayrıcalıklı hesap erişim kontrol modülünde kullanılan metot kullanılarak, okunduğunda anlam ifade etmeyen, 10 karakterden oluşan ve parola karmaşıklık ilkesine uygun şekilde üretilen parola ile değiştirmektedir. 10 karakterden oluşan bu parola içerisinde rakamlar, Türkçe karakterler içermeyen BÜYÜK/küçük harfler ve özel karakter bulunmaktadır. Bu işlem dizin hizmetine eklenen tüm bilgisayarlarda gerçekleştirilebilir.

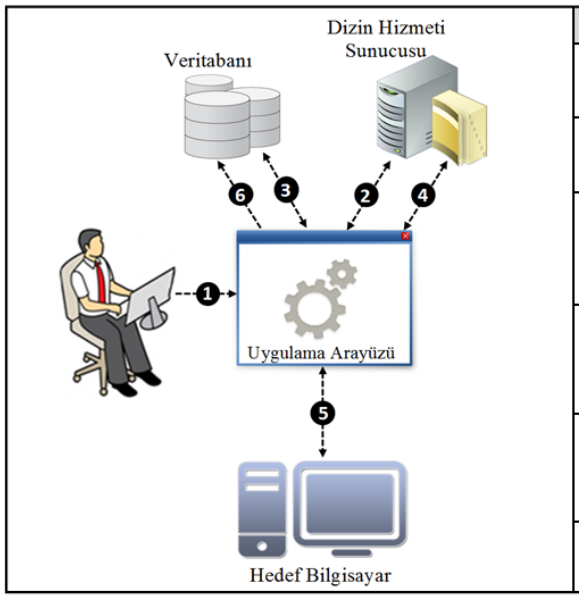
Dizin hizmeti kullanılan bir BT altyapısında, bir bilgisayar bu hizmetten faydalanabilmesi için dizine dâhil edilmiş olmalıdır. Ağa bağlı bir bilgisayar, dizine dâhil edilmezse bu hizmetten faydalanamaz. Bunun nedeni uygulamanın parola değişikliği yapacağı bilgisayarları tanımlamak için dizin hizmetindeki seçkin adlarını kullanmasıdır. Temel olarak dizin yapısı içerisindeki bilgisayarları tespit eder, tespit edilen bilgisayarlar üzerinde dizin hizmeti içerisindeki yetkili kullanıcıya ait yerel yönetici haklarına sahip hesabı kullanarak yerel yönetici hesap parolasını değiştirir. Değiştirilen parola bir veri tabanında şifreli olarak saklanır. Belirlenen periyotlarla veya bu parolaya uygulama ara yüzünden yapılan bir erişim olduğunda parola yeniden değiştirilir ve belirlenen parola şifreli olarak veri tabanına kaydedilir. Bu modülün temel iş akışı Şekil 5.10' da sunulmuştur.

Yerel yönetici hesaplarına ait parola kontrol modülü, BT personelinin kullanımı açısından basit işlem adımlarına sahiptir (Şekil 5.11). Bu modül, yetkili kullanıcı hesaplarının belirlenmesi, dizin hizmeti içerisinde kapsam dâhilindeki bilgisayarların tespiti, parolaların

değiştirilmesi ve gösterilmesi ile tüm işlemlerin kayıt altına alınması amacıyla günlüklerin veri tabanına kaydedilmesi olmak üzere dört temel aşamadan meydana gelmektedir.



Şekil 5.10. Yerel yönetici hesapları parola kontrol modülü temel iş akışı



	İşlem Açıklaması
1	Kullanıcı, uygulama arayüzünden kullanıcı hesabı ve parolası ile oturum açma isteğini gönderir.
2	Dizin hizmeti üzerinde kullanıcının kimlik doğrulama işlemi geçekleştirilir.
3	Kimlik doğrulaması yapılan kullanıcının uygulama arayüzüne oturum açmaya yetkili olup olmadığını kontrol etmek için uygulama tarafından veri tabanında ilgili tablo kontrol edilir.
4	Oturum açan kullanıcının dizin hizmetinde yetkili olduğu havuzda (kuruluş birimi (ou)) bulunan bilgisayarların listesi uygulama arayüzünde listelenir.
5	Bilgisayar listesi içerisinden işlem yapılmak istenen bilgisayar seçilerek var olan parolayı görmek veya değiştirmek için işlem gerçekleştirilir.
6	Yapılan işlemin kayıtları uygulama veri tabanı üzerinde ilgili tabloya kaydedilir.

Şekil 5.11. Yerel yönetici hesapları parola kontrol modülü temel işlem adımları

5.2.1. Yetkili kullanıcı hesaplarının belirlenmesi

Yerel yönetici hesaplarına ait parola kontrol modülü, dizin hizmeti içerisindeki her hesabın kullanımına açık değildir. Sadece yetki verilen kullanıcı personele müsaade edilmektedir. Müsaade edilen kullanıcılar kuruluşun etki alanının yapısına bağlı olarak tek merkezde veya farklı konumlarda yer alabilir. Günümüzde bazı kuruluşlar geniş ve dağıtık yapılara sahiptir. Şubeleri farklı şehirlerde, ülkelerde veya kıtalarda olabilir. Bir kullanıcının uygulama ara yüzünü kullanabilmesi için etki alanı içerisinde bulunması ve dizin hizmeti içerisinde kendisine tanımlanmış bir kullanıcı hesabı bulunması yeterlidir.

BT personelinin, bilgisayarların bakım ve onarım işlemlerini gerçekleştirebilmesi için sorumlu olduğu bilgisayarların bulunduğu dizin hizmetindeki kuruluş biriminde (*organizational unit-OU*) yönetici olarak yetkileri düzenlenmelidir. BT personeli, listelenen bilgisayarlardan sadece yerel yönetici haklarına sahip olduğu kuruluş birimi içerisindeki bilgisayarlar için bu modülü kullanabilmektedir.

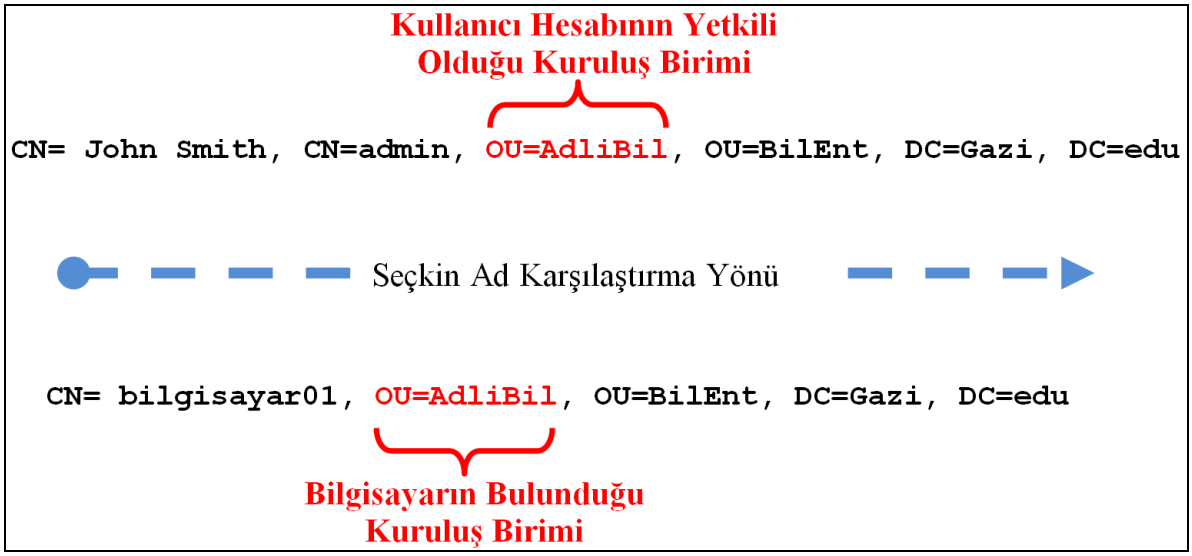
Uygulama, ara yüze oturum açmak isteyen kullanıcının kimlik doğrulama işlemini dizin hizmetinden gerçekleştirmektedir. Uygulama, bir kullanıcının modülü kullanmaya yetkili olup olmadığını kontrol etmek için veri tabanında önceden oluşturulan *yetkili kullanıcı* tablosunu kullanmaktadır. Bu tabloya, AHEKS'in yöneticisi tarafından bilgisayarların bakım, onarım ve idamesinden sorumlu personele ait hesaplar önceden girilmektedir.

5.2.2. Uygulama kapsamındaki bilgisayarların tespiti

BT personelinin, bilgisayarların bakım ve onarım işlemlerini gerçekleştirebilmesi için sorumlu olduğu bilgisayarların bulunduğu dizin hizmetindeki kuruluş biriminde (*Organizational Unit-OU*) yerel yönetici olarak yetkileri düzenlenmelidir. BT personeli, listelenen bilgisayarlardan sadece yerel yönetici haklarına sahip olduğu kuruluş birimi içerisindeki bilgisayarlar için bu modülü kullanabilir. *Yerel yönetici hesaplarına ait parola kontrol* modülü, kuruluş birimleri içerisindeki bilgisayarları çekerek listeler. BT personeline ait hesabın yetkili olduğu bilgisayarların tespit edilmesi aşamasında bu modül, kullanıcı hesabının yetkili olduğu kuruluş birimini tespit etmek için seçkin adları kullanmaktadır.

Kuruluşların tek merkezde bulunmaları durumunda uygulama kapsamına girecek bilgisayarlar genellikle dizin hizmeti içerisinde tek bir kuruluş birimi içerisinde yer alır. Bu durumda uygulama, bu havuz içerisinden tüm bilgisayarları çekerek listelemektedir. Dizin hizmetinde bilgisayarlar, konumu gereği veya farklı departmanların ayrılması düşüncesiyle farklı kuruluş birimleri içerisinde yer alabilir. Bu durumda yetkili kullanıcı uygulama ara yüzüne oturum açtığı zaman listelenecek bilgisayarların seçimi, kullanıcı hesabının yönetici haklarına sahip olduğu kuruluş birimi vasıtasıyla gerçekleştirilmektedir.

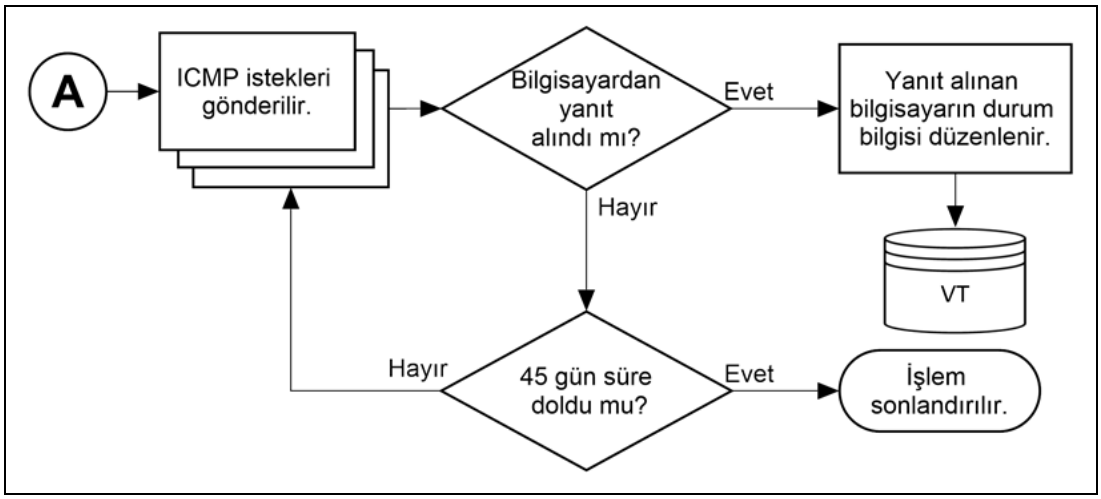
Tüm bilgisayarların seçkin adlarının listelenmesinin ardından ilgili kullanıcı hesabına ait seçkin adla karşılaştırılarak kuruluş birimi eşleşen bilgisayarlar veri tabanında bir tabloda tutulur ve uygulama arayüzünde gösterilir. Karşılaştırma, aşağıdan yukarı doğru, yani ortak addan (*Common Name-CN*) başlayarak etki alanı bileşenine (*Domain Componenet-DC*) doğru yapılmaktadır (Şekil 5.12). Karşılaştırma işleminin aşağıdan yukarı doğru yapılmasının amacı, kullanıcı hesabının dâhil olduğu ancak kullanıcının tamamında yetkili olmadığı kapsayıcı durumdaki kuruluş birimi (*Bkz. Şekil 5.12'deki örnekte ou=BilEnt kapsayıcıdır*) içerisindeki bilgisayarların arayüzde gösterilmesini engellemektir.



Şekil 5.12. Seçkin ad karşılaştırma süreci

Uygulama arayüzünde gösterilen bilgisayar listesi, BT personelinin yerel yönetici haklarına sahip olduğu kuruluş biriminde yer alan bilgisayar seçkin adlarının listesidir. Uygulama arayüzünde listelenen bilgisayarların karşılığında fiziksel olarak bir bilgisayar olmayabilir veya listeleme esnasında bilgisayar/lar kapalı olabilir. Bu nedenle uygulama, karşılaştırma işlemi sonucunda elde edilen seçkin adlardan tespit edilen bilgisayarlara 45

gün süreyle ICMP paketi (*ping)* gönderir. ICMP paketlerinin (*ping)* yanıtları, veri tabanında *bilgisayar listesi* tablosunda ve arayüzde *durumu* sütununda belirtilir (Şekil 5.13). Veri tabanında yer alan bilgisayar listesi ve durum bilgisinin güncel hali bellekte tutulmaktadır.

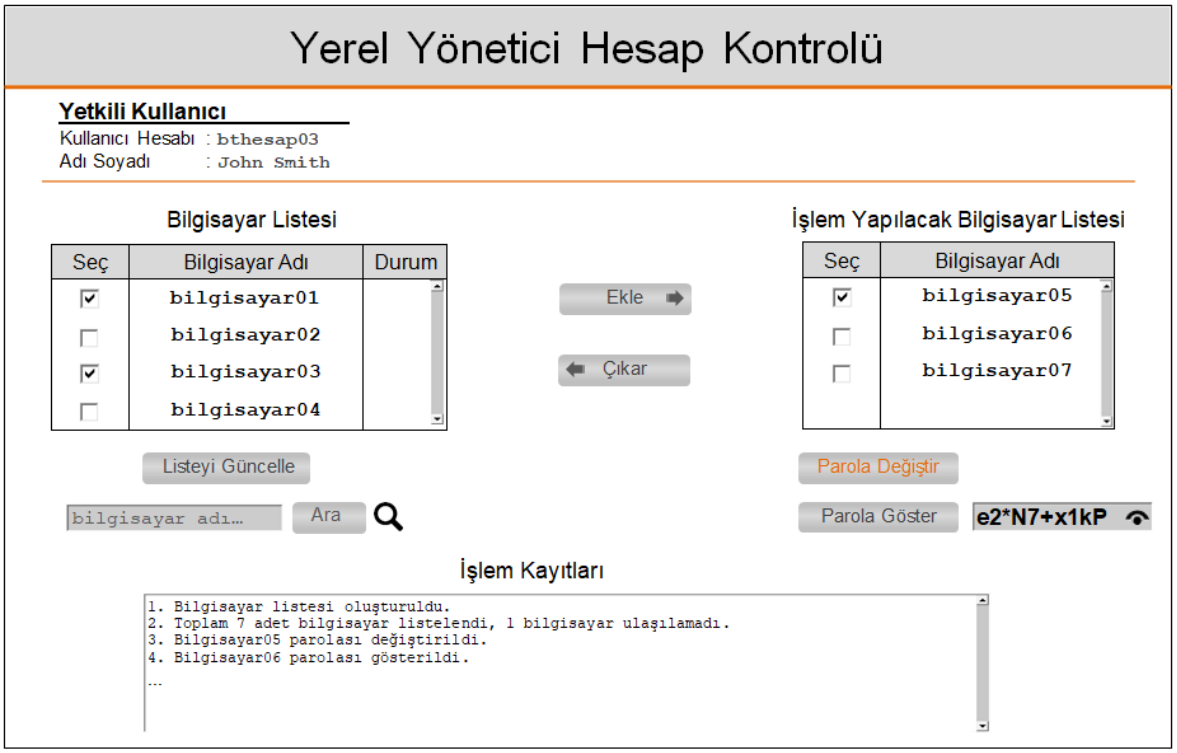


Şekil 5.13. Uygulama kapsamındaki bilgisayarların tespiti alt iş akışı

5.2.3. Yerel yönetici hesap parolalarının değiştirilmesi, gösterilmesi ve saklanması

Yerel yönetici hesapları parola kontrol modülü ara yüzünde listelenen bilgisayarlardan işlem yapılacak olan bilgisayar/bilgisayarlar seçilerek işlem yapılacak bilgisayar listesine aktarılır (Şekil 5.14). Yerel yönetici hesap parolası değiştirilmesi istenilen bilgisayar/bilgisayarlar seçilir ve parola değiştir düğmesi kullanılarak işlem gerçekleştirilir. Yapılan bu işlemler, AHEKS veri tabanı üzerinde bu modül tarafından gerçekleştirilen işlemlerin kaydedilmesi için oluşturulan *işlem* tablosuna işlenmektedir.

Parolanın değiştirilmesi ve değiştirilen parolanın sorunsuz şekilde işlem tablosuna kayıt edilmesinin ardından işlem başarılı olarak *işlem* tablosuna işlenir. Her başarılı parola değişikliğinin ardından veri tabanı işlem tablosu üzerindeki son parola bilgisi yenilenir. Uygulama tarafından değiştirilen parolalar işlem tablosunda Rijndael şifreleme algoritması [124] kullanılarak depolanmaktadır (*uygulamanın geliştirilme aşamasında, yazılımcının seçimine bağlı olarak farklı algoritmalarda kullanılabilir*).

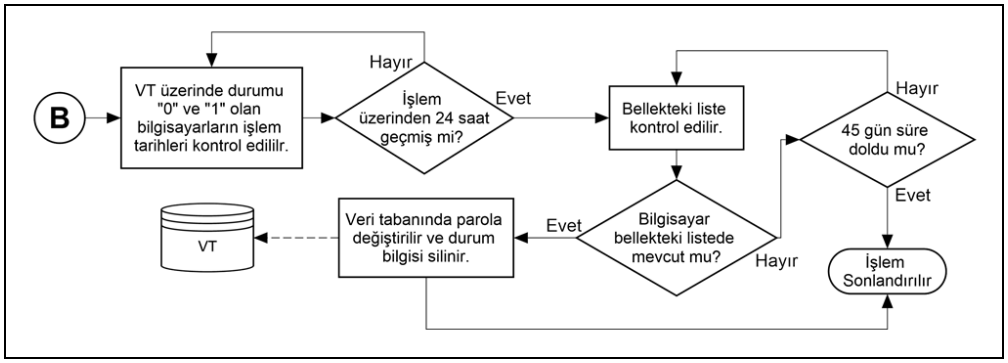


Şekil 5.14. Yerel yönetici hesapları parola kontrol modülü ara yüzü ekran görüntüsü

Uygulama arayüzünde bir bilgisayarın yerel yönetici hesap parolasını görebilmek için parolanın uygulama tarafından daha önce değiştirilmiş olması gerekmektedir. Bunun nedeni, uygulama arayüzünde *parola göster* düğmesi kullanılarak gösterilen parola, hedef bilgisayardan değil uygulama veri tabanı içerisindeki *işlem* tablosundan getirilmesidir.

İşlem tablosunda ayrıca işlem yapılan bilgisayarların adı, işlem tarih/saati ve işlem durum bilgisi tutulmaktadır. Uygulama ara yüzünde listelenen bilgisayarlardan *işlem yapılacak bilgisayar listesine* aktarılanlar veya parolası gösterilen bilgisayarların durum bilgisi için "0" değeri, parolası değiştirilen için durum bilgisinde "1" değeri kullanılmaktadır.

Durum bilgisi "0" ve "1" olarak ifade edilen bilgisayarların parolaları işlem tablosunda belirtilen işlem zamanından 24 saat sonra uygulama tarafından otomatik olarak değiştirilir ve işlem tablosundaki durum bilgisi temizlenir (Şekil 5.15). Tüm bilgisayarların yerel yönetici hesaplarına ait parolaların değiştirilmesi bilgisayar sayısına bağlı olarak fazla zaman ve kaynak tüketebilir. Bu nedenle uygulamanın geliştirilmesi aşamasında toplu parola değiştirme işlemi için iş parçacıkları (*Thread*) oluşturulur ve bilgisayarlar bu iş parçacılarına paylaştırılarak süreç hızlandırılır.



Şekil 5.15. Uygulama kapsamındaki bilgisayarların otomatik parola değiştirme alt iş akışı

Bilgisayar listesi tablosunda yer alan ancak işlemleri başarıyla tamamlanamadığı için işlem tablosunda bulunmayan bilgisayarların parolalarını değiştirmek amacıyla uygulama, 45 gün (*isteğe bağlı*) süre ile söz konusu bilgisayarlara erişmeyi dener. Uygulama tarafından 45 gün süreyle iletişim kurulamayan bilgisayarlara erişim denemeleri sonlandırılır.

Hedef bilgisayar/bilgisayarların yerel yönetici hesapları için uygulama tarafından üretilen parola, Windows sistemlerde Windows Yönetim Aracı (*Windows Management Instrumentation-WMI*) kullanılarak, Linux sistemlerde Web Tabanlı Kurumsal Yönetim (*Web Based Enterprise Management-WBEM*) vb. araçlar kullanılarak değiştirilmektedir.

Uygulama veri tabanı içerisinde, *işlem* tablosuna kayıt edilen bu işlemlerin tabloya başarılı bir işlem olarak kayıt edilebilmesi için parolanın şifreli halinin başarılı şekilde tabloya girilmesi gerekmektedir. Parolanın değiştirilmesi ve değiştirilen parolanın sorunsuz şekilde işlem tablosuna kayıt edilmesinin ardından işlem başarılı olarak tamamlanmış olacaktır. Her başarılı parola değişikliğinin ardından veri tabanı işlem tablosu üzerinde eski parola bilgisi silinmektedir ve yerini yeni parola bilgisi almaktadır.

5.2.4. Yerel yönetici hesapları parola kontrol modülü günlük kayıt işlemi

Yerel yönetici hesapları parola kontrol modülü tarafından gerçekleştirilen işlemlerin günlük kayıtları uygulama veri tabanı içerisinde yer alan *yerel yönetici hesapları parola kontrol modülü günlük kayıt* tablosunda tutulmaktadır. Günlük kayıtların tutulduğu tabloya, uygulama tarafından gerçekleştirilen veya sonuçlandırılamayan tüm işlemlerin kayıtları girilmektedir. Söz konusu tablo içerisinde uygulama tarafından otomatik olarak gerçekleştirilen işlemlerin yanı sıra uygulama arayüzünü kullanmaya yetkili personel tarafından gerçekleştirilen işlemlerin günlük kayıtları da yer almaktadır.

Uygulama veri tabanı içerisinde yer alan günlük kayıt tablosu; girdilerin silinme, ekleme ve değiştirilmesini engellemek amacıyla salt okunur olarak oluşturulmuştur. Günlük kayıtların tutulduğu tablo içerisinde uygulama tarafından üretilen parolalar tutulmamaktadır. Günlük kayıtların tutulduğu tabloda;

- İşlem yapan personele ait kullanıcı hesap bilgisi,
- İşlem yapan personelin dizin ağaç yapısı içerisindeki adı ve soyadı bilgisi,
- Üzerinde işlem yapılan bilgisayar adı,
- İşlem durum bilgisi (0-1),
- Başarısız işlemlerin bilgisi,
- Gerçekleştirilen işlemin açıklaması,
- Gerçekleştirilen işlemlerin tarih/saat bilgisi

yer almaktadır.

5.3. Pilot Kullanım Sonuçları

AHEKS yapısı gereği BT personeline hitap etmektedir. Söz konusu sistem, BT altyapısı içerisinde bazı güvenlik sorunlarının en aza indirilmesini amaçlamaktadır. BT güvenliği konusunda bilinçli BT personeli tarafından bir eksikliği giderdiği düşünülerek AHEKS'in hayata geçirilmesi teşvik edilmiştir. Ayrıca uygulama modelinin teoriden uygulamaya geçtiği ilk dönemlerde yaşanabilecek genel sıkıntılar giderilerek sürecin aksamadan ilerlemesi amacıyla gerekli tedbirler alınmıştır. AHEKS'in BT altyapısına entegre edilme süreci içerisinde aşağıda sıralanmış problemlerle karşılaşılmıştır.

BT personelinin sürece dâhil edilmesi aşamasında ortaya çıkan problemler;

- Daha önce ayrıcalıklı hesaplara sahip BT altyapısından sorumlu personel tarafından, kullanıcı hesaplarına ait yetkilerin düşürülmesi, kendilerine güvenilmediği hissine ve bunun sonucu olarak aidiyet duygusunun azalmasına neden olmuştur,
- BT personeli tarafından daha önce sahip oldukları ayrıcalıklı kullanıcı hesapları sayesinde sorumluluk alanları dışında bulunan sistemlerde gerçekleştirdikleri işlemlerin engellenmesi, söz konusu personel tarafından aksamalara neden olacağı düşüncesine neden olmuştur,

- BT personeli tarafından, yerel yönetici hesaplarının varsayılan adının (*administrator*) değiştirilerek, AHEKS tarafından parolanın değiştirilmesini engellemek, bilgisayarların yerel yönetici grubuna yeni kullanıcı eklenmesi ve dizin hizmeti kullanıcı hesaplarını hizmet veren sunucuların yerel yönetici grubuna ekleyerek uygulamayı devre dışı bırakmak amacıyla bazı işlemler gerçekleştirilmiştir.

Uygulama modelinin teoriden uygulamaya geçtiği ilk dönemlerde yaşanan teknik problemler;

- İlk etap da yerel yönetici hesapları parola kontrol modülü tarafından değiştirilen parolalar veri tabanı üzerinde tutulmamıştır. Ancak parolası değiştirilen ve sonrasında herhangi bir sebeple ağ ile bağlantısı kesilen bilgisayara yerel yönetici hesabı ile girmek istendiğinde en son değiştirilen parola bilgisinin kaydedilmemesi ve bilgisayarın ağa bağlı olmaması nedeniyle parolanın yeniden değiştirilememesi söz konusu bilgisayara oturum açılamamasına sebep olmuştur,
- Yerel yönetici hesapları parola kontrol modülü uygulama ara yüzünün ilk tasarımında "parola değiştir" ve "parola göster" düğmeleri birbirine çok yakın olarak kullanılmıştır. Ara yüz tasarımındaki bu hata, herhangi bir sebeple ağa bağlantısı kesilen bilgisayarın/bilgisayarların parolasını görmek isteyen kullanıcının zaman zaman "parola göster" düğmesi yerine yanlışlıkla "parola değiştir" düğmesini kullandığı gözlemlenmiştir. Bunun sonucu olarak, uygulama veri tabanı işlem tablosu üzerindeki eski parola bilgisinin silinmesine, uygulamanın söz konusu bilgisayara/bilgisayarlara erişimi olmamasından dolayı da yeni bir parola verilememesine neden olmuştur,
- Dizin hizmeti ayrıcalıklı hesap erişim kontrol modülü tarafından üretilen parolaların bellekte saklanması nedeniyle kullanıcının uygulama ara yüzünden oturum kapatmadan çıkması durumunda, söz konusu ayrıcalıklı kullanıcı hesabı için üretilen parola geçerliliğini korumaktadır. Ancak bu işleyiş, kullanıcı tarafından ara yüze tekrar giriş yapılsa dahi görülememesi nedeniyle iş akış sürecinin uzamasına neden olmuştur.

AHEKS'in kullanıldığı kuruluş içerisinde BT güvenliğine katacağı faydalar çalışma boyunca tartışılmıştır. AHEKS'in kullanımına başlanan kuruluş tarafından uygulamanın sağladığı faydaların sonuçları hemen alınabilmektedir. AHEKS'in hayata geçirildiği kuruluş içerisinde sağladığı faydalar aşağıda sıralanmıştır.

- BT personelinin sorumluluğu dışında kalan ve yetkisinin olmadığı kaynaklara erişimi kesilmiştir,
- Saldırganlar tarafından BT altyapısına gerçekleştirilecek parola saldırılarına karşın kuruluşun direnci artmıştır,
- BT personelinin BT güvenliği konusunda farkındalığı artmıştır,
- Kuruluş içerisindeki kötü niyetli kişilerin yetkisi olamayan kaynaklara erişimi büyük ölçüde engellemiştir,
- BT personeli tarafından gerçekleştirilen keyfi işlemler önlemiştir,
- AHEKS tarafından tutulan günlük kayıtlar sayesinde BT personeli tarafından gerçekleştirilen işlemlerin takibi kolaylaşmıştır,
- Kuruluşun BT güvenliği maliyetlerini düşürmüştür,
- BT personelinin sorumluluklarının sınırları net olarak çizilmiştir,
- Kuruluş yöneticilerinin bizzat BT güvenlik sürecine dâhil edilmesi sağlanmıştır.

6. SONUÇ VE ÖNERİLER

Çalışmada sunulan AHEKS uygulama modeli BT altyapısı güvenliğini arttırmayı amaçlamaktadır. Ancak tüm BT güvenlik sorunlarını çözmesi beklenmemelidir. AHEKS, geleneksel BT güvenlik tedbirleri kapsamındaki parola güvenliği sorunlarını en düşük maliyetle çözümleyerek kuruluşlara ve BT personeline yardımcı olmaktadır.

Geleneksel BT güvenliği kapsamında çalışma konusu uygulama modeli, dizin hizmeti kullanılan kuruluşlar için birçok haklara, izinlere ve imtiyazlara sahip ayrıcalıklı kullanıcı hesaplarının kontrol altına alınmasını sağlamıştır. Ayrıcalıklı kullanıcı hesaplarına ait parolaların temel BT güvenlik ilkeleri doğrultusunda belirlenmesi ve parola saldırılarına karşın daha güçlü parolalar oluşturulmasını sağlamıştır.

AHEKS, kuruluş içerisindeki BT personelinin görev ve sorumluluklarına ait sınırları net çizgilerle belirlemiştir. Görev ve sorumlulukların sınırlarının belirlenmesi, BT personelinin iş yükünün eşit dağılmasını ve BT altyapısı içindeki rollerinin belirgin olarak ortaya çıkmasını sağlamıştır. BT personeli için görev dağılımının yapılması sonucunda BT altyapısı içerisinde yer alan verilere, kaynaklara ve hizmetlere ait sorumlulukların tekrar düzenlenerek kuruluş içerisinde olası yetki karmaşası problemleri engellenmiştir.

BT güvenliği kapsamında gizlilik ve bütünlük bileşenlerinin korunması adına kuruluşlara artı değerler katmıştır. Bilgi güvenliği yönetim sistemi (BGYS) yaklaşımını kuruluş içerisinde hayata geçirilmesi adına destek sağlamıştır.

AHEKS'in iş akışına kuruluş yöneticilerinin dâhil edilmesi sayesinde, kuruluş yöneticileri BT güvenlik sürecinin bir parçası haline gelmiştir. Ayrıca BT güvenliği konusunda yeterli bilgiye sahip olmayan BT personeli ve kuruluş yöneticilerinin konunun önemini anlamlarını sağlamış ve konu ile ilgili farkındalığı arttırmıştır.

AHEKS'in iş akış sürecini uzattığı iddia edilebilir ancak BT güvenliği açısından kabul edilebilir bir durumdur. Eski alışkanlıklarından vazgeçmekte zorlanabilecekleri değerlendirildiğinden BT personeline ve kuruluş yöneticilerine AHEKS hakkında mutlaka bilgilendirme yapılmalıdır. Bilgilendirme içeriği, BT personeli ve kuruluş yöneticileri için ayrı olarak düzenlenmelidir. BT personeli için yapılacak bilgilendirme daha ayrıntılı ve aydınlatıcı olmalı, kuruluş yöneticileri için yapılacak bilgilendirme ise gereksiz

ayrıntılardan arındırılmış ve AHEKS'in kuruluşa sağladığı faydalar üzerine yoğunlaşan bir içeriğe sahip olmasına dikkat edilmelidir.

AHEKS'i kendi kuruluşlarına entegre etmeyi planyan BT personeli, içeriği mutlaka değerlendirmeli ve kuruluşunun yapısına uygun hale getirecek tedbirleri alarak, sistemin işlerliğini artırmalıdır. AHEKS için uygulama ara yüzüne oturum açma aşamasında resimli doğrulama (*captcha*), uygulama ara yüzüne erişim için IP kontrolü gibi güvenlik önlemleri alınması önerilmektedir.

Ayrıca Bölüm 6'da bahsedildiği üzere *yerel yönetici hesapları parola kontrol* modülü ara yüzü tasarımında *parola değiştir* ve *parola göster* düğmelerinin yakın olmaları nedeniyle karşılaşılabilecek sorunları önlemek maksadıyla ara yüz tasarımına dikkat edilmelidir.

BT altyapısı içerisinde AHEKS uygulamasını ve uygulamaya ait veri tabanını barındıran sunucular mutlaka bir güvenlik duvarının arkasına konuşlandırılmalıdır. Kuruluşun yerel ağından fiziksel ve mantıksal olarak farklı bir ağın üyesi olması sağlanmalıdır. Fiziksel ve mantıksal olarak ayrılan bu tür ağ alanlarına "*yarı güvenli ağ*" (*Demilitarized Zone -DMZ*) adı verilmektedir. Sunucuların farklı bir DMZ'te konuşlandırılması sayesinde uygulama sunucularına erişim güvenlik duvarı tarafından yönetilecek ve erişimler kontrol altına alınması sağlanacaktır. Bu yapılandırma, AHEKS'i hedef alan saldırıları önleneceğinden dolayı öncelikli olarak önerilmektedir.

Bölüm 6 içerisinde aktarılan hususular mutlaka değerlendirilmelidir. Bölüm 6 içerisinde aktarılan hususlardan iş akışını aksatacağı veya uzatacağı değerlendirilen maddelere yeni çözümler üretilmelidir. AHEKS kuruluş içerisinde tam anlamıyla uygulanmaya başlamadan önce belirli bir süre ile deneme sürecine tabi tutulmalıdır. Deneme süreci sonucunda yapılacak anket ve değerlendirmeler hassasiyetle incelenerek sorunların çözümlenmesinin ardından AHEKS'in tam anlamıyla kullanımına başlanması önerilmektedir.

İleriki dönemde, kiralanan ayrıcalıklı hesaplar vasıtasıyla yapılan işlemlere ait sunucular üzerindeki günlük kayıtların bir kopyasının uygulama veri tabanında bulunan günlük kayıt tablosunda tutulması sağlanabilir. Bu sayede, ayrıcalıklı hesapların denetlene bilirliği arttırılmış olacak ve ayrıcalıklı hesapların maksadı dışında kullanımı daha kolay tespit edilebilecektir.

Gelecekteki çalışmalarda, uygulama sayesinde kontrol edilen hesapların kapsamı, ağ güvenlik sistemleri, aktif ağ cihazları ve farklı amaçlarla bilişim altyapısının merkezi yönetiminde kullanılan uygulamaların yönetici hesaplarını kapsayacak şekilde yapılandırılabilir. Bu sayede siber saldırganlar tarafından ele geçirildiği takdirde tehlike oluşturabilecek tüm hesapların güvenliğini arttıracak ve yönetilmesini sağlayacaktır.

KAYNAKLAR

1. Fitzgerald, S., Foster, I., Kesselman, C., Von Laszewski, G., Smith, W., and Tuecke, S. (1997), August). *A directory service for configuring high-performance distributed computations*. Paper presented at the Sixth IEEE International Symposium, High Performance Distributed Computing, Portland, OR,365-375.
2. Sheresh, B., and Sheresh, D. (2002). *Understanding Directory Services*. Indiana: Sams Publishing, 3-39.
3. Kanalakis, J. (2003). *Developing. NET Enterprise Application.*Using Networking Directory Services. New York, NY:Apress, 71-72.
4. İnternet: Active Directory Service Interfaces. *Microsoft. URL:* http://www.webcitation.org/query?url=https%3A%2F%2Fmsdn.microsoft.com%2Fen-us%2Flibrary%2Faa772170%28v%3Dvs.85%29.aspx&date=2017-05-20, Son Erişim Tarihi: 20.05.2017.
5. İnternet: 389 Directory Server Documentation. *Fedora Project.* URL: http://www.webcitation.org/query?url=http%3A%2F%2Fdirectory.fedoraproject.org%2Fdocs%2F389ds%2Fdocumentation.html&date=2017-05-20, Son Erişim Tarihi: 20.05.2017.
6. İnternet: Novell eDirectory 8.7.3 Installation Guide. *Novell*. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.novell.com%2Fdocumentation%2Fedir873%2Fpdfdoc%2Fqsedir873%2Fqsedir873.pdf&date=2017-05-20, Son Erişim Tarihi: 20.05.2017.
7. İnternet: Oracle Directory Server Enterprise Edition Release Notes 11g Release 1. *Oracle*. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fdocs.oracle.com%2Fcd%2FE20295_01%2Fhtml%2F821-1216%2Fhardware.html&date=2017-05-20, Son Erişim Tarihi: 20.05.2017.
8. İnternet: OpenLDAP 2.4.44 Release Announcement. *OpenLDAP. URL:* http://www.webcitation.org/query?url=http%3A%2F%2Fwww.openldap.org%2Fsoftware%2Frelease%2Fannounce.html&date=2017-05-20, Son Erişim Tarihi: 20.05.2017.
9. İnternet: Apache Directory Studio. *Apache Software*. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fdirectory.apache.org%2Fstudio%2F&date=2017-05-20, Son Erişim Tarihi: 20.05.2017.
10. İnternet: Tivoli Directory Server 6.3 Software Requirements. *IBM.* URL*:* http://www.webcitation.org/query?url=http%3A%2F%2Fwww-01.ibm.com%2Fsupport%2Fdocview.wss%3Fuid%3Dswg27021796&date=2017-05-20, Son Erişim Tarihi: 20.05.2017.
11. Douceur, J. R., Adya, A., Benaloh, J., Bolosky, W. J., and Yuval, G. (2002, December). *A Secure Directory Service based on Exclusive Encryption*. Paper presented at 18th Annual Computer Security Applications Conference, Las Vegas, NV, 172-182.
12. Jøsang, A., Zomai, M. A., and Suriadi, S. (2007, January). *Usability and privacy in identity management architectures.* Australian Computer Society, Paper presented at the fifth Australasian symposium on ACSW frontiers-Volume 68, Ballarat, VIC, 143-152.
13. Bertino, E., Paci, F., Ferrini, R., and Shang, N. (2009). Privacy-preserving digital identity management for cloud computing. *the IEEE Computer Society Technical Committee on Data Engineering Bulletin*, *32*(1), 21-27.
14. El Maliki, T., and Seigneur, J. M. (2007, October). *A survey of user-centric identity management technologies*. Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007. Paper presented at the International Conference,Valencia, 12-17.
15. İnternet: Huey, P., Oracle Database Security Guide 11g Release 2 (11.2).*Oracle*.URL: http://www.webcitation.org/query?url=https%3A%2F%2Fdocs.oracle.com%2Fcd%2FE11882_01%2Fnetwork.112%2Fe36292.pdf&date=2017-03-11, Son Erişim Tarihi: 11.03.2017.

16. De Capitani di Vimercati, S., Paraboschi, S., and Samarati, P. (2003). Access control: principles and solutions. *Software: Practice and Experience*, *33*(5), 397-421.
17. İnternet: Mathers, B., Privileged Accounts and Groups in Active Directory. *Microsoft*. URL: http://www.webcitation.org/query?url=https%3A%2F%2Ftechnet.microsoft.com%2Fwindows-server-docs%2Fidentity%2Fad-ds%2Fplan%2Fsecurity-best-practices%2Fappendix-b--privileged-accounts-and-groups-in-active-directory&date=2017-03-11, Son Erişim Tarihi: 11.03.2017.
18. İnternet: Butler, J. M., Privileged Password Sharing: "root" of All Evil. *SANS Institute*. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.sans.org%2Freading-room%2Fwhitepapers%2Fanalyst%2Fprivileged-password-sharing-root-evil-35195&date=2017-03-11, Son Erişim Tarihi: 11.03.2017.
19. Tep, K. S., Martini, B., Hunt, R., and Choo, K. K. R. (2015, August). *A taxonomy of cloud attack consequences and mitigation strategies: The Role of Access Control and Privileged Access Management*. Paper presented at the 13th IEEE International Symposium on Parallel and Distributed Processing with Applications, Helsinki, 1073-1080.
20. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. (1996). Role-based access control models. *Computer*, *29*(2), 38-47.
21. Buszta, K. (2007), Security management. In Tipton, H. F. and Krause, M. (Eds.), *Information Security Management Handbook* (6th ed.). Auerbach Publications, Boca Raton, FL, 155-164.
22. Sladic, G., Milosavljevic, B., and Konjovic, Z. (2013). Context-sensitive access control model for business processes. *Computer Science and Information Systems*, 10(3), 939-972
23. Eminağaoğlu, M. ve Gökşen, Y. (2009). Bilgi güvenliği nedir, ne değildir, Türkiye'de bilgi güvenliği sorunları ve çözüm önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 11(4), 1-15.
24. Vroom, C. and Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, 23(3), 191-198.
25. Wahl, M., Howes, T., and Kille, S. (1997, December). Lightweight Directory Access Protocol (v3), RFC 2251. *Internet Engineering Task Force.*
26. İnternet: Morgan, S., CyberSecurity Market Report. *Cybersecurity Ventures*. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fcybersecurityventures.com%2Fcybersecurity-market-report%2F&date=2017-03-11, Son Erişim Tarihi: 11.03.2017.
27. Richardson, R. (2008). CSI computer crime and security survey. *Computer Security Institute*, 1, 1-30.
28. Dhillon, G. and Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, 43(7), 125-128.
29. Liao, I. E., Lee, C. C. and Hwang, M. S. (2006). A password authentication scheme over insecure networks. *Journal of Computer and System Sciences*, 72(4), 727-740.
30. Weirich, D. and Sasse, M. A. (2001, September). *Pretty good persuasion: a first step towards effective password security in the real world*. Paper presented at the 2001 workshop on New security paradigms, New York, 137-143.
31. İnternet: Deuby, S., The Keys to the Kingdom: Limiting Active Directory Administrators. *Dell Software.*URL:http://www.webcitation.org/query?url=https%3A%2F%2Fwww.quest.com%2Fdocs%2FKeys_to_the_Kingdom_Limiting_AD_Admins.pdf&date=2017-03-11, Son Erişim Tarihi: 11.03.2017
32. De Clercq, J., and Grillenmeier, G. (2007). 9 - Single Sign-On, In Microsoft Windows Security Fundamentals. *Microsoft Windows Security Fundamentals*. Burlington: Digital Press,533-579

33. İnternet: Fischer International, Privileged Access Management: Take back the keys to the kingdom. *Fischer International*. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.fischerinternational.com%2Fcompetencies%2Fprivileged_account_management.htm&date=2017-03-11, Son Erişim Tarihi: 11.03.2017.
34. Grafton, J. (2013). Avoiding the five pitfalls of privileged accounts. *Network Security*, *2013*(5), 12-14.
35. Stoneburner, G., Goguen, A. Y., and Feringa, A. (2002). SP 800-30. Risk management guide for information technology systems. *Technical Report*. National Institute of Standards & Technology, Gaithersburg, MD, 1-56.
36. Moses, S., Rowe, D. C., and Cunha, S. A. (2015, September). Addressing the Inadequacies of Role Based Access Control (RBAC) Models for Highly Privileged Administrators: Introducing the SNAP Principle for Mitigating Privileged Account Breaches. *International Journal of Intelligent Computing Research*, 6(3), 583-591.
37. Indu, I., and Anand, P. R. (2015, December). *Identity and access management for cloud web services*. Paper presented at 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS), Trivandrum, Kerala, India 406-410.
38. Gaw, S., and Felten, E. W. (2006, July). *Password management strategies for online accounts*. Paper presented at the second symposium on Usable privacy and security, Pittsburgh, PA, 44-55.
39. Slade, R. (2015, November). *Dictionary of Information Security*. Rockland, MA: Syngress Publishing, 43,101.
40. İnternet: Öztürk, G. (2008). BGYS-0005 Bilgi güvenliği politikası oluşturma kılavuzu. *Tübitak UEKAE*.URL:http://www.webcitation.org/query?url=https%3A%2F%2Fwww.bilgiguvenligi.gov.tr%2Fdokuman-yukle%2Fbgys%2Fuekae-bgys-0005-bilgi-guvenligi-politikasi-olusturma-kilavuzu%2Fdownload.html&date=2017-03-11, Son Erişim Tarihi: 11.03.2017
41. İnternet: IsecT, (2013). Information Technology — Security Techniques — Code Of Practice For Information Security Controls (ISO/IEC 27002:2013). *The International Organization for Standardization*. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.iso27001security.com%2Fhtml%2F27002.html&date=2017-05-29 , Son Erişim Tarihi: 29.05.2017.
42. İnternet: Çakır, Z., ISO 27001:2013 ve ISO 27002:2013'te Neler Değişiyor ?. *Tübitak UEKAE*.URL:http://www.webcitation.org/query?url=https%3A%2F%2Fwww.bilgiguvenligi.gov.tr%2Fbt-guv.-standartlari%2Fiso-27001-2013-ve-iso-27002-2013-te-neler-degisiyor.html&date=2017-03-12, Son Erişim Tarihi: 12.03.2017.
43. İnternet: IDG Press Room. Turkish Security Software Market Tipped for Double-Digit Growth as IDC Reveals Latest Five-Year Forecast. *International Data Group*. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.idg.com%2Fnews%2Fturkish-security-software-market-tipped-for-double-digit-growth-as-idc-reveals-latest-five-year-forecast%2F&date=2017-03-12, Son Erişim Tarihi: 12.03.2017.
44. İnternet: Siber Bülten. (2015). Süleyman Özarslan ile söyleşi "*Rahat köşenizde otururak dünya pazarında rekabet edemezsiniz*". *SiberBülten*. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fsiberbulten.com%2Fsektorel%2Ftrky%2Frahat-kosenizde-oturarak-dunya-pazarinda-rekabet-edemezsiniz%2F&date=2017-03-12, Son Erişim Tarihi: 12.03.2017.
45. Knapp, K. J., Marshall, T. E., Rainer Jr, R. K. and Morrow, D. W. (2006). The top information security issues facing organizations: What can government do to help. *Network Security*,15(4), 51-58.
46. Bishop, M., (2003). *What is computer security?*. IEEE Security & Privacy, (1) 1, 67-69.
47. Kaplan, J., Sharma, S. and Weinberg, A. (2011). *Meeting the cybersecurity challenge*. McKinsey Quarterly, 1, 42.
48. Donaldson, S. E., Siegel, S. G., Williams, C. K. and Aslam, A. (2015). *Meeting the cybersecurity challenge*. Enterprise Cybersecurity, 27-44.

49. İnternet: Thompson, M. (2017). Security Issues Facing Companies. *Houston Chronicle*. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fsmallbusiness.chron.com%2Fsecurity-issues-facing-companies-75647.html&date=2017-05-29, Son Erişim Tarihi: 29.05.2017.
50. Younis, Y. A., Kifayat, K., and Merabti, M. (2014, February). An access control model for cloud computing. *Journal of Information Security and Applications*, 19(1), 45-60.
51. Wood, P. (2005, September). Implementing identity management security-an ethical hacker's view. *Network Security*, 2005(9), 12-15.
52. El Maliki, T., and Seigneur, J. M. (2014). Online identity and user management services. In J.R. Vacca (Ed.), *Managing Information Security (2nd Edt.)*. Boston,MA: Syngress,pp. 75-118.
53. Miyata, T., Madsen, P., Adachı, S. I., Tsuchıya, Y., Sakamoto, Y., and Takahashı, K. (2006, January). A survey on identity management protocols and standards. *IEICE Transactıons on Information and Systems*, 89(1), 112-123.
54. Gutierrez, A. J., and Feigenbaum, J. (2006). Towards better digital identity management. *Sensitive Information in a Wired World*, 1-24.
55. Seigneur, M. (2005). *Trust, Security and Privacy in Global Computing*, PhD Thesis, University of Dublin, Trinity College,36-38.
56. Florêncio, D., Herley, C., and Coskun, B. (2007). *Do strong web passwords accomplish anything?* Paper presented at the 2nd USENIX workshop on Hot topics in security (HOTSEC'07). Boston, MA,1-6.
57. Dinoor, S. (2010, December). Privileged identity management: securing the enterprise. *Network Security*, 2010(12), 4-6.
58. Laurent, M., and Bouzefrane, S. (2015). *Digital Identity Management*. Oxford: ISTE Press–Elsevier, 33-40.
59. Alkan, A. ve Kırlıdoğ, M. (2009, Şubat). Kurumsal Kimlik Yönetiminde Güncel Sorunlar. *Akademik Bilişim'10*, 5(4), 292.
60. Ayed, G. B., and Ghernaouti-Helie, S. (2011, September). *Digital identity management within networked information systems: From vertical silos view into horizontal user-supremacy processes management*. Paper presented at 14th International Conference on Network-Based Information Systems (NBiS), Tirana, 98-103.
61. Halim, R. and Shaharyar, S. A. (2009). Digital Identity Management. *Project Report for Information Security Course, Linköping University. The Department of Computer and Information Science,*1-5.
62. İnternet: Nazlı, M. (2009). Bilgi güvenliği açısından erişim kontrolü. *Tübitak UEKAE*. URL:http://www.webcitation.org/query?url=https%3A%2F%2Fwww.bilgiguvenligi.gov.tr%2Fkimlik-yonetimi%2Fbilgi-guvenligi-acisindan-erisim-kontrolu-2.html&date=2017-03-12, Son Erişim Tarihi: 12.03.2017
63. İnternet: Çankaya, Y. (2010). Kurumsal Kimlik Yönetimi ve Güçlü Kimlik Doğrulama. *Tübitak UEKAE*.URL:http://www.webcitation.org/query?url=https%3A%2F%2Fwww.bilgiguvenligi.gov.tr%2Fdokuman-yukle%2F4.-istanbul-etkinligi%2Fkuramsal-kimlik-yonetimi%2Fdownload.html&date=2017-03-12, Son Erişim Tarihi: 12.03.2017
64. Woodard, S., Brain, M., and Gattuccio, N. (1998). *Microsoft Technology: Networking, Concepts, Tools,* (Chapter-7: Network Design Manual, Directory Services: The Active Directory). Upper Saddle River, NJ: Simon & Schuster.
65. Telecommunication Standardization Sector of ITU. (2012). *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services* (ISO/IEC 9594-1). Switzerland, Geneva, 4.

66. İnternet: OCLC. X.500 and LDAP. *Online Computer Library Center*. URL:http://www.webcitation.org/query?url=http%3A%2F%2Fwww.collectionscanada.gc.ca%2Fiso%2Fill%2Fdocument%2Fill_directory%2FX_500andLDAP.pdf&date=2017-03-12, Son Erişim Tarihi: 12.03.2017.
67. Bulusu, P.(2015). *Detection of Lightweight Directory Access Protocol Query Injection Attacks in Web Applications*,Master's Thesis, Department of Computer Science- Kennesaw State University, Kennesaw, GA,10,31.
68. Koutsonikola, V., and Vakali, A. (2004). LDAP: framework, practices, and trends. *IEEE Internet Computing*, 8(5), 66-72.
69. Howes, T. A., Smith, M. C., and Good, G. S. (2003). *Understanding and deploying LDAP directory services*. Boston: Addison-Wesley Longman Publishing, 2-86.
70. Rose, M. (1991, February). Directory assistance service, RFC1202. *Internet Engineering Task Force.*
71. Howes, T., Smith, M., and Beecher, B. (1991, August). DIXIE protocol specification, RFC 1249. *Internet Engineering Task Force.*
72. Yeong, W., Howes, T., and Kille, S. (1995, March). Lightweight Directory Access Protocol, RFC 1777. *Internet Engineering Task Force.*
73. Howes, T., and Smith, M. (1995, August). The LDAP application program interface, RFC 1823. *Internet Engineering Task Force.*
74. Desmond, B., Richards, J., Allen, R., and Lowe-Norris, A. G. (2008). *Active Directory: Designing, Deploying, and Running Active Directory*. Sebastopol, CA: O'Reilly Media, 1-6.
75. İnternet: Microsoft. Active Directory'nin Özellikleri. *Microsoft*. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fweb.archive.org%2Fweb%2F20140221073434%2Fhttp%3A%2F%2Ftechnet.microsoft.com%2Ftr-tr%2Flibrary%2Fcc737139%28v%3Dws.10%29.aspx&date=2017-03-12, Son Erişim Tarihi: 12.03.2017.
76. İnternet: Microsoft. Tutorial Overview: ADSI with Visual Basic. *Microsoft*. URL:http://www.webcitation.org/query?url=https%3A%2F%2Fmsdn.microsoft.com%2Fen-us%2Flibrary%2Faa746492%28v%3Dvs.85%29.aspx&date=2017-03-12, Son Erişim Tarihi: 12.03.2017.
77. De Clercq, J., and Grillenmeier, G. (2007). 11 - Active Directory Delegation, In Microsoft Windows Security Fundamentals. *Microsoft Windows Security Fundamentals*. Burlington: Digital Press, 693-772.
78. İnternet: Microsoft. Securing Active Directory Administrative Groups and Accounts. *Microsoft*. URL:http://www.webcitation.org/query?url=https%3A%2F%2Ftechnet.microsoft.com%2Fen-us%2Flibrary%2Fcc700835.aspx&date=2017-03-12, Son Erişim Tarihi: 12.03.2017.
79. Adams, A., and Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40-46.
80. Kraus, R., Barber, B., Borkin, M., & Alpern, N. (2010). CHAPTER 1 - Windows Operating System – Password Attacks. *Seven deadliest Microsoft attacks*. Boston: Syngress, 1-23.
81. Bonneau, J. (2012, May). *The science of guessing: analyzing an anonymized corpus of 70 million passwords*. Paper presented at 2012 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, 538-552
82. Morris, R., and Thompson, K. (1979). Password security: A case history. *Communications of the ACM*, 22(11), 594-597.
83. Hayashi, E., and Hong, J. (2011, May). *A diary study of password usage in daily life*. Paper presented at the SIGCHI Conference on Human Factors in Computing Systems, Vancouver, BC, 2627-2630.
84. Zhang, L., and McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, 8(3-4), 180-197.

85. Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., Christin, N., and Cranor, L. F. (2010, July*). Encountering stronger password requirements: user attitudes and behaviors*. Paper presented at the Sixth Symposium on Usable Privacy and Security, Washington, 2.
86. İnternet: Süren, E., Parola Analizi. (2012). *Tübitak UEKAE*. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.bilgiguvenligi.gov.tr%2Fweb-guvenligi%2Fparola-analizi.html&date=2017-03-12, Son Erişim Tarihi: 12.03.2017.
87. Yan, J., Blackwell, A., Anderson, R., and Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security & privacy*, 2(5), 25-31.
88. Kuo, C., Romanosky, S., and Cranor, L. F. (2006, July). *Human selection of mnemonic phrase-based passwords*. Paper presented at the second symposium on Usable privacy and security, Pittsburgh, PA, 67-78.
89. İnternet: Doğu, K., Parolanızı Güçlü Kılın. *Tübitak UEKAE*. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.bilgiguvenligi.gov.tr%2Fson-kullanici-kategorisi%2Fparolanizi-guclu-kilin.html&date=2017-03-12, Son Erişim Tarihi: 12.03.2017.
90. İnternet:The Top 500 Worst Passwords of All Time. *Whatsmypass*. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.whatsmypass.com%2Fthe-top-500-worst-passwords-of-all-time&date=2017-03-12, Son Erişim Tarihi: 12.03.2017.
91. İnternet: Gray R. (2013). Most common and hackable passwords on the internet. *The Telegraph*.URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.telegraph.co.uk%2Ftechnology%2Finternet-security%2F10303159%2FMost-common-and-hackable-passwords-on-the-internet.html&date=2017-05-30, Son Erişim Tarihi: 30.05.2017.
92. İnternet: Slain, M. (2016). Announcing our Worst Passwords of 2016. *TeamsID*. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.teamsid.com%2Fworst-passwords-2016%2F&date=2017-03-12, Son Erişim Tarihi: 12.03.2017.
93. İnternet: Parsons, J. (2017). Worst passwords of 2016 revealed - and 123456 is STILL top of the list. *Mirror* .URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.mirror.co.uk%2Ftech%2Fworst-passwords-2016-revealed-123456-9644740&date=2017-05-30, Son Erişim Tarihi: 30.05.2017.
94. İnternet: Grauer, Y. (2017, January 23). 2016's Worst Passwords Are Just As Bad As 2015's. *Forbes*.URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.forbes.com%2Fsites%2Fygrauer%2F2017%2F01%2F23%2F2016s-worst-passwords-are-just-as-bad-as-2015s-so-please-tell-me-yours-is-not-on-the-list%2F2%2F%2369e9d83a59e8&date=2017-05-31, Erişim Tarihi: 31.05.2017.
95. Inglesant, P. G., and Sasse, M. A. (2010, April). *The true cost of unusable password policies: password use in the wild*. Paper presented at the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, GA, 383-392.
96. Gehringer, E. F. (2002, June). *Choosing passwords: security and human factors*. Paper presented at IEEE 2002 International Symposium on Technology and Society,*(ISTAS'02)*, Raleigh,NC, 369-373.
97. Scarfone, K. and Souppaya, M. (2009, April). Guide to Enterprise Password Management, *NIST SP 800-118 DRAFT*,25-26.
98. Hansman, S., and Hunt, R. (2005, February). A taxonomy of network and computer attacks. *Computers & Security*, 24(1), 31-43.
99. Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., and Kalita, J. K. (2014, April). Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications*, 40, 307-324.
100. Wilhelm, T. (2009). *Professional penetration testing: creating and operating a formal hacking lab*. Burlington, MA: Syngress Publishing, 339-391.

101. McClure, S., Scambray, J., and Kurtz, G. (2005). *Hacking exposed: network security secrets and solutions*. New York: McGraw-Hill/Osborne, 349,340.
102. Kraus, R., Barber, B., Borkin, M., & Alpern, N. (2010). CHAPTER 2 - Active Directory – Escalation of Privilege, In Seven Deadliest Microsoft Attacks. *Seven deadliest Microsoft attacks*. Boston: Syngress, 25-48.
103. Tsoutsos, N. G., and Maniatakos, M. (2014, March). Fabrication attacks: Zero-overhead malicious modifications enabling modern microprocessor privilege escalation. *IEEE Transactions on Emerging Topics in Computing*, 2(1), 81-93.
104. İnternet: The MITRE Corporation (2017). Authorization bypass through user-controlled key, CWE-639. *The MITRE Corporation* URL: http://www.webcitation.org/query?url=https%3A%2F%2Fcwe.mitre.org%2Fdata%2Fdefinitions%2F639.html&date=2017-05-31, Erişim Tarihi: 31.05.2017.
105. Monshizadeh, M., Naldurg, P., and Venkatakrishnan, V. N. (2014, November).*Mace:Detecting privilege escalation vulnerabilities in web applications*. Paper presented at the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, 690-701.
106. Weidman, G. (2014). *Penetration Testing: A Hands-on Introduction to Hacking*. San Francisco, CA: No Starch Press,109/197-215.
107. Graves, K. (2007). *CEH: Official Certified Ethical Hacker Review Guide: Exam 312-50*. Indianapolis,IN: John Wiley & Sons,74-78.
108. İnternet: TBD Bilişim Terimleri Karşılıklar Sözlüğü. *Türkiye Bilişim Derneği*. URL: http://www.webcitation.org/query?url=http%3A%2F%2Feski.tbd.org.tr%2Findex.php%3Fsayfa%3Dsozluk%26mi1%26tipi%3Dentr%26harf%3DA&date=2017-05-31, Erişim Tarihi: 31.05.2017.
109. Akyıldız, M. A.(2015). *Uygulamalarla Siber Güvenliğe Giriş*. Ankara: Gazi Kitapevi,211-247.
110. Arifoğlu,A., Demirer, M.,ŞENGÜL,G. ve ÖZ,O. (2006,Mayıs). *Bilişim Terimleri Sözlüğü*. Ankara: Onur Matbacılık,95-96.
111. Erguler, I. (2016, April). Achieving flatness: Selecting the honeywords from existing user passwords. *IEEE Transactions on Dependable and Secure Computing*, 13(2), 284-295.
112. Ghosh, R., Verma, S., Kumar, R., Kumar, S., and Ram, S. (2015). Design of Hash Algorithm Using Latin Square. *Procedia Computer Science*, 46, 759-765.
113. Federal Information Processing Standards Publication (2015, August). Secure Hash Standard (SHS), *FIPS PUB 180-4*.
114. İnternet: Barreto, P. S. L. M. (2008). The Hash Functions. *Laboratory of Computer Networks and Architecture*. URL:http://www.webcitation.org/query?url=http%3A%2F%2Fwww.larc.usp.br%2F%7Epbarreto%2Fhflounge.html&date=2017-03-12, Son Erişim Tarihi: 12.03.2017.
115. İnternet: The Open Web Application Security Project-OWASP, Testing for Brute Force,*OWASP-AT-004*, URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.owasp.org%2Findex.php%2FTesting_for_Brute_Force_+%28OWASP-AT-004%29+&date=2017-05-31, Son Erişim Tarihi: 31.05.2017.
116. İnternet: Security Focus (1997). NT "Pass the Hash" with Modified SMB Client Vulnerability. *Security Focus*. URL:http://www.webcitation.org/query?url=http%3A%2F%2Fwww.securityfocus.com%2Fbid%2F233%2Fdiscuss&date=2017-03-12, Son Erişim Tarihi: 12.03.2017
117. Ewaida, B.(2010). Pass-the-hash attacks: Tools and Mitigation. *Information Security Reading Room, SANS Institute*, 2.
118. Jadeja, N., and Parmar, V. (2016). Implementation and Mitigation of Various Tools for Pass the Hash Attack. *Procedia Computer Science*, 79, 755-764.
119. Allen, M. (2006). Social engineering: A means to violate a computer system. *Information Security Reading Room, SANS Institute*, 4-8.

120. Abawajy, J., Thatcher, K., and Kim, T. H. (2008, April). *Investigation of stakeholders commitment to information security awareness programs*. Paper presented at International Conference on Information Security and Assurance, ISA 2008. Busan 472-476.

121. Fujita, K., and Hirakawa, Y. (2008, September). *A study of password authentication method against observing attacks*. Paper presented at 6th International Symposium on Intelligent Systems and Informatics, Subotica, 1-6.

122. İnternet: Microsoft (2015, May). Local Administrator Password Solution (LAPS) Now Available.*Microsoft Security Advisory 3062591*. URL:http://www.webcitation.org/query?url=https%3A%2F%2Ftechnet.microsoft.com%2Fen-us%2Flibrary%2Fsecurity%2F3062591.aspx&date=2017-03-12, Son Erişim Tarihi: 12.03.2017

123. Waldemar, D. P. (2016). *Numerical methods, algorithms, and tools in C#*. Boca Raton: CRC Press, 286-287.

124. Daemen, J., and Rijmen, V. (1999, September). *AES Proposal: Rijndael*. National Institute of Standards and Technology (NIST), 1-45.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	:	SİNDİREN, Erhan
Uyruğu	:	T.C.
Doğum tarihi ve yeri	:	17/07/1979 Hamburg
Medeni hali	:	Evli
Telefon	:	0542 363 68 01
Faks	:	-
e-posta	:	erhan.sindiren@gazi.edu.tr

Eğitim Derecesi	**Okul/Program**	**Mezuniyet yılı**
Yüksek lisans	Gazi Üniversitesi /Adli Bilişim ABD	Devam Ediyor
Lisans	Anadolu Üniversitesi/ İşletme Bölümü	2010
Lise	MEBS Eğt.K.lığı/ Bilgi Sistemleri Teknik Astsubay Hazırlama Okulu (*Elektronik Bölümü*)	1997 1996

İş Deneyimi, Yıl	**Çalıştığı Yer**	**Görev**
1997- devam ediyor	Jandarma Genel Komutanlığı	Astsubay (*Bilgi Sistemleri, Ağ Güvenliği*)

Yabancı Dili

İngilizce

Yayınlar

Sindiren, E. and Ciylan, B., (2018, Jan.). Privileged Account Management Approach for Preventing Insider Attacks. International Journal of Computer Science & Network Security, 18(1), 1-10.

Hobiler

Amatör Balıkçılık, Yüzme, CTF Çözümleri, Sızma Testi Araçları

GAZİLİ OLMAK AYRICALIKTIR.