T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SİBER TEHDİTLERE KARŞI YENİ NESİL GÜVENLİ BASKI YÖNTEMİ; BİR İŞLETMEDE UYGULANMASI

YÜKSEK LİSANS TEZİ

Deniz GÖKÇEK

Enstitü Anabilim Dalı	**:**	**ELEKTRİK –ELEKTRONİK MÜHENDİSLİĞİ**
Enstitü Bilim Dalı	**:**	**ELEKTRİK MÜHENDİSLİĞİ**
Tez Danışmanı	**:**	**Prof. Dr. Ertan YANIKOĞLU**

Şubat 2022

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SİBER TEHDİTLERE KARŞI YENİ NESİL GÜVENLİ BASKI YÖNTEMİ; BİR İŞLETMEDE UYGULANMASI

YÜKSEK LİSANS TEZİ

Deniz GÖKÇEK

Enstitü Anabilim Dalı	**:**	**ELEKTRİK –ELEKTRONİK MÜHENDİSLİĞİ**
Enstitü Bilim Dalı	**:**	**ELEKTRİK MÜHENDİSLİĞİ**
Tez Danışmanı	**:**	**Prof. Dr. Ertan YANIKOĞLU**

Bu tez 02.02.2022 tarihinde aşağıdaki jüri tarafından oybirliği / oyçokluğu ile kabul edilmiştir.

Jüri Başkanı	**Üye**	**Üye**

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Deniz GÖKÇEK
02.02.2022

TEŞEKKÜR

Yüksek lisans eğitimim boyunca değerli bilgi ve deneyimlerinden yararlandığım, her konuda bilgi ve desteğini almaktan çekinmediğim, araştırmanın planlanmasından yazılmasına kadar tüm aşamalarında yardımlarını esirgemeyen, teşvik eden, aynı titizlikte beni yönlendiren değerli danışman hocam Prof. Dr. Ertan YANIKOĞLU'na, ilgilerini ve yardımseverliklerini her zaman hissettiğim değerli hocam Dr. Erdal ÖZDOĞAN'na teşekkürlerimi sunarım.

Üzerimde çok emekleri olan anneme, ahiret alemine göç etmiş babama ve kardeşlerime ayrıca çalışmalarım sırasında, maddi ve manevi desteklerini her zaman hissettiğim eşim Yurdanur GÖKÇEK'e çok teşekkür ederim. Şehadet şerbetini içen tüm şehitlerimize de Allah'tan rahmet diliyorum.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

AD	: Aktif Directory
API	: Application Programming Interface
BGYS	: Bilgi Güvenliği Yönetim Sistemi
DNS	: Domain Name System
DNS	: Domain Name System
IIS	: Internet Information Services
IP	: Internet Protocol
ISO	: Uluslar Arası Standartlar Teşkilatı
LAN	: Local Area Network
LDAP	: Lightweight Directory Access Protocol
MBYS	: Merkezi Baskı Yönetim Sistemi
MFP	: Multifuntional Printer
PAN	: Personal Area Network
QR	: Quick Response Code
SCCM	: Microsoft System Center Configuration Manager
SNMP	: Simple Network Management Protocol
SSH	: Secure Shell
USB	: Universal Serial Bus
WAN	: Wide Area Network

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Baskı güvenliği, merkezi baskı yönetim sistemi, SecuriPrint uygulaması, veri güvenliği, QR kod, MFP, yazıcı

Veri ihlalleri dünyanın her yerinde küçümsenmeyecek oranda artmaktadır. İşletmeler, siber saldırılar sonucunda potansiyel olarak itibar, yasal ve finansal kayıplara maruz kalmaktadır. Bu tehditlere karşı kurum ve kuruluşlar sürekli yeni çözümer geliştirmekte verilerin güvenlik ve gizliliğini sağlamak için çeşitli çözümler sağlamıştır. Fakat bilişim teknolojileri alanında yapılan bu atılımlara rağmen sıklıkla gözden kaçan sorunlardan biri de baskı altyapısıdır. Şirketler kritik iş süreçlerini yönetmek için baskı hizmetlerinden faydalanmaktadır. Değerli ve gizli birçok hassas veri içeren dokümanları yazıcılar üzerinden tedarik etmektedirler.

Artan bu siber tehditlere ve kötü amaçlı yazılımlara karşı baskı altyapısını geliştirmek ve çalışanlarının bilgi ve belge güvenliğini sağlamak her şirketin en önemli vazifesidir. Özellikle çalışan sayısı giderek artan şirketlerde iyi bir baskı altyapısı oluşturmak ve yeni bir baskı çözümü uygulamak en az ağ altyapısı kadar önemlidir.

Bu tez çalışmasında, üç farklı yerleşkede hizmet veren büyük bir şirketin baskı altyapısı incelenmiştir. İncelemeler neticesinde şirketin olumlu ve olumsuz durumları tespitler edilerek yeni bir baskı modeli tasarlanmıştır. Bu model ile şirketin bütün yerleşkeleri tek bir Merkezi Baskı Yönetim Sistemi (MBYS) altında birleştirilmiş baskı işlerinin merkezi olarak yönetilmesi sağlanmıştır. Yeni çözümün şirkete entegre edilmesi ile birlikte çalışanların baskı güvenliği sağlanmış belge takibi ve güvenliği ciddi oranda sağlanmıştır. Ayrıca güvenli baskı altyapısı ile yazıcı, kağıt, elektrik, toner gibi çeşitli sarf malzemlerden tasarruf edilmiş şirketin maliyet politiklarına önemli katkılar sağlanmıştır.

NEW GENERATION SECURE PRINTING METHOD AGAINST CYBER THREATS; IMPLEMENTATION IN A ORGANIZATION

SUMMARY

Keywords: Secure printing, central print management system, SecuriPrint application, data security, QR code, MFP, printer

With the developing technology, data has become the most valuable asset for companies and institutions. Parallel to this situation, there is a serious increase in data breaches. Businesses are potentially exposed to reputational, legal and financial losses as a result of cyber attacks. Institutions and organizations are constantly developing new solutions against these threats and have provided various solutions to ensure the security and confidentiality of data. However, despite these breakthroughs in the field of information technologies, one of the problems that is often overlooked is the printing infrastructure. Companies use printing services to manage critical business processes. They supply documents containing valuable and confidential data through printers.

It is an important duty for every company to develop the printing infrastructure against the increasing cyber threats and malicious software and to ensure the information and document security of its employees. Establishing a good printing infrastructure and implementing a new printing solution is as important as the network infrastructure, especially in companies with an increasing number of employees.

In this study, the printing infrastructure of a large company serving in three different campuses has been examined. Analyzing pros and cons of the existing printing model our new solution is determined. With our model, all campuses of the company were combined under a single Central Print Management System (CPMS) and centralized management of printing works was ensured. With the integration of the new solution into the company, the printing security of the employees has been ensured and document tracking and security has been ensured to a great extent. In addition, thanks to the secure printing infrastructure, various consumables such as printer, paper, electricity and toner have been saved and significant contributions have been made to the company's cost policies.

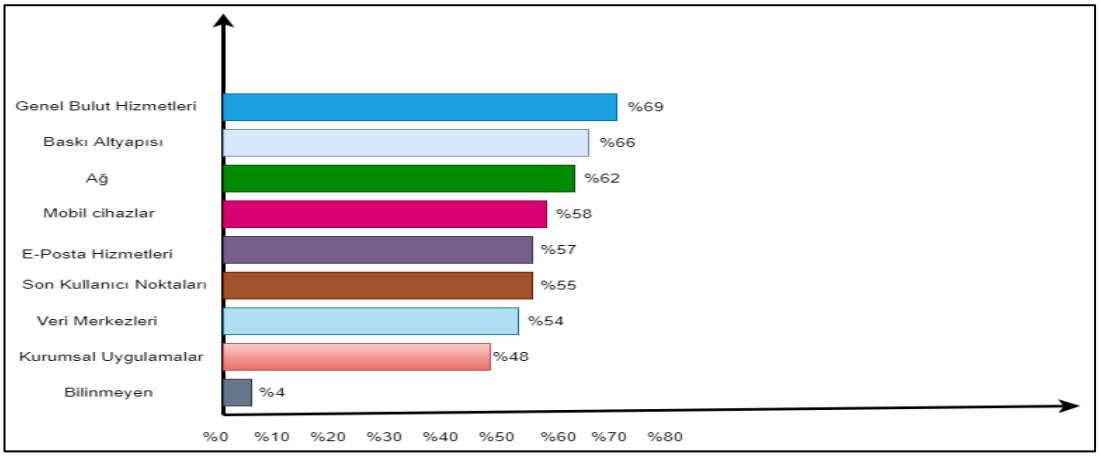
BÖLÜM 1. GİRİŞ

Bilgi teknolojilerindeki hızlı gelişme, kurum ve kuruluşların bilgiye her yerden ve merkezi olarak erişimi kolaylaştırmasından dolayı bilgi sistemleri teknolojileri hayatın her alanında etkin bir şekilde kullanılmaktadır. Günümüzde eğlenceden eğitime, ev ortamından en karmaşık yapıdaki şirketlere ve kamu kurumlarına kadar bilgi teknolojileri hayatımızın her alanında yer almaktadır [1]. Bilişim sistemlerinin ve ağ teknolojilerinin kullanım alanlarının artması ve bulut bilişimin kamu kurumları dahil birçok işletmede kullanıyor olması, üretilen ve işletilen bilginin güvenliğinin sağlanmasını da zorunlu hale getirmiştir [2]. İnternetin yaygınlaşması ile birlikte kurumlar ve şirketler ağ üzerinde önemli mahrem bilgiler paylaşmaktadır. Bu bilgilerin erişim izni olmayan üçüncü bir tarafın eline geçmesi halinde ciddi zararlara sebep olabilecektir [3]. Bir kurumdaki güvenlik açıkları, maruz kaldıkları başarılı siber saldırıları ve bilgi kayıpları kurumların itibarlarını ciddi oranda zedelemekte, güvenilirliklerini sarsmakta, pazar ve müşteri kayıplarına neden olabilmektedir. Bu saldırıların sonuçlarının getirdiği riskler düşünüldüğünde, bir kurum için bilgi güvenliğinin sağlanması hayati önem arz etmektedir [4]. Kurumlar, saldırıların etkilerini minimize etmek bilgi güvenliğini sağlamak amacıyla çeşitli yazılım ve uygulamalar geliştirmekte ve yeni metotlar aramaktadırlar. Fakat bilgi güvenliği uzmanlarının gözden kaçırdığı bir alan da baskı güvenliğidir.

Bilgisayar ağlarında kişisel bilgisayarlar, dizüstü bilgisayarlar ve sunucular gibi yaygın olarak kullanılan diğer bir ağ donanımı da yazıcılardır. Eskiden yazıcılar bilgisayarlara seri ya da paralel iletişim yöntemiyle bağlanan ve bilgisayarlarla doğrudan haberleşen, sadece çıktı almak için kullanılan makinelerdi. Ancak günümüzde teknolojinin gelişmesiyle kopyalama, yazdırma, tarama ve fax çekme özelliğine sahip Çok Fonksiyonlu Yazıcılar (Multifuntional Printer - MFP) halini aldılar. Ağa bağlı olarak çalışan bu cihazlar uzaktan yönetilebilmektedir. Bu gelişmelerle birlikte ağa bağlı diğer cihazlarda olduğu gibi yazıcıların da güvenlik

zafiyetleri ve eksik cihaz yapılandırmaları kurum ve kuruluşların ağ güvenliğini tehdit etmektedir. Yazıcılar, kendilerine özgü iletişim protokolleri gereği ağa bağlı diğer cihazlara oranla daha kolay istismar edilebilmektedir.

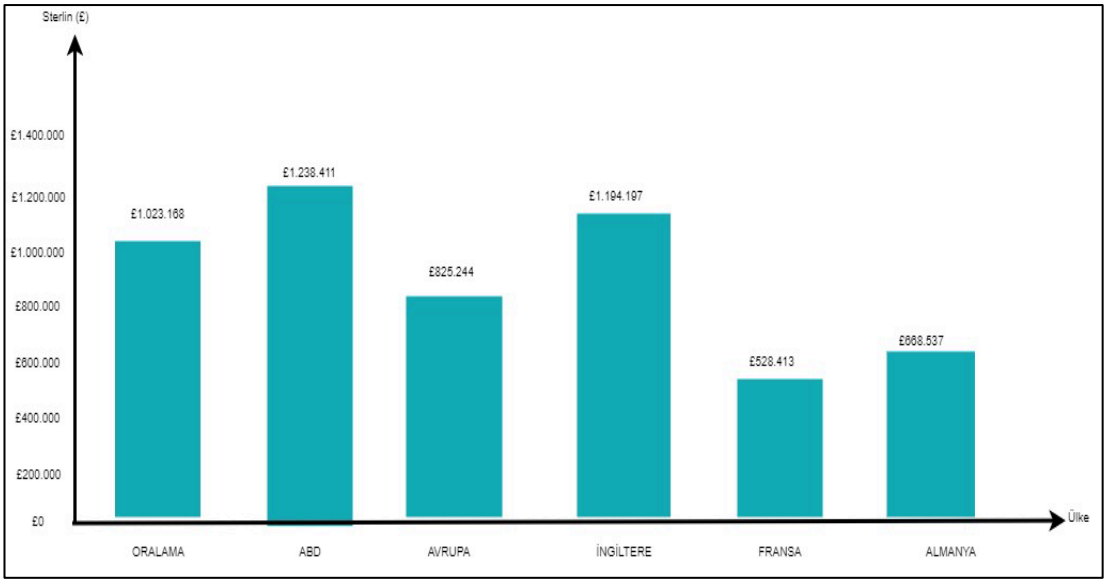
Quocirca'nın Baskı Güvenliği 2019 raporu, baskı güvenliğinin büyük bir endişe taşıdığını şirketlerin %59 ünün 2018 yılında belgelerin yazıcıya güvenli bir şekilde bırakılmadığından baskı ile ilgili veri kaybı yaşadığını belirtmektedir. İngiltere, Amerika Birleşik Devletleri (ABD) ve Fransa gibi ülkelerden 250 şirket üzerinden yapılan bir ankette ise genel güvenlik sorunları ve veri ihlallerine yol açabilecek riskler araştırılmış ve ihlallerin en yaygın olduğu beş alan listelenmiştir. Baskı güvenliğinden kaynaklanan veri ihlallerinin genel bulut hizmetinden kaynaklı veri ihlallerinden sonra ikinci sırada yer aldığı görülmüştür. Üstelik toplam veri ihlallerinin %66 'sının bu beş risk grubunda olduğu ve baskı güvenliği riskinin %69 gibi büyük bir paya sahip olduğu raporlanmıştır. Kurumlar kendilerini baskı güvenliğinden kaynaklı tehditlere karşı nasıl korumalıdır? Güvenlik ihlalleri ve veri sızıntısı ile ilgili endişeler sorulduğunda, ankete katılanların %73'ü endişeli veya çok endişeli olduğunu ifade etmiştir. Bu endişeye rağmen baskı altyapısının güvenlik ihlallerine karşı korunup korunmadığı ile ilgili soruya ise katılımcıların sadece %24'ü gerekli önlemlerin alındığını ve veri ihlallerinin yaşamadığını ifade etmiştir [5].



Şekil 1.1. Güvenlik ihlallerine yol açabilecek bilgi teknolojileri risklerinin derecelendirilmesi [5]

Bütün dünyayı derinden etkileyen covid-19 salgını her ne kadar insanları evde çalışmaya zorlasa da Quocirca'nın Baskı Güvenliği 2020 raporuna göre baskı

altyapılarının güvenliğine olan güven eksikliği göz önüne alındığında %64 oranında veri ihlali yaşandığı tespit edilmiştir. Bir önceki yıl yayınlanan raporda bu oran %66 olarak belirtilmişti. Baskı ile ilgili olarak maruz kalınan veri kayıplarının arkasındaki en önemli nedenler, çalışanların gizli belgeleri güvenli bir şekilde elden çıkaramaması, kötü amaçlı yazılımlar ve yazıcı tepsisinde biriken belgelerin yetkisiz kullanıcılar tarafından alınması gibi hususların olduğu değerlendirilmiştir [6]. Yine aynı rapora göre bu veri kayıpları, kuruluşlara yılda ortalama 1 milyon sterline mal olmaktadır. Kayıplar ABD'de 1,2 milyon sterline yükselirken ve Avrupa'da 825 bin sterlin seviyelerini görmektedir.



Şekil 1.2. Veri kaybının ortalama maliyet grafiği [6]

Veri kayıplarının bilançosu kapsamlı bir çalışmanın neticesinde ortaya çıkmaktadır. Şirketin yeteneklerin geliştirilmesi için yapılan yatırımların yanı sıra, bir veri kaybın ardından gerekli eylemlerin gerçekleştirilmesi için kaybolan zaman ve emek maliyeti, zarar gören müşterinin kaybolan güven ve itibar maliyeti gibi hususlar da düşünüldüğünde 2020 yılı için on milyon sterlinin üzerinde olduğu değerlendirilmektedir [6].

Bilgisayar ve yazılımdaki gelişmeler ve bilgi aktarımının elektronik belge sistemi ile yapılması baskı ihtiyacını kademeli olarak azaltması gerekiyordu ancak tam aksine basılı belge sayısı Quocirca'nın Baskı Güvenliği 2019 raporuna göre her yıl ortalama

%20 artmaktadır [5]. Bu durum maliyetin yanı sıra aşırı baskı, bir dizi kimyasal madde içeren mürekkep ve kağıt kullanımından kaynaklanan çevre sorunlarına da neden olmaktadır. Artan kağıt tüketimi ormanların yok olmasına da sebep olmaktadır.

Bu tez çalışmasında büyük bir şirketin baskı altyapısı ele alınacaktır. Şirketin mevcut baskı altyapısı, güçlü ve zayıf yönleri belirlenmiştir. Bu veriler ışığında güvenli Merkezi Baskı Yönetim Sisteminin (MBYS) altyapısı için gerekli çalışmalar ve gereksinimler adım adım analiz edilmiştir. Uzun bir araştırmanın neticesinde şirket ihtiyaçlarına büyük oranda cevap veren Entera A.Ş. firmasının SecuriPrint uygulaması çözüm olarak belirlenmiştir. Seçilen uygulama ile üç ayrı yerleşkede hizmet veren şirketin baskı altyapısı merkezi olarak yönetilmesine olanak sağlanmıştır. Şirketin baskı politikaları belirlenmiş, dokümanların takibi ve raporlanması sağlanmıştır. Ayrıca gereksiz kağıt, kartuş, elektrik vb. gibi çeşitli sarf malzemelerin tüketimi engellenmiş şirket kaynakları en verimli şekilde kullanılması sağlanmıştır.

BÖLÜM 2. BASKI GÜVENLİĞİ

2.1. Baskı Güvenliği Nedir?

Baskı güvenliği; istenilen belge ve dokümanlara sadece yetkilendirilmiş kişilerin ulaşabilmesini sağlayarak veri güvenliği hususunda karşılaşılabilecek her türlü kötü amaçlı tehditlerin önlenmesini sağlamak, yazıcılara (MFP) yetkilendirme yazılımları kurarak bu cihazlara yalnızca kişiye özel Kişisel Kimlik Numarası (Personal Identfication Number-PIN) kodu ve kimlik kartları ile erişim imkanının sağlamaktır. Güvenli baskının temel amacı, hassas verileri muhafaza etmek, bilgi ve belgelerin yanlış ellere girmesini engellemektir.

Ağ yazıcılarının kullanımının artması ile veriler daha değerli hale gelmiştir. Bu artış yanında bilinçli veya bilinçsiz veri ihlallerini ve veri hırsızlığını da beraber getirmiştir. Veri hırsızlığı, fiziksel belgelerin yazıcı tepsisinden çıkmasıyla başlar. Hırsızlar, faturalar, özel belgeler, kredi kartı bilgileri, banka hesap numarası, sertifikalar, kişisel kayıtlar gibi gizli bilgilere ve özel bilgileri içeren diğer birçok yasal belgeye yazıcı tepsisinden doğrudan erişim sağlayabilir. Örneğin, çoğu kamu kurumu veya özel kuruluş gizli veya hizmete özel belgeleri ağa bağlı bir yazıcı üzerinde basmaktadır. Belge yazıcıda çıktığı anda kötü niyetli kişiler belgeyi ele geçirebilir ya da fotoğrafını çekerek sosyal medya platformlarında paylaşabilmektedir [7]. Bu davranış hem kurum itibarını zedelemekte hem de birçok çalışanın mağdur olmasına sebep olmaktadır.

Ağ yazıcılarını korumanın bir diğer yöntemi ise siber tehditlere karşı sistemin güvenlik açıklarını tespit etmek ve bu tehditlere karşı hem ağ yapısını hem de yazıcıların güvenlik açıklarını en aza indirgenmektir. Bu açıkları kapatmanın en iyi yolu ise gelişmiş güvenli baskı uygulamalarını mevcut baskı sistemine entegre etmekle mümkün olabilir. Belgeler filigran, kare kod vb. özellikler sayesinde hem kötüye

kullanıma karşı caydırıcılığı arttıracak hem de merkezi olarak evrak takibi yapılabilecektir. İyi bir baskı altyapısı sadece çalışanları memnun etmekle kalmayacak aynı zamanda kurumun imajını da artıracaktır. Bu tez çalışmasında, mevcut baskı altyapısı yeniden tasarlanacak ve sistem zafiyetleri en aza indirilecektir. Tüm çalışanlar için baskı güvenliğini sağlayacak bir baskı çözümü sunulacaktır.

2.2. Baskı Güvenliğini Etkileyen Faktörler

2.2.1. Ağ güvenliği ve yönetimi

İlk bilgisayar 1970 li yıllarda icat edildi ve ilk kez askeri kurumlar başta olmak üzere diğer devlet kurumlarında iletişim ve bilgi paylaşımını kolaylaştırmak için bilgisayarlar arası ağ bağlantısı bu dönemlerde kurulmuştur. Bu ağ yapısını kurmanın en büyük nedenlerinden biri ise bilgisayarın depolama alanını paylaşmak ve bunları bir yazıcıya bağlamaktı [8].

Bilgisayar ağları bir şirketin farklı coğrafi alanlarında faaliyet gösteren birimleri arasında iletişim sağlayabildiğinden kurumsal işletmelerin çoğunda kritik öneme haizdir. İşletmeler gelişim ve büyümelerine paralel olarak daha fazla uygulama ve kullanıcıyı destekleyen büyük ağlara gereksinim duymaktadırlar. Bunun neticesinde ağlar; bağlantı kabloları, anahtarlar, yönlendiriciler, ana bilgisayarlar ve diğer aygıtları içeren çok sayıda ve birbiriyle etkileşimi olan donanım ve yazılım bileşenlerini kapsamaktadır. Ağa bağlı bu sistemlerin çalışması, yönetimi, bakımı doğru yapılandırılması işletmelerin en büyük arzusudur. Çünkü ağda meydana gelen en ufak bir arıza her kuruma büyük zaman ve maliyet kaybına neden olacağı aşikardır. Şirketlerin geniş alana yayılmış çok sayıda ağ bileşeninin takibini yapabilmesi için merkezi bir ağ izlenme, yönetme ve kontrol etmeye yardımcı olacak yazılım ve donanım araçlarına ihtiyaç duymaktadırlar. Ağ yönetimi, bir sistemin kurumsal hedeflere uygun olarak etkin ve verimli şekilde çalışmasını sağlayan işlemler bütünüdür. Bunu başarmak için ağ kaynaklarının denetlenmesi, ağ hizmetlerinin koordine edilmesi, ağ durumlarının izlenmesi ve ağ durumunun raporlanması gerekmektedir [9].

Ağ güvenlik yönetiminin anlaşılabilmesi için öncelikle ağ kavramının açıklanması gerekmektedir. Temel olarak bilgisayarlar, yazıcılar, sunucular gibi bilişim sistemlerini anahtar ve yönlendirici gibi aracı cihazlar ile birbirine bağlayan sistemlerdir. Bilgisayar ağları çalışma prensipleri, amaçları, büyüklükleri gibi çok çeşitli açılardan kategorize edilebilir. Bu kısımda ağ yazıcılarının ve baskı hizmetlerinin kullanımı göz önüne alınarak büyüklüklerine göre sınıflandırmaya değinilecektir.

Kullanılan ağlar büyüklüklerine göre:
Kişisel Alan Ağı (Personal Area Network - PAN); 10 m gibi kısa mesafeye yayılan bireyin çalışma alanına odaklanan araçları birbirine bağlamak için kullanılır. Bu ağ, bilgisayarlar, cep telefonları, tabletler ve bireysel dijital cihazları gibi araçlar arasında bilgi aktarımı sağlar [10]. Bir yazıcı ile kişisel bir bilgisayar arasında oluşan ağ kavramı bir PAN örneğidir

Yerel Alan Ağı (Local Area Network - LAN); bir ev, işyeri, bina veya kampüs gibi sınırlı bir alandaki bilgisayarları ve cihazları birbirine bağlayan özel bir ağdır. Tipik bir LAN bilgisayar, yazıcı ve bunun gibi diğer cihazları birbirine bağlar. LAN'lar kullanıcıların uygulamalara ve ağa bağlı cihazlara ulaşım, sisteme bağlı cihazlar arasında dosya paylaşımı, elektronik posta ve çeşitli uygulamalar vasıtasıyla haberleşme gibi pek çok avantaj sağlamaktadır [10]. Bu tür ağlarda genellikle ağ yazıcıları kullanılır ve kurumsal birden çok şubeye hizmet verecek şekilde tasarlanır.

Geniş Alan Ağı (Wide Area Network -WAN); farklı coğrafi alanlara dağıtılmış çoklu erişim düğümlerini birbirine bağlayan bir telekomünikasyon ağıdır. İşletmeler WAN'ları farklı şubelerine bağlanmak ve bir bulut bilişim sağlayıcısından sağlanan bulut hizmetlerine ulaşmak için kullanır [11]. LAN'ları birbirine bağlanmasını sağlayan çok geniş ağlardır. En meşhur geniş alan ağı internettir.

Kuruluşlar envanterlerinde bulunan ağ cihazlarının yönetimi için gerekli olan birinci unsur ağ yönetim protokollerinin aktif hale getirilmesidir. Ağ yönetim sistemlerinin

cihaz yönetimi için kullandığı ağ yönetim protokolleri, Basit Ağ Yönetim Protokolü (Simple Network Management Protocol-SNMP) ve Uzaktan Ağ Yönetme Protokolü (Remote Network Monitoring-RMON) protokolleridir. Anahtar ve yönlendirici gibi aktif kullanılan ağ cihazlarında bu işlem komut satırı ara-yüzü (Command Line Interface-CLI) üzerinden yapılmaktadır. Komut satrı ekranına, ağ cihazının uzaktan erişim ara-yüzünden (Secure Shell-SSH/ Telecommunication Network-TELNET) veya konsol portu üzerinden erişim sağlanarak istenilen yapılandırma ayarları yapılabilir. Benzer şekilde ağ hizmetini sekteye uğratacak ya da cihazların çalışmasını engelleyecek siber saldırılara karşı güvenlik önlemlerinin alınması da önemli bir koşuldur. Ağ cihazlarının doğru ve sistemli yapılandırması ve gerekli güvenlik önlemlerinin alınması, şirket içi veya dışarıdan yapılabilecek siber saldırılara karşı ağ altyapısını güvende tutacaktır. Özellikle Ortam Erişim Yönetimi (Media Access Control- MAC) adresi, Dinamik Host Yapılandırma Protokolü (Dynamic Host Configuration Protocol -DHCP) ve Domain Name System (DNS) üzerinden yapılacak siber atakları engellemek amacıyla ağ bileşenlerinde yapılan güvenlik yapılandırmaları şirketin hizmet kalitesini artıracak ve kesintileri önleyecektir. Sistemde bulunan ağ cihazlarına güvenli protokoller (SSL, HTTPS) üzerinden bağlantılar yapılmalı, yetkisiz erişimleri ve araya girme (man in the middle) saldırılarının önüne geçilmelidir [9]. Özetle, ağ cihazlarının güvenliğinin sağlanması yazıcı ve baskı hizmetlerinin de güvenli bir şekilde sağlanması içinde önemlidir. Ağa yapılan her saldırı kurumun hassas verilerine erişim riskini tetiklemektedir.

2.2.2. Ağ aygıtlarının güvenliği

Ağ aygıtları doğrudan birbirine bağlı olan veya bir bilgisayar ağı üzerinden veri alan ya da gönderen anahtar, yönlendirici, hub vb. tüm cihazlardır. Bu çalışmada kullanıcı bilgisayarı ile yazıcı arasındaki bağlantıyı analiz etmek önem arz etmektedir. Yerel yazıcılar ile ağ yazıcıları arasındaki fark yerel yazıcıların doğrudan bilgisayarlara bağlı olmasıdır. Genellikle birkaç metrelik kısa Evrensel Seri Veriyolu (Universal Serial Bus -USB) kablo ile yazıcıya yerel olarak bağlı olduğundan dolayı sadece yalnızca bir kullanıcı bağlanabilmektedir. Bu özelliği sebebiyle yerel yazıcılar çoğunlukla evlerde ve küçük işletmelerde kullanılmaktadır. Ağ yazıcıları ise ağa bağlı bilgisayarda toplu

olarak baskı yapan orta ile büyük ölçekli kurumsal şirketler tarafından tercih edilmektedir. Bu yazıcılar bir ağ yazıcı kartına sahip olup, yazıcı yapılandırıldıktan sonra bir IP adresi ile ağa tanımlanabilmektedir [12]. Ağ cihazları genellikle birbirleri ile sürekli bir iletişim halinde oldukları için herhangi bir ağ aygıtını ele geçiren bir saldırgan diğer ağ cihazlarını da ele geçirmesi kaçınılmazdır. Dolayısıyla ağ aygıtlarında meydana gelen bir güvenlik açığı sistemin baskı altyapısı içinde büyük bir tehlikedir.

BÖLÜM 3. GÜVENLİ MERKEZİ BASKI YÖNETİM SİSTEMİ

3.1. Amaç

ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) kalite sisteminin kurum ve işletmelerde uygulanması gereken birçok süreç bulunmaktadır. Bu süreçlerde kuruluşların yaptığı iş ve işlemlerin doküman haline getirilmesi, raporlanması, bilgi varlıklarının envanterlerinin tutulması gibi pek çok bilginin tutulması gerekmektedir. Elde edilen bu bilgilerin zaman içinde değişiminin takip edilmesi, farklı mecralarda elde edilen belgelerin iz bilgilerinin takip edilmesi kurumlar için en önemli unsurdur. Kuruluşların bu gizli ve özel bilgileri çeşitli baskı cihazları aracılıyla temin etmesi bu cihazların önemini artırmaktadır. Bir şirketteki her çalışanın istisnasız kullandığı baskı sistemlerinin alt yapısını siber ataklara karşı korumak, güvenli bir baskı çözümü uygulamak her kuruluşun temel görevidir. [13].

Bu tezin temel amacı, merkezi bir baskı merkezi sistemi tasarlamak ve bu sistemi kurumsal bir şirkette hayata geçirmektir. Bu vesile ile yazdırma işlerinde yazıcı ve yazdırma güvenliğini sağlanması, depo kayıtlarının takip edilmesi, toner ve yazdırma tasarrufu sağlanması, süreç takibinin yapılabilmesi, tasarruf tedbirleri kapsamında maliyetlerin minimize edilmesi ve iş yükünün azaltılması amaçlanmıştır. Bunu yaparken öncelikle kurumun mevcut durumu analiz edilmekte şirketin güçlü ve zayıf yönleri tanımlanmaktadır. Yeni modelin tasarımı oluşturulduktan sonra, uygulama prosedürü tanımlanarak uygulama süreci belirlenmektedir. Daha sonra ise eski sistemden yeni sisteme geçişi şirkete benimsetmek, sistem uygulanırken personel tarafından gelebilecek olası fırsat ve tehditleri tanımlamaktır. Son olarak, bu değişikliklerin uygulanması için bir mali analiz ve bir zaman çizelgesi oluşturmaktır.

Merkezi Baskı Yönetim Sistemi (MBYS), uygulandığı şirketlere birçok fayda sağlamakla birlikte en önemli özellikleri aşağıda açıklanmaktadır.

3.1.1. Merkezi yönetim

Çalışan sayısı fazla olan kurumsal ağlar, şirketin farklı coğrafi birimleri arasında iletişim sağlayabildiğinden üzerinde çok fazla yazılım ve donanım araçları bulundurmaktadır. Bu durum büyük ağlarda yönetimsel problemlerin meydana gelmesini tetiklemektedir. Bu dağıtık mimariler birden fazla uygulama sunucusu bulunduğu için sunucuların ayrı ayrı yönetilmesi ve lisanslanması zordur. Merkezi yönetim, dağıtık yapıdaki birden çok uygulama sunucusun yönetimini, lisanslanması ve loglarının izlenmesi tek merkezden yapılmasına imkan tanımaktadır.

3.1.2. Kimlik doğrulama

Kurum veya kuruluşlar bünyesinde birçok uygulama, ara-yüz ve sisteme kullanıcı girişi sağlamak için veri tabanı ile iletişime geçip daha önceden sisteme kayıtlı olan kullanıcı adı, parola ve yetki grubu bilgilerini doğrulaması gerekmektedir. Çoğunlukla her uygulamanın veri tabanı ayrı olduğu için bu durum her uygulamanın kendine özgü bir kimlik doğrulama mekanizmasının olması sonucunu doğurmuştur. Bu durum belli süre sonra karmaşık bir hal alıp, kullanıcı adı ve parolaların hangi uygulamaya ait olduğu gibi birtakım soru ve sorunlara sebep olacaktır. Bununla birlikte parola gizliliğini de göz önünde bulundurmak gerekmektedir [14].

Yazıcılar için kimlik doğrulaması, yerel ve iş kimlik doğrulması olmak üzere iki farklı yöntemle yapılabilmektedir. Yerel kimlik doğrulama, yazıcıya kayıtlı kullanıcı bilgilerini izleyen kimlik doğrulamayı tanımlamak için kullanılan bir yöntemdir. Yerel kimlik doğrulamasında, ayrıntılı kullanıcı yönetimi veya uzaktan yönetim araçlarının erişimi bulunmaz (ssh, rdp vs.). İş kimlik doğrulaması, Active Directory, Kerberos, LDAP gibi bir kimlik doğrulama sunucusuyla bağlantı kurarak kimlik doğrulama yöntemi belirtilir. Buna ek olarak kullanıcıların kart okuyucu teknolojisiyle bir kart ve şifre birleşimini kullanarak iki aşamalı bir doğrulama yapmaları da alınabilecek başka bir güvenlik önlemidir.

Yazıcı ve sunucu üzerinde kurulu bulunan çeşitli uygulamalar sayesinde elektronik kimlik kartları ile temessız giriş yaparak ya da kullanıcı adı ve parola yoluyla yazıcı ile iletişim kurulması sağlamak bu sayede çıktı alınacak dokümanın yetkisiz kişişlerin eline geçmesi engellenecektir.

3.1.3. Baskı politikaları belirleme

Üst yönetim tarafından onaylanmış baskı kuralları oluşturulmalıdır. Bu kurallar üst yönetimin bilgi güvenliği yönetimi politikaları ile ilgili taahhüdünü ve kurumsal yaklaşımını yansıtmalıdır. Baskı politikaları, bilgi güvenliği yönetiminin daha verimli hale getirilmesi için tasarlanmıştır. Kurum içi veya dışı yanlış ve kötü amaçlı kullanıma karşı bilgi ve belgelerin korunması için gerekli beklentilerin karşılanması hedeflenir [15]. Politikalar, hizmetleri amaçlandığı gibi yani sadece yetkili personel tarafından yönetilmesine imkan tanımaktadır. Merkezi olarak çeşitli baskı politikaları belirleyerek kullanıcıların ihtiyacına göre zaman ve maliyet tasarrufunun yanı sıra evrak güvenliği de sağlanabilecektir.

3.1.4. Maliyet yönetimi ve tasarruf

Kurumların son zamanlarda en çok dikkat ettiği konulardan bir diğeride tasarruf ve maliyet yönetimidir. Şirketler, mürekkep/toner ve kağıt tüketimini azaltarak para tasarrufu konusunda muazzam bir potansiyele sahiptir. Bunu yapmanın en önemli yollarından biri mürekkep/toner tüketimini azaltan özel olarak tasarlanmış yazı tiplerini kullanmak, diğeri ise genel baskı maliyetlerini azaltmak için tasarlanmış yazılım çözümleri baskı altyapısına entegre etmektir [16].

Geleneksel baskı yönteminde bilgisayar ortamında gönderilen bütün çıktılar yazıcı üzerinde doğrudan alınabilmektedir. Yanlış yazdığınız ya da düzeltmek istediğiniz bir dokümanı geri getirme şansımız yoktur. Bu durum yazıcı ömrünün azalması, enerji, kağıt, toner vb. kayıplara neden olmaktadır. Yeni baskı sistemi ile yazıcıya üzerinde kimlik doğrulaması yapıldıktan sonra sadece çıktı alınmak istenen doküman seçilip

alınabilmektedir. Yanlışlıkla gönderilen ya da çıktı alınması istenmeyen belgeler, tanımlanan saat aralıklarında sistem tarafından otomatik olarak silinmektedir.

3.1.5. Filigran ve QR kod uygulaması

Yazıcılar günümüzde kurumlar, işletmeler ve bireyler tarafından yaygın olarak kullanılan ofis ekipmanlarıdır ve dijital baskıda insanların günlük yaşamlarında yaygın olarak kullanılmaktadır. Dijital içeriğin önemli bir parçası olarak Kare (Quick Response-QR) kodları genellikle gazetelerde, dergilerde, reklam broşürlerinde, kitaplarda, ambalajlarda, ve bazı kişisel kartvizitlerde basılmaktadır. Kullanıcılar, bilgi edinme, web sitesi yönlendirme, reklam gönderme, sahteciliğe karşı izlenebilirlik, mobil ödeme, bilgi teknolojisi vb. amaçlar için QR kodlarını bir cep telefonu kamerasıyla taratıp istenilen bilgiye erişim sağlayabilmektedir [17].

Filigran ve QR kod fiziksel dokümanların takibini sağlayan güvenlik uygulamalarıdır. Kurumsal dokümanlar üzerinde QR kodunun yazıcı kaynağının belirlenmesi büyük önem taşımaktadır. Çıktı alınan doküman çok gizli ya da hizmete özel bir belge olabilir. Bu belgenin sosyal medya gibi çeşitli ortamlarda paylaşıldığını düşünürsek kurumsal itibarı ne kadar sarstığını hayal bile edemeyiz. Bu tür sorunların önüne geçebilmek için baskı sırasında belge üzerinde bulunan filigran ve QR kod sayesinde belgenin kimin tarafından alındığı, ne zaman alındığı hangi IP ve bilgisayar üzerinde alındığı gibi bilgilere ulaşılabilmektedir.

3.1.6. İçerik bazlı filtreleme

İçerik Bazlı Filtreleme terimi, gelişen teknoloji sonucunda oluşan veri miktarının artışıyla birlikte günümüzde en çok kullanılan terimlerden biri haline gelmiştir. Veri kaynaklarının hızla artmasıyla farklı kaynaklardan ve farklı tiplerde veriler hayal edilemeyecek miktarda bir yer kaplamaya başlamıştır. Sahip olunan verinin depolanması, işlenmesi, analiz edilmesi gerekmektedir. İstenilen verinin çok fazla kaynak arasından seçilmek zorunda olunması ve alternatiflerinin artması problemin temelini teşkil etmektedir. Bu noktada içerik bazlı filtrelemeye ihtiyaç duyulmaktadır.

Daha detaylı olarak belirtmek gerekirse, içerik bazlı filtreleme sistemlerinin amacının kullanıcıların aradığı ve ihtiyaç duyduğu bilgilerin bir an önce kullanıcıya doğru bir şekilde getirmesi olarak özetlenebilir [18]. Örneğin; içerisinde "Gizli" ibaresi geçen belgelerin çıktı alınması engellenebilir.

3.2. Şirketin Mevcut Durumu

Hedeflere başarılı bir şekilde ulaşmak için, kuruluşun çevresini analiz etmek, yani mevcut durumunu tanımlamak ve belirli sorunları belirlemek gerekir. Bu tez çalışması kapsamında gerçekleştirilen uygulama gerçek bir kurum ortamında yapılmıştır. Geliştirilen çözüm her ne kadar bu şirket içerisinde uygulanmış olsa da çalışma kapsamında tüm kurumlar için geçerli olacak şekilde genel bir yaklaşım benimsenmiştir. Böylece benzer özelliklere ve sorunlara sahip başka kuruluşlar da aynı yöntemi uygulayabileceklerdir. Sorun, şirketteki tüm çalışanları ilgilendiren güvenli olmayan yazdırma süreci olduğu için, sorun ve organizasyon hakkında temel bilgiler elde etmek gerekmektedir. Bu bilgileri elde etmek için şirketin yöneticisiyle ve teknik personeli ile doğrudan iletişime geçilmiş ve kurumda bulunan yazıcı sayısı, türleri, işlevleri ve yazıcıların dağılım şekilleri ilgili detaylı bilgi toplanmıştır. Bu bilgiler ışığında mevcut durum analiz edilerek kurumun talepleri ve beklentileri tespit edildi. Elde edilen tüm veriler, kurumun taleplerine uygun bir baskı çözümü bulmak için kullanıldı.

Bu bölümde yeni baskı sisteminin analizinin ve uygulamasının gerçekleştirileceği organizasyonun tanıtımı yapılacaktır. İlk olarak kurumun mevcut durumu değerlendirilerek güçlü ve zayıf yönleri ortaya çıkarılacaktır. Bu yönler tanımlandıktan sonra uygun çözüm sağlayıcı aranacak, ilk tasarım çözümlerini oluşturmak mümkün olacaktır. Sunulan fazlalıklara göre potansiyel sağlayıcılar ele alındıktan sonra, belirli bir çözüm için bir finansal bütçe hazırlanacaktır. Bütçenin kuruluş tarafından onaylanmasının ardından, firma ile iş birliği içinde çözümün ilk aşamasına geçilecek ve model bir çözüm hayata geçirilecektir. Uygulamadan sonra, çözüm belirli bir süre çalıştırıldıktan sonra test edilmesi için bir test grubu oluşturulmuştur. Çözümün test edilmesine müteakip, kurumun yeni durumunu

tanımlanacak ve böylece yeni sistemin kurumda benimsenmesi için çalışmalar yapılacaktır.

3.2.1. Şirketin yapısı ve tanımı

Çözümün uygulanacağı kuruluşun adı kurumun güvenlik politikaları sebebiyle gizli tutulmuştur. Ancak, aynı sorunu yaşayan diğer şirketler için çözüm genel çerçeve olarak benzer şekilde olacaktır. Kurum, Türkiye'de faaliyet gösteren büyük şirketler arasında yer alan ve bölge genelinde birkaç farklı yerleşkede hizmet veren bir şirkettir. Kurum yasal ve uluslararası faaliyetlerde bulunan hiyerarşik bir yapıya sahip olmakla birlikte aynı şehirde hepsi tek bir organizasyon yapısına ait üç farklı lokasyonda hizmet vermekte, her biri çoğunlukla bir bilgisayarda çalışan ve bir yazıcıya erişmesi gereken yaklaşık 2500 çalışanı bulunmaktadır. Merkez binalar "O" şeklinde birbirine bağlanan on kat ve dört ana koridordan oluşmaktadır. Her katta ofisler, 12-36 metrekare olan hücrelere bölünmüştür. Çalışanların dağılımı yaptıkları işlere göre değişmektedir. Şube müdürleri, 12 metrekarelik ayrı ofislere sahiptir. Yaptıkları işlere göre 1-4 kişilik veya daha fazla çalışanların bulunduğu ofisler bulunmaktadır. Organizasyon, çeşitli bölümlere ayrılan birkaç bölümden oluşmaktadır. Yazıcılar her binanın ara katında bulunan bir yazıcı odasında hizmet vermektedir. Çalışanlar çıktı almak istediklerinde yazıcı odasına gidip imza karşılığında çıktılarını teslim alabilmektedirler.

Şirketin yerleşim düzeni, personelin kişisel veri güvenliğinin sağlanması veya diğer nedenlerden (hassas verilerin gizliliği vb.) dolayı yazıcılara erişiminin kolay olması önem arz etmektedir. Bu nedenle, çalışanların yazıcılara mümkün olduğunca yakın ve çok fonksiyonlu yazıcılara ihtiyacı duyduğu anlaşılmaktadır. Ancak en önemli sorunlardan biri de yazdırılan sayfa sayısının fazla olmasıdır. Bu durumu engellemek için şirket, yıllar içinde farklı türde fotokopi makinelerinin yanı sıra birçok yazıcı satın almıştır. Bunları sağlıklı bir şekilde işletmek ve yönetmek, kurum için önemli kaynaklar tüketmektedir. Bu makinelerin belli bir plan kapsamında satın alınmaması, yanlış yapılandırılması nedeniyle birçok yazıcı türü ve yazıcılara uyumlu sarf malzemesi türü ortaya çıkmıştır. Şirketin her tür yazıcı için ayrı yazıcı malzemesi,

toner, bant birimleri ve çeşitli parçalar için ayrı ayrı sipariş vermeleri gerekmektedir. Bu durum şirkete zaman ve maliyet açısında ciddi zararlar vermektedir.

Küçük yazıcılar fiyat olarak daha ucuz, ancak toner ve diğer sarf malzemeleri gibi malzemeler, daha büyük ve daha modern makinelere göre sayfa sayısına göre çıktı alındığında maliyetler kurum bütçesini daha fazla etkilemektedir. Bu durum Tablo 3.1.'de sayısal değerler ile ifade edilmiştir.

Tablo 3.1. Farklı yazıcı türleri için yazdırılan sayfa fiyatlarının karşılaştırılması [19]

Yazıcı Türü	Kartuş Başına Fiyat (TL)	Yazdırılan Sayfa Sayısı	Sayfa Başına Fiyat (TL)
Küçük Renkli Yazıcı # 1	327	475	0.69
Küçük Renkli Yazıcı # 2	730	1400	0.52
Ortaboy Renkli Yazıcı #1	978	8000	0.12
Ortaboy Renkli Yazıcı #2	999	9200	0.11
Büyük Renkli Yazıcı # 1	1650	7500	0.09
Büyük Renkli Yazıcı # 2	600	25,000	0.02

3.2.1.1. Teknik destek

Destek masası, şirkette bulunan teknik malzemelerin sorunsuz çalışmasının sağlandığı, bütün teknik sorunların iletildiği bir uygulamadır. Baskı hizmeti bu kategoride bulunduğu için baskı makinelerinin yönetimi, bakımı ve sarf malzemelerinin yenilenmesi destek masasına kaydedilmekte ve ilgili teknik personele yönlendirilmektedir. Yazıcılara kağıtların doldurması işlemi haricinde, çalışanların tüm ekipman ve yazıcılara müdahale etmeleri kurumsal politika gereği yasaklanmıştır. Yazıcıların arıza vermesi büyük bir kaosa neden olmaktaydı. Özellikle teknik personelin yetersiz kaldığı durumlarda süreç yönetilemez bir hal almaktaydı. Bu nedenle şirket mevcut durumu iyileştirmeye ve merkezi bir baskı sistemi kurarak şirket kaynaklarını doğru kullanmaya karar vermiştir.

3.2.1.2. Şirketin ihtiyaçları

Şirketin, tüm sorunları tek seferde çözecek yeni bir tasarımının eksiksiz bir analizini hazırlaması gerekmektedir. Şirketin, mevcut karmaşık sistemi terk etmesi ve daha önce bahsedilen sorunları çözmesi için hedeflenen durumunu iyi belirlemesi gerekmektedir. Yeni baskı sisteminin tüm çalışanların baskı ihtiyacını karşılayacağı baskı sonrası malzemelerde gerekli tasarrufu sağlayarak bütün lokasyonları kapsaması amaçlanmaktaydı. Yeni sistem sadece yazılımla ilgili değil, aynı zamanda yeni tasarımı uygulamak için ihtiyaç duyulan yeni ekipmanların satın alınmasıyla da ilgili bir konudur. Bu kapsamda maliyet konusunda da şirketin bütçesi ile orantılı olmalıdır. Sistem hem çalışan hem de teknik destek personeli için kullanımı kolay olmalıdır. Teknik personel sistem üzerindeki çeşitli tablo ve grafikler sayesinde arızaları takip edebilmeli, yazıcıların toner ve kağıt durumlarını takip edebilmelidir. Aynı şekilde, sistemin bir yedek çözümü olmalı ve büyük problemler olması durumunda kolayca tamir edilebilir veya değiştirilebilir olmalıdır. Mevcut sistemde önemli bir sorun olan dokümanların fiziksel güvenliğinin de çözülmesi gerekmektedir. Çalışanlar kendi baskılarından sorumlu olmalı, çıktıların yetkisiz kişilerin ellerine geçmesi engellenmelidir. Kullanıcıların yanlış gönderdiği çıktılar engellenmeli ve yazıcılarda onay kuralı tanımlanmalıdır.

3.2.2. Yeni çözüm önerisi

Şirketin teknik personeli ile işbirliği içinde elde edilen gözlem ve verilere dayanarak, organizasyonun mevcut durumunun değerlendirilmiş ve gerekli bilgiler elde edilmiştir. Mevcut durumu ele almadan önce, asıl sorunun güvenilmez ve kullanışsız olan eski bir baskı yapısı olduğunu belirlemek mümkündür. Yazıcılar bir USB kablosuyla istemci bilgisayarlara doğrudan bağlı çalışmaktadır. Bu tür yazıcılar şirkette bulunan yazıcıların %20‘sini oluşturmaktadır. Bu tür yazıcılar, bazı gizli bilgilerin işlendiği ve işlemlerin ivedilikle yapılması ihtiyacının bulunduğu birimlerde kullanılmaktadır. Şirkette bu tarz ağa bağlı olmayan yazıcılardan 27'den fazla farklı tip ve marka yazıcı bulunmaktadır. Şirket birçok farklı türde tonere ve diğer sarf malzemelerine ihtiyaç duymaktadır. Şirkette bulunan küçük yazıcılarla ilgili diğer bir

yaygın sorun ise, kağıt sıkışması veya çalışanların yazıcılara bilinçsiz müdahalesidir. Bu durum yazdırma işleminin durmasına ve yazıcının uzun süre işlevsiz kalmasına neden olmaktadır. Kağıt sıkışırsa, yazıcıyı dikkatli bir şekilde açmalı ve kağıdı tek parça halinde çekilerek üretici tarafından belirtilen adımların tam olarak takip edilmesi gerekmektedir. Eğer yazıcının içindeki kağıt yırtılırsa, yazıcı yavaş yavaş açılmalı ve temizlenmelidir. Yazıcıda herhangi bir kağıt parçası veya kir kalırsa yazıcı çalışmaz ve uzun bir süre yenisiyle değiştirme ihtiyacı gerektirebilmektedir.

Şirkette kullanılan ikinci tip yazıcı ise ağ yazıcısıdır. Bu yazıcı, ağa bağlandığında kendisine bir IP adresi atanmakta ve bu ağa bağlı herkes tarafından kullanabilmektedir. Ancak bu durum, bütün şirket çalışanının yazıcıyı kullanabileceği anlamına gelmemektedir. Öncelikle teknik personelden birisinin yazıcıyı bilgisayara kurması ve bilgisayarın gerekli belgeleri yazıcıya gönderebilmesi için yazıcı sürücülerini bilgisayara yüklemesi gerekmektedir. Çalışanlar, böyle bir kurulum için gerekli bilgi ve idari haklara sahip değildir. Bir ağ yazıcısının avantajı, bir ağa bağlıyken herhangi bir yerde yazıcıdan çıktı alınabilmesidir. Şirkette bu yazıcı türleri genel olarak sadece bir katta bulunan yazıcı odalarında bulunmaktadır. Ağ yazıcıları çıktı alma, fotokopi, tarama, fax işlemleri gibi birçok işlevi yapabilmektedir. MFP'ların bir başka avantajı da taranan materyalleri doğrudan çalışanların e-posta adreslerine gönderme olanağıdır. Bir depolama aygıtı veya manuel ayar gerektirmez. Kullanıcı sadece bir adres veya listeden personel isimlerini seçerek taranan belgeleri doğrudan istediği kişiye e-posta gönderebilmektedir. Şirkette ağ yazıcılarının oranı %80 gibi büyük bir kısmını temsil etmektedir. Fakat yazıcıların ağa yerleşimi belgelerin fiziksel güvenliği sebebiyle sadece belli katlarda yoğunlaşmıştır. Bu durum çalışanlar için büyük bir sorun teşkil etmektedir. Çalışanlar basılı dokümanları alabilmek için binanın başka katlarına veya bölümlerine gitmeleri gerekmektedir.

Şirkette bulunan yerel ve ağ yazıcılarının türü ve sayısı Tablo 3.2.'de gösterilmektedir.

Tablo 3.2. Şirkette bulunan yazıcı türü, sayısı ve model dağılımı

Yazıcı Türü	Yazıcı Sayısı	Model Sayısı	Oran
Yerel Yazıcılar (USB)	40	27	%20
Ağ Yazıcılar (LAN)	152	7	%80
Toplam	192	34	

Tablo 3.2.'ye göre kurumun toplam 192 adet yazıcı bulunmaktadır. Bunlar 27 türde 40 yerel yazıcı ve yedi türde 152 ağ yazıcısından oluşmaktadır. Yerel ve ağ yazıcıları arasındaki oran 152/40'tır. Yazıcıların tür sayılarının fazla olması aynı sarf malzemelerini kullanmayan yazıcı türlerinin çok fazla olduğu anlamına gelmektedir. Her tür yazıcı için, diğer yazıcı türleriyle uyumlu olmayan sarf malzemeleri sağlanması gerekmektedir.

Bununla birlikte, yazıcıların temel sorunu kullanılma problemlerinden ziyade baskı sistemidir. Sistem, bir doküman alır almaz normal yazıcılarda yazdırmakta ve yazdırılan bu belgelerin şahsen alınması gerekmektedir. Gün boyunca, birkaç kişi aynı anda bir birinden bağımsız olarak belgelerini yazdırmakta ve çıktılar yazıcı tepsisinde sıralanmaktadır. Bazen iş yoğunluğu ve kullanıcı hatalarından dolayı çalışanlar yanlışlıkla başka birinin belgelerini alırsa, doküman sahibi basılı materyallerini boş yere saatlerce aramak zorunda kalabilmektedir. Materyalleri kaybetme, kişisel verileri tehlikeye atma, gizli bilgilerin yanlış ellere geçmesi gibi durumlar kurumsal güvenlik açısından büyük bir risk taşımaktadır. Bu durumda yazıcılarla ilgili birçok şikayet ve taleplerin gelmesine ve kurumsal bilgi güvenliğinin zedelenmesine neden olmaktadır [18].

3.2.3. Şirketin güçlü ve zayıf yönleri

Şirketin durumuyla ilgili mevcut bilgilere dayanarak, şirketin temel güçlü ve zayıf yönlerini tanımlamak mümkündür. Şirketin güçlü yönleri arasında öncelikle hazırda çalışan bir baskı sistemi yer almaktadır. Bu, sistem mükemmel olmasa bile işlevsel olduğu için mevcut baskı trafiğini yönettiği anlamına gelmektedir. Diğer bir güçlü yön ise şirketin kendi içinde yeterli donanıma sahip olmasıdır. Yeterli miktarda ve kalitede kurumun baskı işlerini yapabilen yazıcılar vardır. Son olarak nitelikli ve profesyonel destek masasının olması teknik yardım için şirket çalışanlarına önemli bir avantaj sağlamaktadır. Bu çalışanlar aynı zamanda bu konularda eğitim almış ve görevlerinde yetkin personelden oluşmaktadır. Teknik personeli yetkin olması yeni sistemin hayata geçirilmesi ve yönetilmesi konusunda da kritik öneme sahiptir.

Sistemin zayıf yönlerden ilki eski bir baskı sistemi olmasıdır. Sistem birbiriyle uyumlu olmayan, birden fazla bilgisayarla çalışmayı istenen düzeyde desteklemeyen, farklı tür yazıcılardan oluşan kaotik bir yapıya sahiptir. Zayıf yönlerinin ikincisi olarak, yazıcıların kullanıcılardan uzak bulunan bir baskı odasında bulunması olarak değerlendirilebilir. Merkezi ağ yazıcılarının çalışanlardan uzak olması, yazıcıların bulunmadığı kör nokta sayısının artmasına sebep olur. Bu nedenle, zaman içinde yazıcı bulunmayan yada yazıcılara uzak olan birimler kullanmak için küçük yazıcılara ihtiyaç duymaktadır. Bu problemi çözmek için ise bakımı pahalı, kontrolü zor olan ucuz yazıcıların satın alınması yoluna başvurulmaktadır. Bu tür yazıcıların bakımı yeni büyük ağ yazıcılarıyla karşılaştırıldığında, birkaç kat daha pahalıdır. Birçok küçük ucuz yazıcı, yalnızca sarf malzemelerini satmak için piyasaya çıkmaktadır. Bu yazıcılar maliyet ve güvenlik açısında oldukça zararlıdır.

Sistemin en ciddi sorunu, bilgi sızıntısına neden olabilecek veya kurumsal verileri ihlal edebilecek ağ yazıcılarını güvenli bir şekilde kullanmamaktır. Basılı materyalin başka bir kişi tarafından çalınmasını önlemek ağ yazıcısının güvenliğini sağlamadan mümkün değildir. Bunun için aynı anda birden fazla çalışanın çıktı almasının engellenmesi ve çıktıların kontrollü alınmasına ihtiyaç duyulmaktadır. Daha önce bahsedilen bir diğer dezavantaj, baskı hareketlerini izlemedir. Yazıcılardan alınan baskı sayısı, sarf malzemelerinin takibi, en çok çıktı alan personel ve yazıcıların belirlenmesi gibi konuların sağlıklı bir sistem izlenmesi ile tespit edilebilir. Bu veriler çalışanları ve sistemi denetlememizi ve gerekli işlemleri yapmamızı sağlamaktadır. Örneğin, bir çalışanın mesai saatleri dışında çok fazla belge ve doküman baskısını aldığını gördünüz. Çalışan kişiyi belirleyip gerekli işlemleri başlatmak zor olmayacaktır. Benzer şekilde sarf malzemesi biten bir yazıcının alarm vermesi, yazıcıyı zamanında iyileştirme konusunda size avantaj sağlayacaktır. Son zayıf yön ise çalışanın değişime olan korkusudur, bu her yeni sistem için doğal olarak meydana gelen bir endişedir. Çeşitli kurs ve eğitimlerle zaman içinde bu olgunun pozitif şekilde değişeceği düşünülmektedir.

Tablo 3.3. Mevcut sistemin güçlü ve zayıf yönleri

Güçlü Yönleri	Zayıf Yönleri
Mevcut durumda çalışan bir baski sistemi	Kötü bir yazıcı düzeni
Yeterli sayıda teknik ekipmanın varlığı	Pahalı bakım ve malzemelerin varlığı
İyi bir baskı altyapısı	Yazıcı çeşit sayısının fazla olması
Yetkin teknik destek personeli	Makinelerin veri ihlallerine açık olması
	Materyallerin çalınma olasılığı
	Çalışanların değişime olan korkusu
	Makine ve çalışanların takip edilememesi

3.2.4. Talep edilen baskı hizmetleri

Talep edilen baskı hizmetlerini belirlemek için şirketin mevcut durumunu ve gereksinimlerini dikkate almak gerekir. Yeni baskı sistemi tasarımının, sistemle ilgili bir sorun ya da teknisyenin müdahalesi gerektiği durularda bir bildirim sistemi başta olmak üzere, kullanıcı dostu bir uygulama tasarlamak, kurumun bütün yerleşke ve birimlerinde baskı sistemlerini yönetmek için merkezi bir ağ baskı çözümü oluşturmaktır.

Çözüm, kurumda yazdırılan tüm işlerin merkezi olarak yönetilebileceği bir yazıcı sunucusunun kurulmasıyla oluşur. Sistemin çalışma mantığı, baskı işlerini sisteme tanımlamak ve çıktı alınacak dokümanları istenilen yere göndermektir. Ancak, güvenli baskı ortamını oluşturmak için sistem güvenli yazılımlarla korunacaktır. Yani çalışanların yazıcıları kullanabilmesi için sisteme tanımlı olmaları ve kimlik doğrulamaları gerekecektir. En yaygın kullanılan kimlik doğrulama yöntemleri PIN kodları veya akıllı kartlardır. Kullanıcı tanımlı olduğu yazıcıya işi gönderdikten sonra yazıcı üzerinde kimlik doğrulamasını yaparak işi yazıcı ekranında görebilecek istediği materyali seçerek yazdırabilecektir.

Uygulama ayarları kuruluşun gereksinimlerine göre yapılacaktır. Uygulama, baskı sisteme bağlı tüm yazıcılar için mevcut durumları ve kullanıcıların yazdırma işlerinin durumu hakkında ayrıntılı raporu içerecektir. Kullanıcılar, Active Directory ile senkronizasyon yoluyla sisteme eklenecektir, yani bir çalışan hesabı oluşturulduğunda

veya devre dışı bırakıldığında uygulama üzerinde otomatik olarak eklenecek veya çıkarılacaktır.

Kurulumun teknik personeli, oturum açmış kullanıcılar için güvenlik kurallarını belirleyebilecek ve bu kuralları yazıcılara ya da kullanıcılara tanımlayabilecektir. Uygulama ayrıca, kağıt sıkışması, cihaz hasarı/hatası veya sarf malzemelerinin mevcut uyarı seviyesi gibi cihazın durumu hakkında önceden belirlenmiş bir kişiyi (teknik destek) uyaran bir güç tüketimi bildirim sistemi içerecektir. Bu tür bildirimler doğrudan sorunu çözmekten sorumlu destek masası çalışanına gönderebilecektir. Çalışanların yazıcılarla ilgili destek masasına herhangi bir arıza talebi yazmalarına gerek kalmayacaktır. Bu sistem, yetkisiz personelin yazıcıyı onarmak için müdahale etmesinden kaynaklanan hasarları da önleyecektir.

Uygulama ayrıca filigran ve QR kod özelliklerine sahip olacak bu özellikler çıktı alınacak tüm dokümanlara basılacaktır. QR kod içerisinde filigran kodunu barındıracak ve filigran, kullanıcının çıktı aldığı bilgisayar adını, yazdırma işleminin yapıldığı tarihi, çıktı gönderen personelin kimlik bilgileri vb. verileri barındıracaktır.

Yeni sisteme geçerken, hangi yazıcıların yeni uygulamaya uygun olup olmadığını belirlemek gerekmektedir. Yeni sistemde yalnızca ağ erişimi, dokunmatik ekran, sayısal tuş takımı, akıllı kart okuyucu özelliklerine sahip yazıcılar hizmet verebilmektedirler. Sistemde bulunan bütün yazıcılar merkezi olarak yönetileceği için yerel USB yazıcıların sisteme uyumlu olmayacağını varsayabiliriz. Tablo 3.2.'de görüldüğü gibi elimizdeki yazıcıları %20'sini oluşturan yerel USB yazıcıların tamamı bu sisteme dahil edilememektedir. 192 adet MFP yazıcılarının ise tamamının sisteme dahil edilebilir özellikte olması kurum için önemli bir avantajdır.

3.2.5. Yeni baskı sistemine geçiş

Yeni bir yerleşim planı tasarlarken, şirket binasına ilişkin verileri kullanmak mümkündür. Bu bilgilere göre şirketin merkez yerleşkesi 10 katlı bir binada oluşmakta olup, her kat 50 metreyi geçmeyen A,B ve C olarak adlandırılan üç farklı koridordan

oluşmaktadır. Bazı katlarda koridorlar arası geçişe müsaade ederken bazı katlarda bu imkan bulunmamaktadır. İşlem yoğunluğuna göre değişmekle beraber genellikle her koridorda şirketin bir departmanı görev yapmaktadır. Örneğin üçüncü katın A koridorunun bulunduğu ofisler personel temin hizmetlerinde görevli iken, B koridorunda bulunan ofisler şirketin bilgi işlem hizmetlerini yürütmektedir. Yani yazıcı koridorun ortasına yerleştirilirse, her çalışanın ofisten maksimum 25 m uzaklıkta bir yazıcısı olacaktır ki bu kabul edilebilir bir durumdur. Merkez yerleşke için, eşit dağılımda her koridor için bir renkli bir renksiz yazıcı olmak üzere 60 cihaza ihtiyaç duyulduğu anlamına gelir. Bu durum şirketin diğer iki yerleşkesi için de değerlendirildiğinde A yerleşkesi için 40, B yerleşke için ise 50 adet MFP yazıcıya ihtiyaç duyulmaktadır. Önerilen donanım, PIN girişi ve kart okuyucu ile kullanımı kolay bir ekrana sahip klasik MFP bir yazıcıdır. Bu cihazların sarf malzemelerinin tedariki ve yönetimi oldukça kolaydır.

Merkezi baskı yönetim sisteminin en büyük avantajı, bütün yerleşkelerde bulunan yazıcıları tek merkezde yönetmesidir. Bu durum bir yazıcı arızası olduğunda yakınındaki başka bir yazıcıya giderek dokümanı orda yazdırma imkanı sunmaktadır. Bu özellik çalışanların iş hızını ve performansını olumlu yönde etkilemektedir.

Kurumda bulunan 40 adet yerel USB yazıcılarının doğrudan çalışanların erişiminin olmadığı daha büyük kapalı ofislerde kullanılması daha uygundur. Ancak çeşit sayısının fazla olması ve sarf malzemelerinin çeşitli olması maliyet bakımında yüksek olduğu için zamanla elden çıkarılması tavsiye edilmektedir. Mevcutta bulunan 152 adet çok işlevli ağ yazıcısının ise planlanan durumda kurumun ihtiyaçlarını karşılayacağı değerlendirilmektedir.

Bu kapsamda üç yerleşkede yazıcıların yerleşimi, bina genelinde güvence altına alınmıştır. Her koridorda, yeni baskı uygulamasının bulunduğu MFP'lardan iki cihaz bulunmaktadır. Yazıcıların herhangi bir ofise uzaklığı maksimum 25 m olarak tasarlanmıştır. Çalışanlar sisteme kayıt olduktan sonra, kurum kimliği veya kullanıcı adı ve parolasıyla yazıcıya giriş yapabilmektedir. Belgeleri yazıcı sunucusuna gönderdiği için yazıcı menüsünde birkaç seçenek görecektir. Yazdırılan tüm işler

menüde sıralanır. Personel, materyalleri yazdırması gerektiğine karar verdikten sonra, bireysel belgelerinin çıktısını alabilecektir. Avantajı, yazıcının belgeleri tanımlanana kadar yazdırmaması ve başka bir çalışanın basılı materyalleri ve başka bir kişi tarafından çıkarılan materyallerle karıştırılmamasıdır. Belge yazdırıldıktan sonra çalışanın başka bir dokümanı yazdırmaya devam etme ya da sistemden çıkış yapma seçeneği vardır. Makine arızalanırsa, personel çıktılarını başka bir yazıcıya gönderilebilir ve orada yazdırmayı bitirebilir. Arıza veya başka bir kusur olması durumunda, sistem teknisyene hatanın türünü bildirir.

Yeni bir baskı çözümünün benimsenmesiyle kurumun tamamını kapsayacak şekilde yazıcılar orantılı olarak dağıtılmaktadır. Her koridorda bir renkli biri renksiz olmak üzere iki MFP yerleştirilmiştir. Yazıcının teknik açıdan başka bir kurulumu veya konfigürasyonu gerekli olmayacaktır. Yeni sistemin yapılandırma ayarları ve güvenlik kuralları tanımlandıktan sonra çalışanlar tamamen güvenli bir şekilde çıktı alabilecekledir. Kullanılmış eski yerel yazıcıların kademeli olarak azaltılması ve tek bir yazıcı türüne odaklanmasının ardından, sarf malzemesi türlerinin sayısını da azalması sağlanmış olacaktır. Sarf malzemesi, küçük yerel yazıcılar için toner kartuşlarının planlanması ve sipariş edilmesindeki sorunları giderilmiş olacaktır. Yeni baskı çözümü yalnızca izleme yaparak yazıcı hatasını erkenden tespit etmekle kalmamakta, aynı zamanda gerekli verileri toplayarak belirli bir çalışan başına yazdırılan sayfa sayısı hakkında rapor oluşturmaktadır. Bu özellik sayesinde personel denetlenebilir ve iş dışında alınan çıktı işlerini minimum seviyeye düşürmektedir. Ayrıca, yazıcıları tek bir konuma bağlı olmayacak şekilde yeni sistemle birleştirecektir. Çalışanlar, binadaki herhangi bir yazıcıda konumundan bağımsız olarak yazdırabilir. En önemli özelliklerinden bir tanesi ise yeni baskı çözümü diğer sistemlerden veya tedarikçi desteğinden bağımsızlıktır. Uygulama tamamlandıktan sonra kurum sistemi kendi imkanlarıyla yönetebilecektir.

Yeni sistem uygulanırken birçok tehdit ortaya çıkmaktadır. Bunların en önemlisi ve zor olanı çalışanlardan gelen tepkilerdir. Bu tarz değişim süreçleri bazı çalışanlar tarafından kişisel yenilenme, gelişim, ilerleme fırsatı olarak algılanırken, bazı çalışanlar bu durumu bir belirsizlik, çatışma, kurumsal ve kişisel anlamda bir tahmin

edilemezlik, tehdit kaynağı, kendi statü ve çıkarları için bir tehdit olarak algılamaktadırlar. Ancak değişime direnmeyen ancak değişimin tanıtım ve uygulama biçimine, eşitsizliklere, tehdit ve benzeri makul sorunlara direnen kişiler dikkate alınmalı ortaya atılan sorunlar titizlikle analiz edilmelidir. Çalışanların bu yeni ortama adapte olmak için daha fazla bilgi ve eğitim talep etmeleri makul bir beklentidir. Çalışanları değişimin nedeni ve önemi hakkında bilgi veren etkili bir iletişim stratejisi ve eğitim faaliyetleri değişime karşı olmayan çalışanlar arasında direncin düzeyini kesinlikle azaltacaktır. Bu durumun değişimi hedefleyen her kurum için geçerli olan bir yöntemdir. Özellikle, değişim hakkında zamanlı ve yeterli bilgi verildiği ve değişimin nedenlerinin uygulanan iletişim stratejileri ile net şekilde ortaya konduğu durumlarda değişimin kabul edilmesi, kabul hızı ve oranının artması yüksek olasılıktır [19]. Yeni bir sistem çalışanların sisteme yabancı olmasından dolayı çeşitli tepkilere yol açabilir. Hatta bazı kullanıcılar eski sistemin daha iyi olduğunu iddia edebilirler. Ancak, bu tür tehditler, iyi bir planlama ve titizlik ile en aza indirilebilir.

3.3. Şirkette Kullanılan Güvenli Baskı Çözümü - SecuriPrint

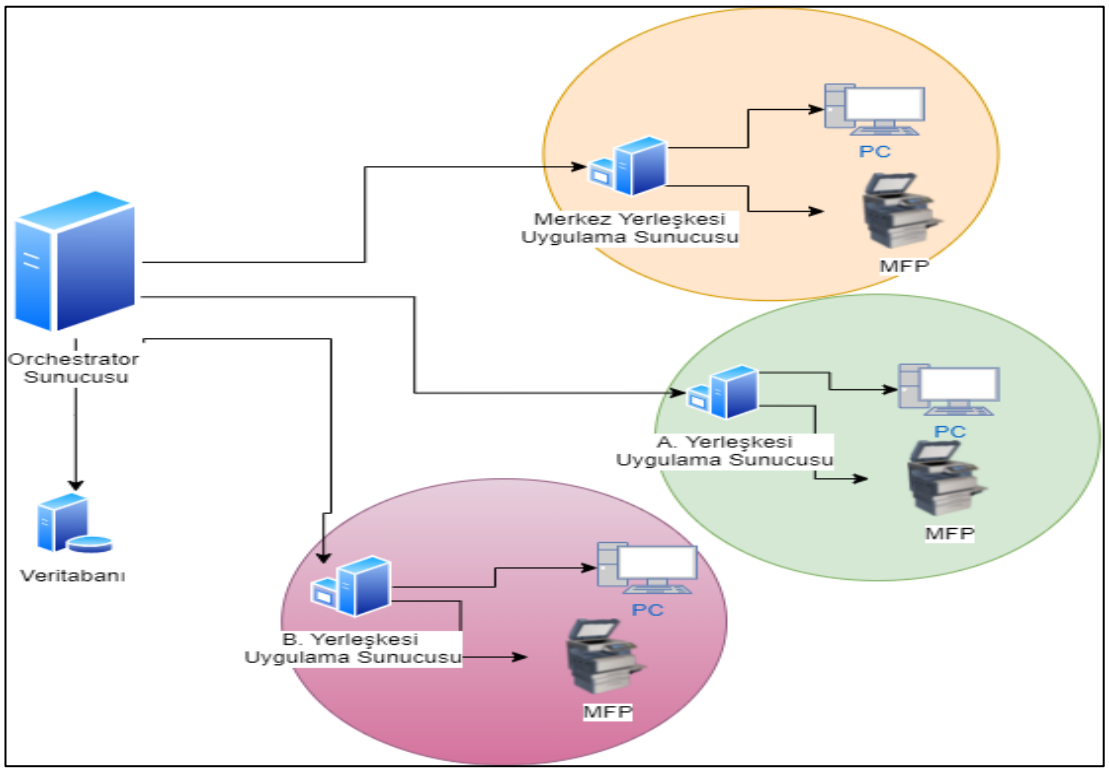
Yeni baskı sistemini belirlemek ve şirket ihtiyaçlarını karışılmak maksadıyla baskı hizmeti sağlayan beş firma ile görüşülmüş ve yazılımlar ayrı ayrı analiz edilmiştir. Yapılan değerlendirmeler neticesinde kurum ihtiyaçlarına en fazla cevap veren yönetimi ve kullanımı kolay kullanıcı dostu Entera A.Ş firması tarafından sağlanan SecuriPrint yazılımı tercih edilmiştir.

SecuriPrint dağıtık yapıdaki kurumsal altyapılar üzerinde devam etmekte olan baskı işlemlerinin güvenliği, takibi tanımlanması, raporlanması ve merkezi olarak yönetilmesini sağlayan bir güvenlik çözümüdür. Bilgisayar ve yazıcı üzerinde kimlik doğrulama mekanizması ile dokümanların sadece yazdıran kişi yetkilendirilen kişi tarafından alınması sağlanır. Yazdırılan ve dokümanlar üzerinde kullanıcı veya sistem bazında özelleştirilmiş filigran ve QR kod işleyerek bir takım bilgileri şifreli olarak verilmesi ve bu bilgiler sayesinde dokümanların izlenmesi ve raporlanması sağlanmaktadır. Kullanıcı ve grup bazlı kullanım kotası belirlenmesi, baskı alınmayan

dokümanların gün sonunda silinmesi ve yanlışlıkla gönderilen belgelerin çıktı alınmaması gibi özellikleri sayesinde maliyet yönetimi rahatlıkla yapılabilmektedir.

3.4. Sunucu Mimarisi

SecuriPrint, dağıtık yapıdaki kurumsal ağlar üzerinde yer alan kullanıcıların bilgisayarlarına kurulu bileşenler ve bu kullanıcıların bağlı bulundukları uygulama sunucuları üzerinde çalışmaktadır. Sunucular üzerinde tanımlı yazıcılar aracılığıyla yürütülen yazdırma işlemlerinde çok sayıda yerel ve ağ yazıcıları bir arada kullanılabilmektedir. Performans, yedeklilik ve coğrafi seviyede dağıtık yapıları desteklemek amacıyla uygulama sunucuları yatayda ölçeklenebilir şekilde tasarlanmıştır.



Şekil 3.1. Dağıtık yapılarda SecuriPrint sunucu mimarisi

Orchestrator sunucusu, mimaride bulunan SecuriPrint uygulama sunucularına tanımlanan ilgili portlar üzerinde erişim sağlamaktadır. Bu erişim ile uygulama sunucusu üzerindeki log kayıtlarına ve raporlara erişim sağlamakla birlikte ihtiyaç

olması durumunda lisans gönderimi yapmaktadır. Orchestrator sunucusu üzerindeki loglar ve kayıtlar MSSQL merkezi veritabanı üzerinde tutulmaktadır.

3.4.1. Sunucu bileşenleri

Temel sunucu bileşenleri her kurulum için aynı olmamakla birlikte aşağıdaki bileşenlere bağlıdır.

3.4.1.1. Core sunucusu

Temel uygulama sunucusudur. Sunucu mimarisi içerisinde tüm yapılandırma ve kayıtların depolandığı sunucudur. Tüm kullanıcıları ve yazıcıları yönetmekten sorumludur. Sisteme ekli bütün yazıcıların ağ ayarlarının, kullanıcı bilgilerinin departman, işlem, detaylı raporlama, kullanıcı yetkileri, politika ayarları bu sunucuda tanımlanır ve saklanır [20]. Karar mekanizmalarının oluştuğu sunucu mimarisidir.

3.4.1.2. Application programming interface (API) sunucusu

Uygulama Programlama Ara-yüzü anlamına gelen Application Programming Interface (API), yazıcı ve İstemci bilgisayarların iletişim sağladığı temel noktadır. Agent ve yazıcının sunucu ile iletişimini sağlamakla birlikte bu şekilde tüm bağımlılıklardan kendilerini arındırarak geliştiricilerin amaçları doğrultusunda son kullanıcılara hizmet vermekte olan uygulama programlama ara-yüzüdür. HTTP protokolü üzerinden kullanıcı isteği doğrultusunda veritabanında veri oluşturma, silme, güncelleme, getirme işlemlerini yapabilme veri alışverişinde bulunabilme imkanı da sağlamaktadır [21].

3.4.1.3. Agent

İstemci bilgisayarı üzerine kurulan bilgisayarın sunucu ile haberleşmesini sağlayan ajan uygulamasıdır. Bu uygulama kurulumundan sonra İstemci bilgisayar üzerindeki yazdırma fonksiyonları kontrol altına alınmaktadır.

3.4.1.4. Orchestrator sunucusu

Merkezi raporlama ve logların depolandığı sunucu bileşenidir. Birden çok core bileşeninin olduğu yapılarda merkezi loglama ve rapor çözümü için geliştirilen bileşendir. Ayrıca lisans yönetimi de bu sunucu üzerinde merkezi olarak yapılmaktadır.

3.4.1.5. Yazıcı uygulamaları

Kullanıcıların yazıcı üzerinde kimlik doğrulama yapmasını ve sistemde bekletilen işlerini yönetmesini sağlayan yazıcı üzerinde çalışan uygulamalardır.

3.4.1.6. Veritabanı sunucusu

Logların ve kayıtların tutulduğu merkezi veritabanı sistemidir. SecuriPrint yazılımı birçok veritabanı uygulamasını desteklemekle birlikte çalışmamızda tercihen MSSQL veri tabanı uygulamasını kullanılmıştır.

3.4.1.7. Kuyruklama mekanizması

Kullanıcılar tarafında yapılan tüm işlemler bu kuyruklama mekanizmasında sıralanmaktadır. Dolayısıyla aynı anda yapılan birçok işlem varsa bu işlerin bir dar boğaz oluşturulması engellenmektedir.

3.4.1.8. Çok işlevli yazıcı (Multifunction Printer- MFP)

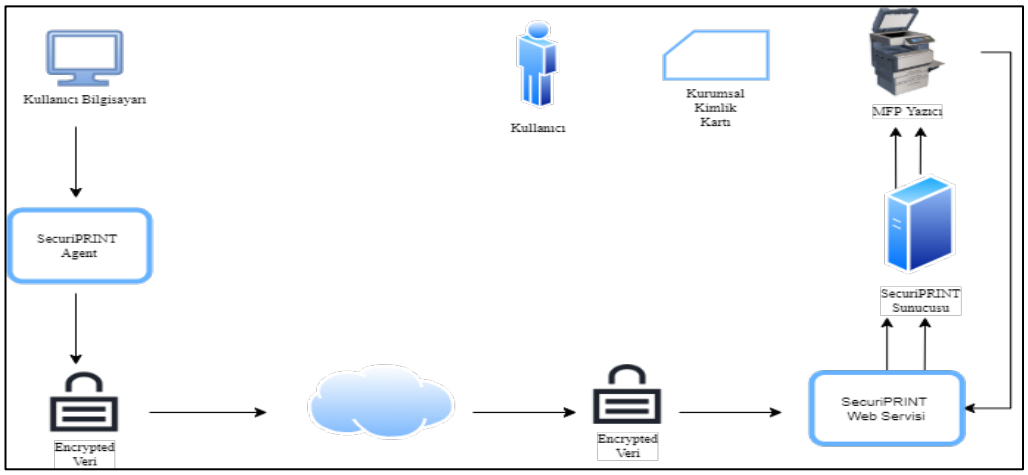
Çok işlevli bir yazdırma aygıtı, yazdırma amacıyla kullanılan bir donanım aygıtıdır. Dijital ortamdaki belgeleri kağıt üzerine baskı ile aktarmasını sağlayan asıl donanımdır. Tüm küçük, orta veya kurumsal kuruluşların çalışanları, kuruluşun günlük operasyonel işlevleri için yazıcılar, fotokopi makineleri, tarayıcılar, fakslar ve MFP'lerden yararlanır. MFP'lar yerel veya ağ bağlantılı olabilir. Ancak bu tezin amacı doğrultusunda, ağa bağlı MFP üzerinde çalışmalar incelenecektir. MFP'lerin işlevli

yazdırma aygıtı denmesinin sebebi tarama, e-postalar, fotokopi özellikleri yanı sıra renkli ve siyah-beyaz görüntüleri basabilme özelliğine sahip olmasıdır [22].

3.4.1.9. Yazıcı sürücüsü

Uygulamalar tarafından oluşturulan yazdırma işlerini belirli bir yazdırma aygıtı için uygun bir komut dizisine dönüştüren bir yazılımdır. Yazıcı sürücüsü, yazıcıya gelen işleri, yazıcı tarafından anlaşılabilecek şekilde bir formata dönüştürülmektedir [22]. Ayrıca yazıcının birçok özelliğini kontrol eder. Örneğin; kenar boşluklarını belirler, sayfalamayı kontrol eder ve yazdırma işlerinin sağlıklı tamamlanması için diğer görevleri üstlenir. Her yazıcı sürücüleri kendine özgü bir marka model yazıcıya ve işletim sistemine özgüdür. Bu nedenle sorunları önlemek için doğru ve güncel sürücüyü kullanmak önemlidir.

3.4.2. SecuriPrint uygulamasının iş akışı



Şekil 3.2. SecuriPrint uygulaması iş akış süreci

Kullanıcı bilgisayar üzerinde hazırladığı bir dokümanı öncelikle istemci bilgisayar üzerinde kurulu bulunan SecuriPrint Agent vasıtasıyla şifrelenmiş bir şekilde kurum ağından geçerek API sunucusuna göndermektdir. API sunucusu gelen işleri SecuriPrint core sunucusuna aktarır. Burada gelen dokümanlar işlenir yani işi gönderen kullanıcının sisteme tanımlı olup olmadığı, hangi kurallardan etkilendiği teyit edilir ve doküman burada kuyruklanır.

Kullanıcı yazıcıdan çıktı almak istediğinde kullanıcı adı ve parolasıyla ya da daha önce tanımlı kurumsal kartını kart okuyucusuna okuttuktan sonra yazıcı ekranına kullanıcı bilgisayarında gelen işler gözükmektedir. Yazdırılmak istenen işler seçilip yazdır seçeneği tıklandıktan sonra yazıcı API sunucusuna bilgilerini (IP adresi, seri numarası vb.) göndererek iletişime geçer. API sunucusu, core sunucusu ile iletişime geçerek yazdırma işlemini gerçekleştir ve kullanıcı dokümanları yazıcı tepsisinden güvenli ve hızlı bir şekilde erişim sağlayabilmektedir. Dokümanlar yazıcı tepsisine düşene kadar sürecin her aşamasında şifrelenmiş bir şekilde saklanmaktadır.

BÖLÜM 4. UYGULAMA

Uygulama süreci içinde öncelikle hem şirket hem de firma için gerekli olan isterlerin hazırlanmasına odaklanmak gerekir. Uygulama bütün teknik isterlerin hazırlanacağı kurulum öncesi bir ön hazırlık ile başlamaktadır. Uygulamanın hazırlanmasından sonra, sistemin yapılandırılması tamamlanarak tüm ince ayarları yapılacaktır. Kurulum tamamlandıktan sonra, uygulamanın bütün özelliklerini test etmek için bir test çalışması yapılarak sitemin hata ve kusurları tespit edilebilecektir. Hatalar giderildikten sonra mevcut sistem ve son durum karşılaştırılarak kurumun ihtiyaçlarının karşılanıp karşılanmadığı tespit etmek mümkün olacaktır.

4.1. Sistem Gereksinimleri

4.1.1. Yazılım gereksinimleri

SecuriPrint yazılımı Windows Server 2008 R2 ve üstü işletim sitemlerini desteklemektedir. Projede Core ve Orchestrator sunucularına, Windows Server 2019 işletim sistemi kurulmuştur.

4.1.1.1. Microsoft internet information services (IIS)

IIS (Internet Information Services), web sayfalarının yayınlanmasını ve web uygulamalarının çalışmasını sağlayan, istemcilerden HTTP ve FTP üzerinden gelen talepleri Microsoft Windows sunucu tabanlı işletim sistemlerinde karşılayan birimdir. Genellikle Web tabanlı uygulamaları dış dünyaya yayınlamak için kullanılmaktadır [23]. Sunucuya HTTP protokolü üzerinden istek geldiği zaman, sunucu üzerinde istemciyi ilk olarak IIS karşılamaktadır. API, IIS üzerinden hizmet vermektedir.

4.1.1.2. Net framework 4.6.2

.NET, Microsoft tarafından yazılım geliştiricilere kolaylık sağlamak için kurulan programlama sistemidir. Bu sisteme uygun birçok işletim sistemine uyumlu yazılım geliştirilmektedir. .NET Framework ise geliştiriciler tarafından hazırlanan yazılımların windows işletim sistemine uyumlu çalışmasını sağlayan bir .NET türüdür.

4.1.1.3. ErLang OTP 19+

1986 yılında Erlang Ericsson firması tarafından 1986'da Joe Armstrong, Robert Virding ve Mike Williams önderliğinde geliştirilen genel amaçlı bir programlama dilidir. ErLANG uygulaması, RabbitMQ uygulamasının ön gereksinimidir.

4.1.1.4. Rabbit MQ

Rabbit MQ bir kuyruklama mekanizmasıdır. Amacı gelen doküman isteklerini bir sıraya koyduktan sonra başka bir kaynağa sırası geldiğinde iletmektir. Gönderilen istekler alıcıaya ulaştırılmadan önce bir sıraya konur. Gelen yoğunluğa göre veya alıcıya erişilemediği durumlarda, gelen tüm mesajlar kuyrukta yani diskte saklanır. Eğer bu süreç uzun sürer ise disk şişebilir.

4.1.1.5. Donanım gereksinimleri

Donanım gereksinimleri sistem yapılarına göre değişmektedir. Ancak SecuriPrint sunucu kurulumu için Entera A.Ş. tarafında kullanıcı ve uygulamaya göre tavsiye edilen gereksinimler Tablo 4.1.'de verilmiştir.

Tablo 4.1. SecuriPrint donanım gereksinimleri

KULLANICI SAYISI		1000 Kullanıcı	10000 Kullanıcı	50000 Kullanıcı
İŞLEMCİ		Tek çekirdekli minimum işlemci	Çift çekirdekli minimum işlemci	Dört çekirdekli minimum işlemci
RAM		4 GB	8 GB	16 GB
DİSK ALANI	PROGRAM Dosyaları	200 MB	200 MB	200 MB
	Uygulama Verileri	5 GB	50 GB	100 GB
	Veritabanı Dosyaları	10 GB	200 GB	400 GB

Tablo 4.1.'e göre şirketin üç yerleşkesinde ortalama 2500 çalışan olduğu için çift çekirdekli 8 GB RAM ve yeterli büyüklükte disk alanına sahip bir sanal sunucuyu şirketin Hyper-V sanallaştırma platformuna kurulması ihtiyaçlarımız için yeterli olacağı değerlendirilmiştir.

4.1.2. Veri tabanı gereksinimleri

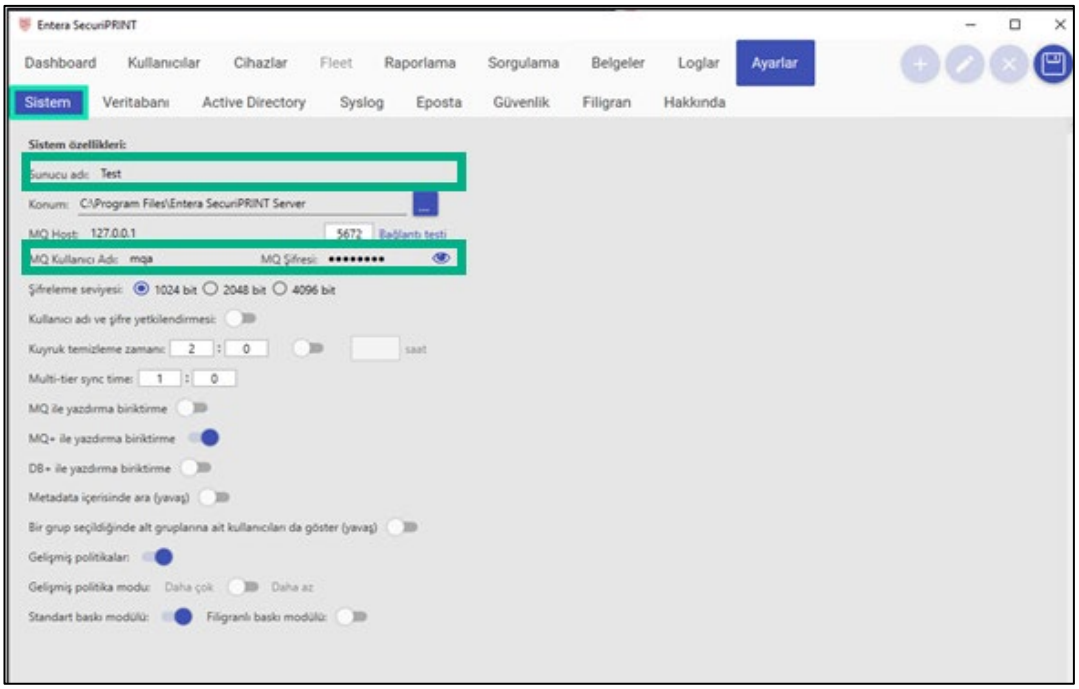
Sistem PostgreSQL, MySQL, Oracle vb. birçok veri tabanı uygulaması tarafından desteklenmektedir. Topolojimize uygun olması sebebiyle projemizde MS SQL veritabanı uygulaması kullanılmaktadır.

4.2. Sistemin Yapılandırılması

Sistem tarafından ihtiyaç duyulan donanımlarda sanal sunucular kurulduktan sonra ilgili yazılımlar yüklenip kurulum işlemleri tamamlanmıştır. Bundan sonra yönetici hesabıyla uygulamanın ara-yüzüne erişim sağlanabilmektedir. Test işlemlerine başlamadan önce sistemin veritabanı ve Aktif Directory senkronizasyonu gibi sistemin diğer önemli yapılandırma ayarlarının yapılması gerekmektedir.

4.2.1. Temel sistem ayarları

Masaüstünde bulunan SecuriPrint uygulamasını yönetici olarak çalıştırıldığında aşağıdaki ekran açılacaktır. Ekranda temel ayarlar yapılandırılmadığı için menülerden bazıları pasif olarak gelecektir. İlk adım ayarlar sekmesinde bulunan sistem seçeneği seçilir ve gerekli konfigürasyon ayarları yapılır.



Şekil 4.1. SecuriPrint temel sistem ayarları menüsü

Öncelikle sistem özellikleri bulunan kısma kurulumu yapılan sunucunun adı girilmelidir. Merkezi lisanslama kullanılması durumunda buradaki sunucu adı ve Orchestrator sunucusu üzerinde tanımlanan sunucu adı aynı olmalıdır. Uygulamanın kurulu olduğu dizin bilgisi konum alanına girilir ve MQ Host kısmına RabbitMQ uygulamasının üzerinde çalıştığı sunucu IP adresi tanımlanır. RabbitMQ uygulaması farklı bir sunucu üzerine kurulması varsayılan değer yerine kurulum yapılan sunucun IP adresi girilmelidir. MQ kullanıcı adı, RabbitMQ yapılandırması adımında oluşturulan sistem kullanıcı adı, varsayılan kurulumda mqa olarak gelmektedir. MQ şifresi ise Rabbit MQ kurulumu sonrasında bat uzantılı dosya ile verilen şifre girilecektir. Kullanıcı adı ve şifresi yetkilendirmesi ayarının aktif durumda olması halinde İstemci bilgisayarında çıktı alma işlemi yapmadan önce kimlik doğrulaması zorunluluğu bulunmaktadır. Eğer ikinci bir kimlik doğrulaması seçeneği istenmiyor ise bu seçenek devre dışı bırakılabilir.

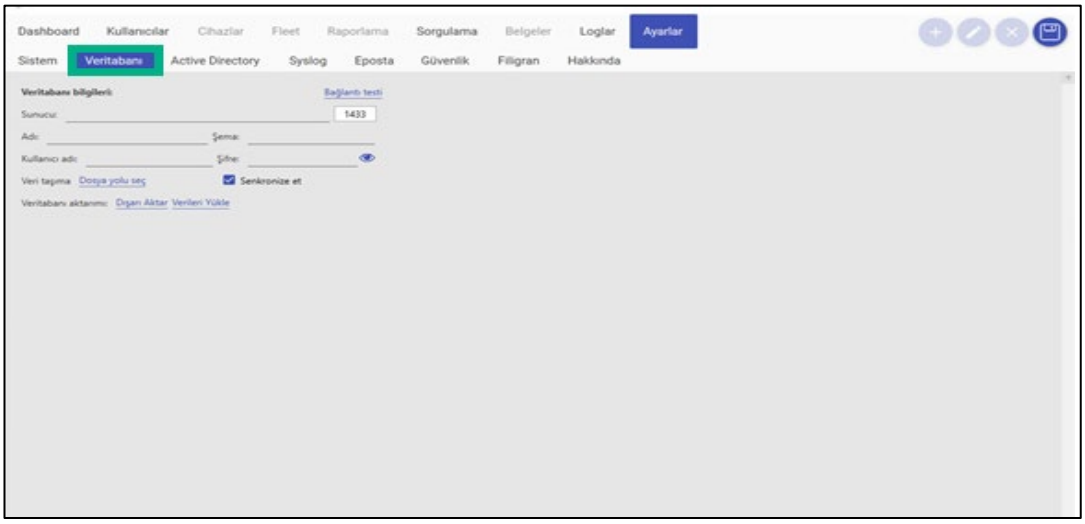
Kuyruk temizleme zamanı ayarlandığında kullanıcıların gönderdikleri işlerin merkezi olarak belirli bir süre sonra silinmesini sağlayacaktır. Kullanıcıların gönderdikleri işler belirlenecek bir saatte veya her işin bir saklanma süresinden silinmesi sağlanabilir. MQ ve MQ+ ile yazdırma biriktirme ayarı kartlı sisteme gönderilen işlerin RabbitMQ

ve RabbitMQ+ sunucusu üzerine saklanmasını sağlamaktadır. DB+ ile yazdırma biriktirme ayarı ise kartlı sisteme gönderilen işlerin DB+ sunucusu üzerine saklanmasını sağlamaktadır.

Metadata içerisinde ara fonksiyonu kullanılmak istenirse Metadata içerisinde ara seçeneği aktif hale getirilmelidir. Bir grup seçildiğinde alt gruplarına ait kullanıcıları da göster seçeneği alt gruplar bir grup seçildiğinde görüntülenmek istenirse aktif hale getirilir. Gelişmiş politikalar, kullanıcı yetkilendirmesi sırasında gelişmiş politikalar kullanılmak istenmesi durumunda bu seçenek kullanılır. Gelişmiş politika modunun detaylandırma tercihine göre bu seçenek "daha çok" ya da "daha az" olarak seçilebilir. Standart baskı modülü seçeneği, filigransız baskı yapılması durumunda, filigranlı baskı modülü seçeneği ise filigranlı baskı yapılması tercih edilmesi durumunda aktif hale getirilir

4.2.2. Veri tabanı entegrasyonu

İkinci yapılması gereken ayar veritabanı entegrasyon yapılandırmalarıdır. Uygulama local, MSSQL ve Oracle veritabanlarını desteklemektedir. Kurum bu proje Mssql veritabanını tercih etmiştir. Bu kapsamda yapılandırma ayarlarını için aşağıdaki tabloda istenilen bilgiler girildikten sonra "Bağlantı testi" tıklanarak veri tabanı bağlantısı test edilir.



Şekil 4.2. SecuriPrint veritabanı entegrasyon menüsü

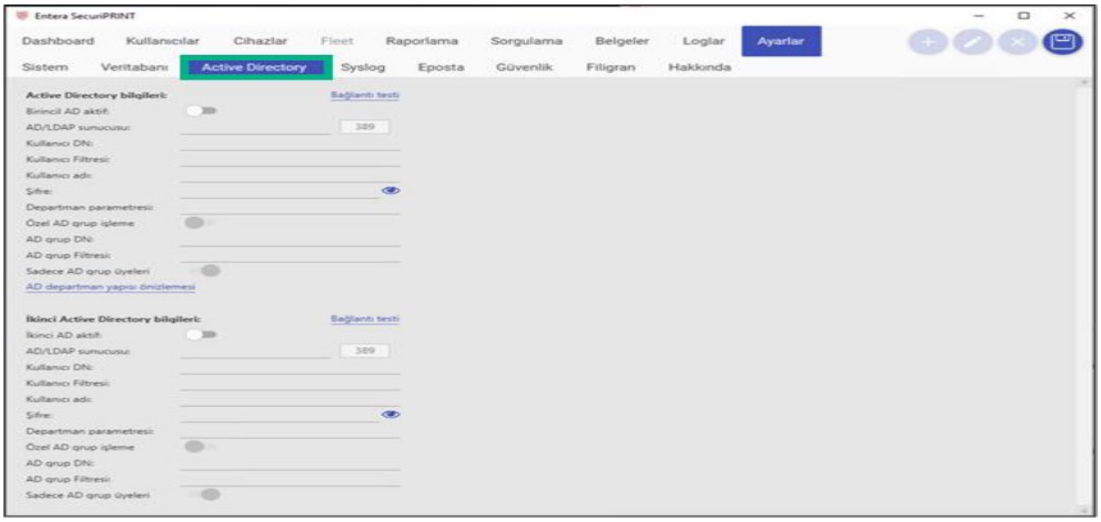
MSSQL veri tabanı ile ilişkilendirilecek sunucunun IP adresi ilgili alana girildikten sonra kurulumu yapılan MSSQL veri tabanı adı, şema biçimi, kullanıcı adı ve şifresi sırasıyla belirtilen alanlara girildikten sonra veri tabanından veri taşınmak isteniyorsa "Dosya yolu seç" tıklanarak taşınacak yol ve veritabani dışa aktarılmak isteniyorsa "Disa Aktar", dışarıdan içeri veri aktarılmak isteniyorsa "Verileri Yükle" seçenekleri seçilerek gerekli tanımlamalar yapılır.

4.2.3. Aktif directory entegrasyonu

Active Dizin, Microsoft ağlarında kullanılan dizin hizmetidir. Bu dizin hizmetinde veritabanı, kullanıcılar, bilgisayarlar, sunucular, yazıcılar gibi kuruluşun tüm bilgilerini saklar. Dizin üzerinde çeşitli yönetimsel kısıtlamalar oluşturulabilir ya da kullanıcıların çalışma ortamları ihtiyaçlar ve standartlar doğrultusunda şekillendirilebilir. Aktif Directory hizmeti üzerinde oluşturulacak hesaplar her kurumun organizasyon yapısına uygun bir şekilde kurulan servis aracılığı ile rahatlıkla oluşturulabilmektedir. Aktif Directory içindeki herbir nesnenin adı vardır. Bu ada Distinguished Name denir. Bu adlar nesnenin bulunduğu domain'i tanımlar.

Microsoft Aktif Directory yapısı üzerinde LDAP (Lightweight Directory Access Protocol – Basit Dizin Erişim Protokolü) protokolünün yaygın olarak kullanımı görülmektedir. LDAP, TCP/IP ağlarında çalışan dizin hizmetlerini sorgulamak ve değiştirmek için kullanılan bir uygulama protokolüdür. Kimlik doğrulama ve yetkilendirme işlemlerinin yönetimini merkezileştirmeye yardımcı olmaktadır. LDAP, veritabanı gibi verileri tablolarda değil bazı kurallar dahilinde hiyerarşik bir dizin yapısında depolanmaktadır [24].

SecuriPrint core uygulama sunucusu bütün kullanıcı bilgilerini Aktif Directory üzerinden almaktadır. Merkezi kimlik doğrulama için kurumda bulunan LDAP sunucu bilgileri aşağıdaki alana girilmelidir. Aktif olması istenen Aktif Directory (birincil ve ikincil) seçilmelidir.

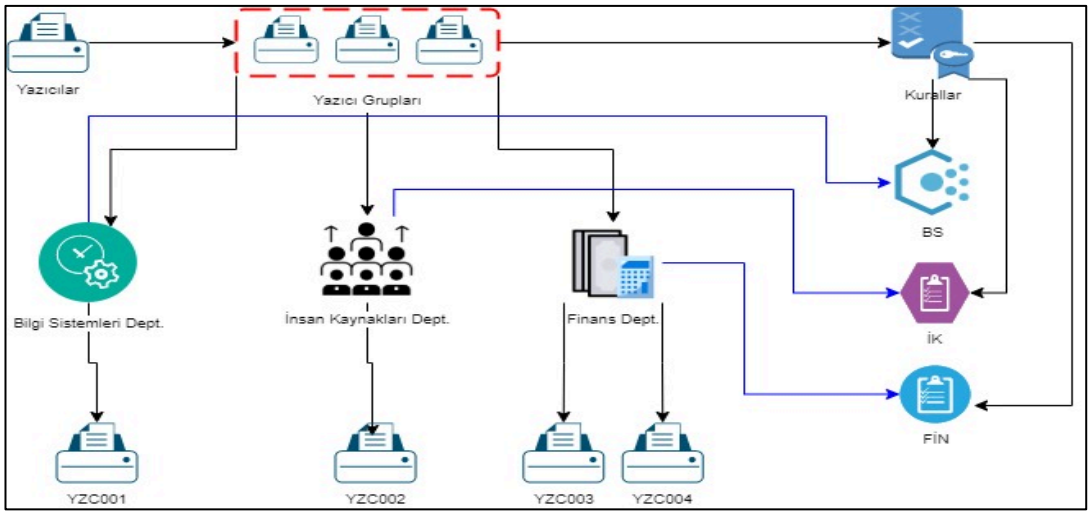


Şekil 4.3. SecuriPrint Aktif Directory entegrasyon menüsü

AD/LDAP sunucusu bölümüne Aktif Directory üzerinde bulunduğu sunucunun IP adresi girildikten sonra kullanıcı DN sekmesine kullanıcılar hangi yönetimsel birimden alınacaksa o yönetimsel birimin Domain distinguish name bilgisi yazılır. Aktif Directory için kullanılmak istenen kullanıcı filtreleri ilgili alana yazılır ve Aktif Directory'de bulunan standart yetkilere sahip hesabı servis kullanıcısının adı ve şifre bilgisi, Aktif Directory üzerinden kullanıcılar Departmana göre gruplandırmak isteniyorsa gerekli parametreler doldurulur. Seçilmek istenen Aktif Directory grubunun distinguish name bilgisi girilir. AD departman yapısı ön izlemesi yapılarak mevcut yapılandırmaların yapıldığı departman yapısının bir ön izlemesi görüntülenir.

4.3. SecuriPrint Uygulamasının Kullanımı

SecuriPirint uygulama yazılımında, bilmemiz gereken üç önemli kavram bulunmaktadır. Bunlar yazıcılar, yazıcı grupları, kurallar ve bunlar arasındaki ilişkidir. Onun için bu üç temel kavram üzerinde detaylı bir şekilde incelenecek ardında uygulamanın tüm adımları ayrı ayrı anlatılacaktır. Öncelikle yazıcıları eklemeden önce mutlaka bir isim standartlının oluşturulmas gerekmektedir. Belirlenen isim standartlarına uygun şekilde SecuriPrint Managmant uygulama ara-yüzüne eklenen yazıcılar departmanlarına göre yazıcı gruplarına ayrılır. Her yazıcı ilgili departman grubuna eklenir. Gerekli kurallar tanımlanarak ilgili yazıcıya sadece sahip olduğu departmanda çalışan kullanıcıların çıktı alması sağlanır.



Şekil 4.4. SecuriPrint uygulmasının çalışma prensibi

Örneğin, Şekil 4.4.'de görüldüğü gibi şirketimizde Bilgi Sistem (BS), İnsan Kaynakları (İK) ve Finans (FİN) departmanları bulunsun. Burada öncelikle her bir departman için yazıcı grupları oluşturmamız gerekmektedir. Bunlar Bilgi Sistem, İnsan Kaynakları ve Finans Dept. yazıcı grupları olsun. Daha sonra uygulamaya tanımladığımız yazıcıları ilgili departmanın yazıcı grubuna eklenmesi gerekmektedir. Amacımız her yazıcı sadece kendi departmanına hizmet vermesidir. Mesela, YZC001 sadece Bigi Sistemleri departmanına, YZC002 İnsan Kaynakları departmanına hizmet vermesini istiyoruz. Yazıcıları ilgili departmanın yazıcı grubuna dahil ettikten sonra YZC001 yazıcısının BS departmanına, YZC002 yazıcısının İK departmanına hizmet vereceğiyle ilgili ayrıntılar kurallar ile tanımlanmaktadır. Her departman için yazdırma detayları ile ilgili kurallar ve kuralın hangi departmanındaki yazıcı grubunu etkileyeceği belirlenir. Gerekli tanımlamalar yapıldıktan sonra şirketin yapısına göre ve talep edilen departmanlara göre kurallar ilgili departmanlara uygulanır. Şirkette her çalışan kendi departmanında tanımlanan kurala baskı hizmetlerini yürütmektedirler.

4.3.1. Dashboard

Uygulamanın kullanımı ile ilgili özet bilgileri barındırır. Günlük ve haftalık olmak üzere iki farklı zaman dilimine göre uygulamanın kullanım detaylarını özetler. En çok çıktı alan kullanıcı bilgileri, günlük yazdırılan çıktı işlem sayısı ve maliyet göstergesi bu ara-yüzde analiz edilmektedir.

4.3.2. Kullanıcılar

SecuriPrint uygulamasını kullanabilecek olan kullanıcılar burada listelenir. Temel yapılandırma ayarlarında "Active Directory" ayarlarının yapılandırılmış ise active directory senkronizasyonu beklenmeden aşağıdaki "AD kullanıcılarını ekle" butonuna tıklanarak kullanıcıların senkronizasyon sürecinin manuel olarak tetiklenmesi sağlanabilir.

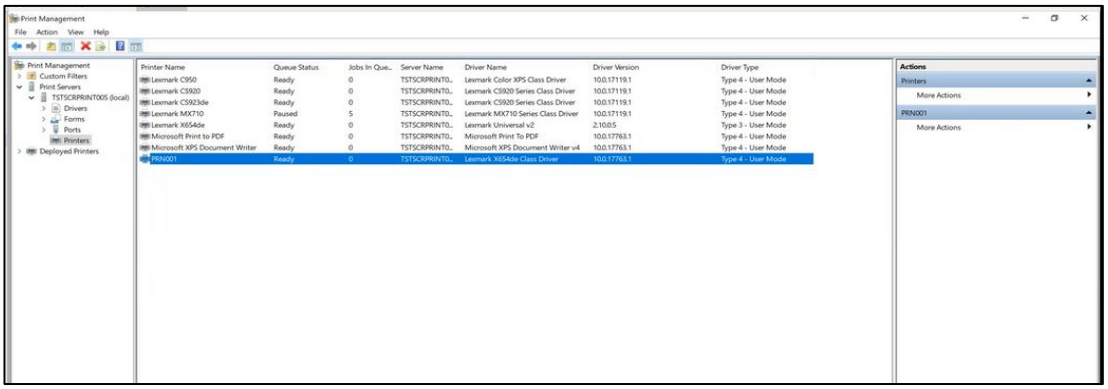
Şekil 4.5. SecuriPrint ara-yüzüne kullanıcı tanımlanması

Kullanıcılar bu ara-yüzde listelenir ve istenilen kullanıcı seçilip kullanıcıya istenilen kurallar ve kısıtlamalar uygulanabilmektedir.

4.3.3. Yazıcılar

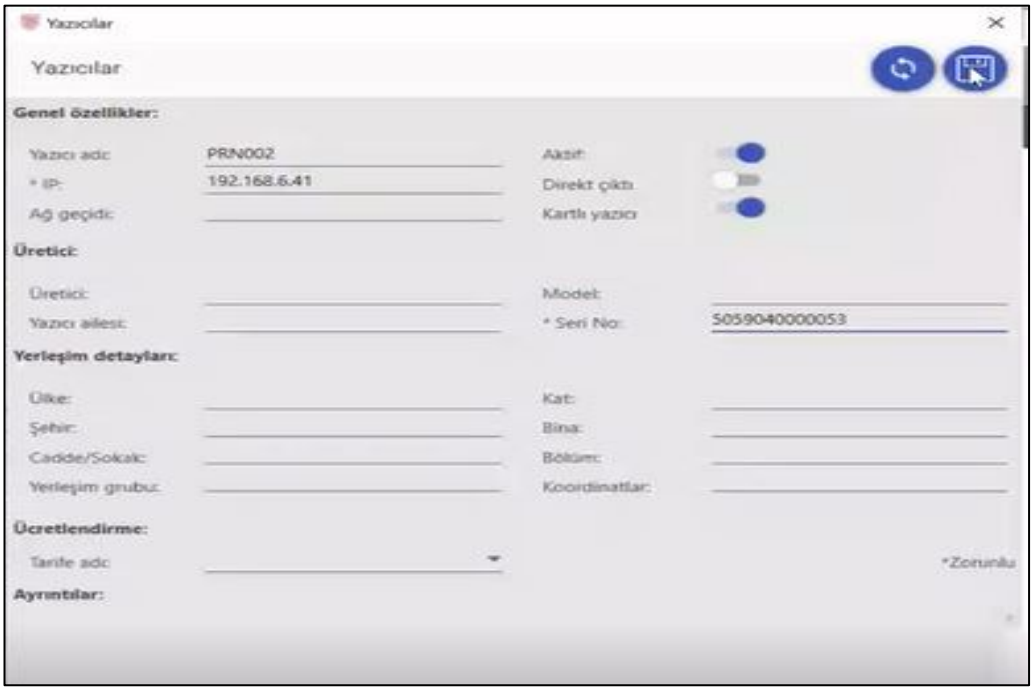
Yazıcılarla ilgili yapılması gereken ilk adım yazıcıların hangi isimle siteme ekleneceğine yönelik bir isim standartının belirlenmesi gereğidir. Bu hiyerarşik isim yapısı yapacağımız merkezi baskı yönetim siteminde yazıcıların kolay eklenmesine ve yönetilmesine olanak sağlayacaktır.

İkinci önemli adım ise kurulumu yapılacak yazıcıya windows driver kurulumunun yapılması gerekmektedir. Uygulama sunucusunun print management servisine, eklenecek yazıcının IP adresi ve belirlenen isim standartlarında uygun yazıcı isimi ile windows driver kurulumu yapılması gerekmektedir.



Şekil 4.6. Yazıcı sunucusuna windows driver yüklenmesi

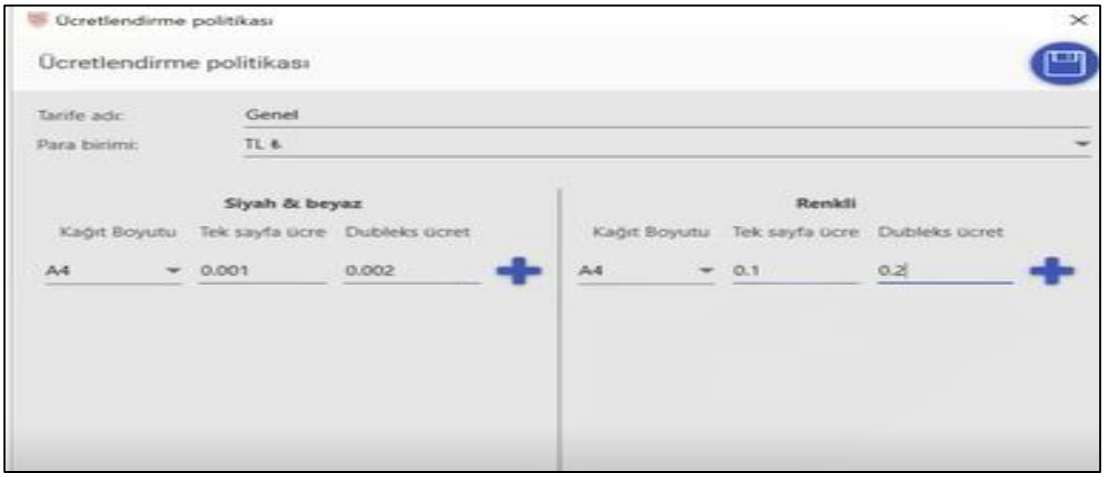
Üçüncü adımda SecuriPrint Management ara-yüzü açılır ve yazıcılar sekmesi seçilerek yazıcı ekleme işlemlerine başlanır. Bu adımda sunucu üzerinden eklenen sürücü adı ve uygulama üzerinden eklenen yazıcının adı aynı olmalıdır.



Şekil 4.7. Yazıcıların yönetim ara-yüzüne tanımlanması

Zorunlu alanlar olarak belirtilen yazıcı adı, ip adresi ve seçilmek istenen çıktı seçimi elle girilmektedir. Yazıcının seri numarası ve diğer bilgileri otomatik olarak gelmektedir. Yerleşim detaylarına yazıcının bulunduğu bina, kat vb. bilgileri tanımlandıktan sonra kullanmakta olduğunuz renkli ve siyah-beyaz yazıcıların

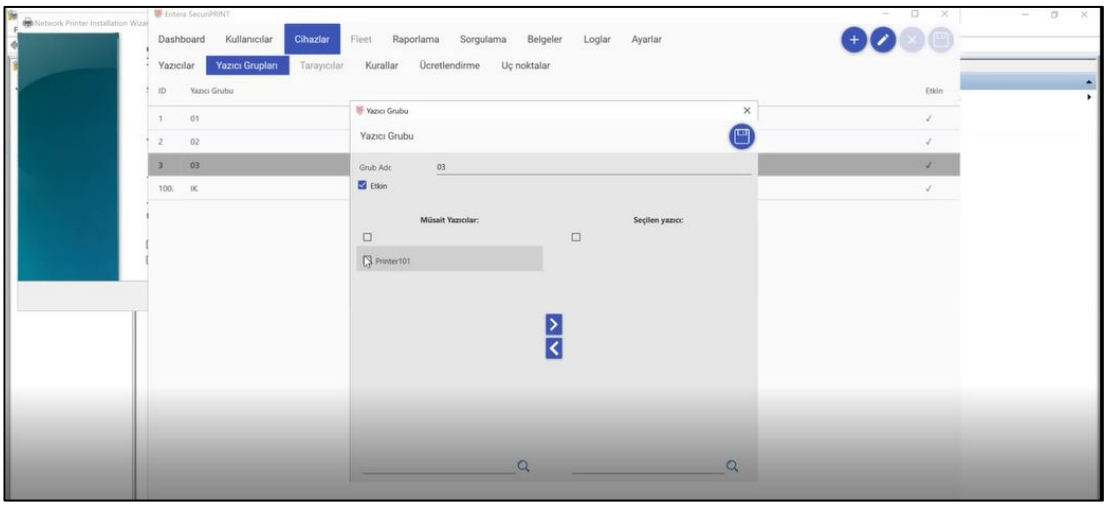
maliyetlerini ücretlendirme alanında oluşturabilirsiniz. Bu aşamada yapılan ücretlendirme politikaları ilgili cihazda güncellenmesi gerekmektedir.



Şekil 4.8. Ücretlenrme politikasının belirlenmesi

4.3.4. Yazıcı grupları

Yazıcılar yönetim ara-yüzüne tanımlandıktan sonra yapılması gereken ikinci adım yazıcı gruplarını oluşturmaktır. Yazıcı grupları kurumun farklı departman ve birimlere ait yazıcılarda sadece o yazıcıya tanımlı birimlerde çalışan kullanıcıların çıktı almasını sağlamaktadır. Bunun için kurumdaki her bir departman için yeni bir yazıcı grubunun oluşturulması gerekmektedir. Yazıcı grubu yönetici ara-yüzünde yazıcı grupları sekmesi üzerinde oluşturulmaktadır.

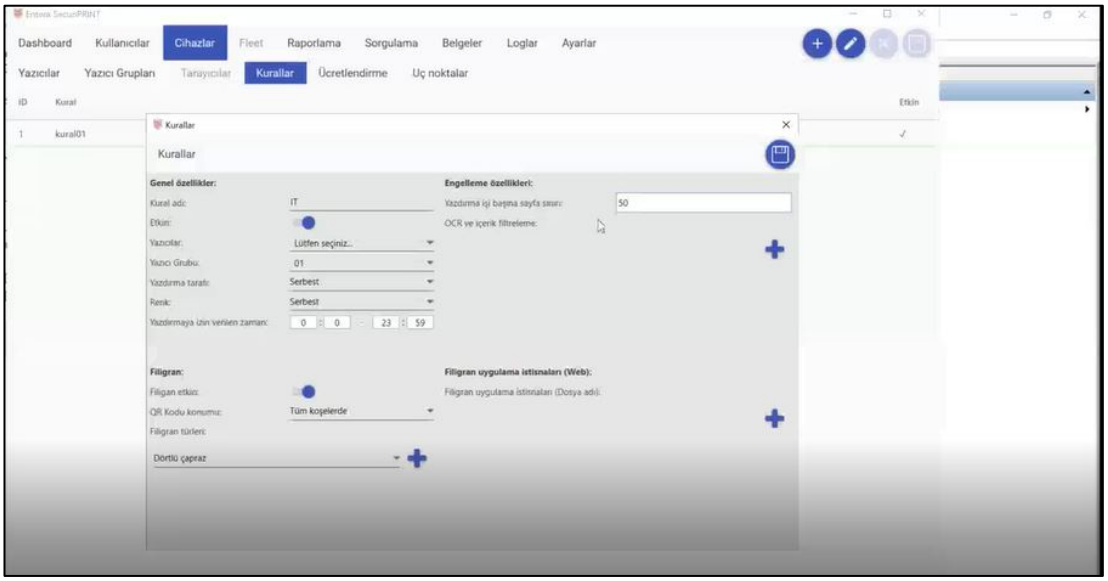


Şekil 4.9. Yazıcı gruplarının oluşurulması ve yazıcıların gruplara dahil edilmesi

Departmanlara göre yazıcı grubu oluşturulduktan sonra en son eklenen ya da herhangi bir gruba dahil olmayan yazıcılar müsait yazıcılar grubunda gözükmektedir. Yazıcının ekleneceği departman seçildikten sonra yön tuşu ile yazıcı seçilip istenilen gruba üye edilebilmektedir. Yazıcı hangi departman grubuna eklenmişse o departmanda bulunan kullanıcılar yazıcı üzerinde çıktı alabileceklerdir. Her yazıcı sadece bir yazıcı grubuna dahil edilebilmektedir.

4.3.5. Kurallar

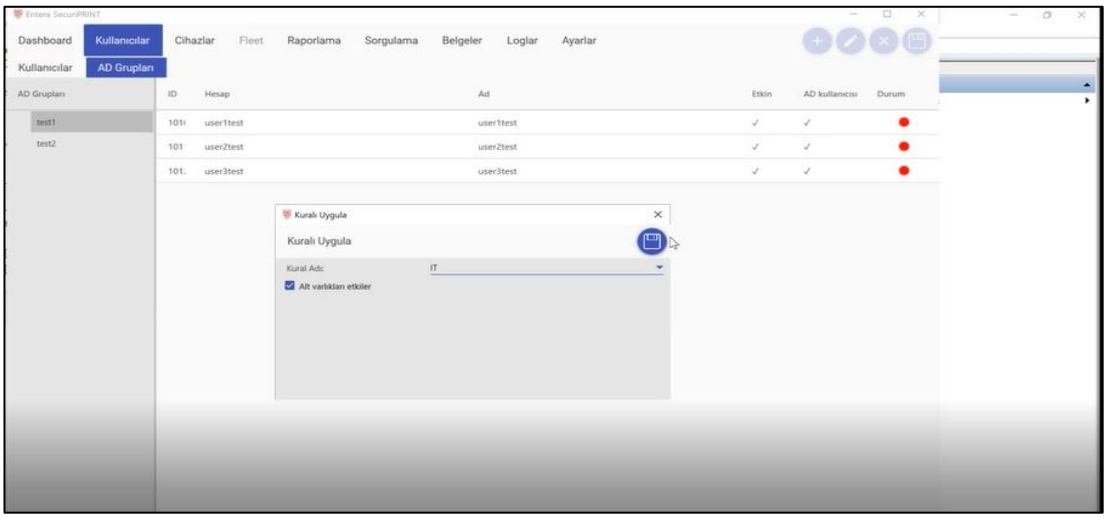
Kurallar, hangi yazıcının hangi departmana hizmet vereceğini, çıktı alınacak doküman üzerinde QR kod yada filigran ayarlarının tanımlanması gibi yazıcı bazlı politikaların belirlendiği alandır.



Şekil 4.10. Şirket isterlerine göre kuralların belirlenmesi

Kural adı tanımlandıktan sonra kuraldan etkilenmesini istediğim yazıcı grupları seçilir. Yazdırmaya izin verilen zaman ve filigran ayarları kurum politikalarına göre düzenlendikten sonra bir kullanıcının tek yazdırma işleminde maksimum çıkı sayısı ayarlanır. Bu düzenlemeler sayesinde çıktı alınacak dokümanların iz bilgileri, çıktı alma sınırı, kullanıcıların çıktı alabilecekleri zaman aralıkları tanımlanabilmektedir.

SecuruPrint uygulamasında oluşturulan kurallar yazıcılara değil, kullanıcılara uygulanmaktadır. Bu nedenle oluşturduğumuz kuralı kullanıcılar sekmesi altında bulunan AD gruplarına ya da kullanıcılara ile ilişkilendirilmesi gerekmektedir.



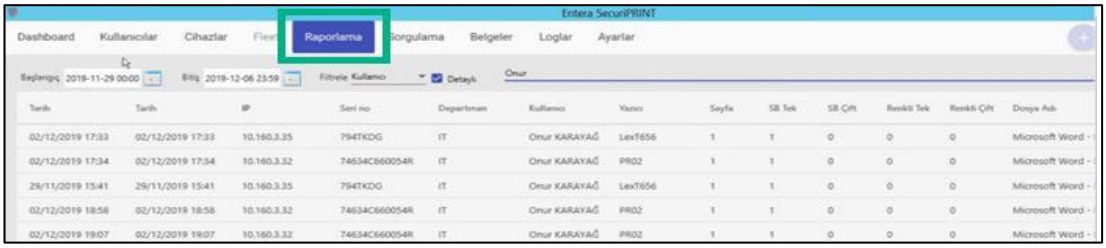
Şekil 4.11. Kuralların yazıcı gruplarına uygulanması

Kural AD kullanıcıları ile ilişkilendirildikten sonra AD üzerinde tanımlanan gruba eklenen her kullanıcı bu kuraldan etkilenmektedir.

Şirketin ihitiyaç ve taleplerine göre üç farklı kural belirlenmektedir. Genel kural, şirkette bulunan bütün kullanıcıların etkilendiği, çıktı alınan her doküman üzerinde filigran ve QR kodu birlikte barındıran kuraldır. İstisna uygulanmayan tüm kullanıcılar bu kuraldan etkilenmektedir. Bazı kullanıcılar ise çeşitli nedenlerden dolayı çıktı alınan belgeler üzerinde QR koda ya da filigran bulunmasını istememektedirler. Böyle durumlarda iki farklı istisna kuralı tanımlanabilmektedir. Birincisi filigran istisna kuralıdır. Bu kuralın tanımlı olduğu kullanıcı yada departmanlarda çıktı alınan dokümanlar üzerinde sadece QR kod bulunmakta filigran bulunmamaktadır. İkinci istisna kural ise QR kod ve filigranın her ikisinin de istisna edildiği kuraldır. Bu kuralın tanımlandığı yazıcı grupları yada kullanıcılar, üstünde filigran ve QR kodun bulunmayan dokümanları çıktı alma yetkisine sahiptirler.

4.3.6. Raporlar

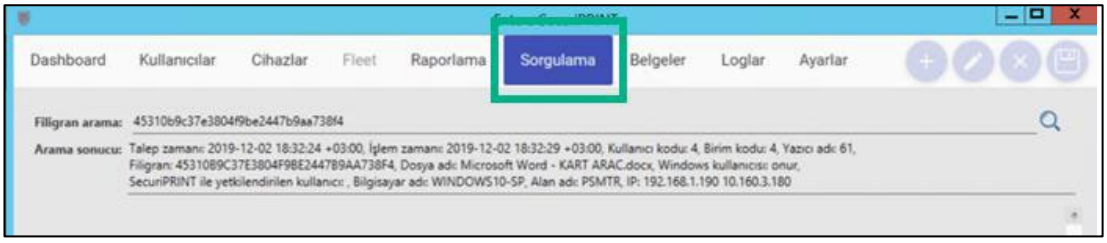
Raporlar seçilen tarih aralığına göre kullanıcı, birim veya yazıcı bazlı alınabilmektedir. Kullanıcının istenilen tarih aralığında hangi yazıcılardan ve kaç sayfa çıktı aldığı yazıcıların IP adresi, adı, departmanı gibi bir çok bilgiler raporlanabilmektedir.



Şekil 4.12. Uygulamanın raporlama özelliğinin test edilmesi

4.3.7. Sorgulama

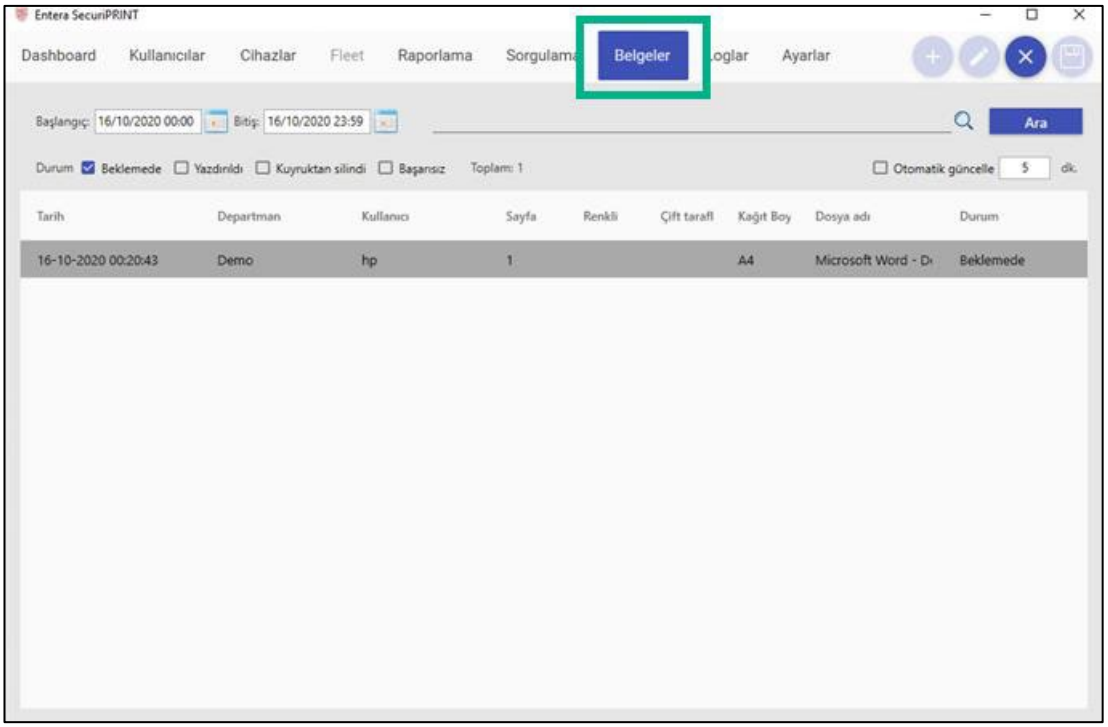
Tanımlanan kurallar sayesinde yazıcıdan alınan her doküman üzerinde, filigran ve filigran bilgisi içeren QR kod basılmaktadır. Kurumla ilgili gizli bilgi içeren bir belgenin yetkisi kişilerin eline geçmesi yada basına sızması durumunda üzerinde bulunan filigran numarası sorgulama ekranına girilerek belgenin çıktı alındığı ve kişi bilgisayar hakkında detaylı bilgiyi elde etmemize imkan sağlamaktadır.



Şekil 4.13. QR kod ve filigran özelliği ile elde edilen sorgulama sonuçları

4.3.8. Belgeler

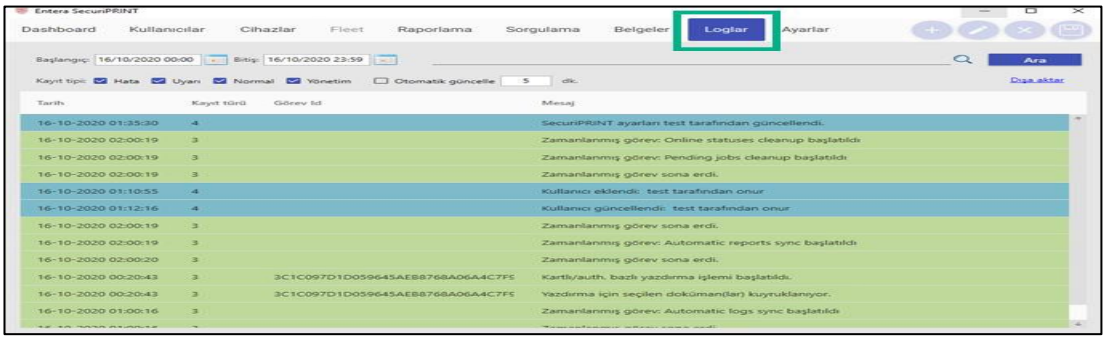
Belgeler sekmesinde kullanıcılar tarafından gönderilen işlerin iş detayları bulunmaktadır. Gönderilen işin durumuna, tarih aralığına ve kullanıcıya göre filtreler oluşturulabilir.



Şekil 4.14. Belge durumlarının analiz edilmesi

4.3.9. Loglar

Ağ cihazları sistem üzerinde gerçekleşen işlem ve olaylar hakkında kayıt yapma özelliğine sahiptirler. Bu kayıtlar sayesinde ağ ve cihazlar üzerinde güvenlik olaylarının tespit edilmesi ve gerekli önlemlerin alınması sağlanmaktadır. Sistem güvenliğini bu şekilde analiz edilmesine Log Analizi denilmektedir. Log analizi kullanıcıların sisteme ekleme durumlarını, çalışan ve duran servis bilgilerini, yazıcılardan kimlerin çıktı aldığını, çıktı alınan bilgisayar adı ve IP adresi gibi birçok işlemleri analiz edebilmektedir.



Şekil 4.15. Sistem loglarının detaylı izlenmesi

Sistem üzerinde yapılan tüm işlemlere ait log kayıtları Şekil 19' daki ekranda yer almaktadır. Sorgulanması istenilen tarih ve saat aralığı girildikten sonra sorgulaması yapılacak logun durumu belirlenir. Log kayıtlarının analiz edilmesinden sonra sistem üzerinde gerekli iyileştirmeler yapılabilmektedir.

4.4. Yazıcı Uygulamaları

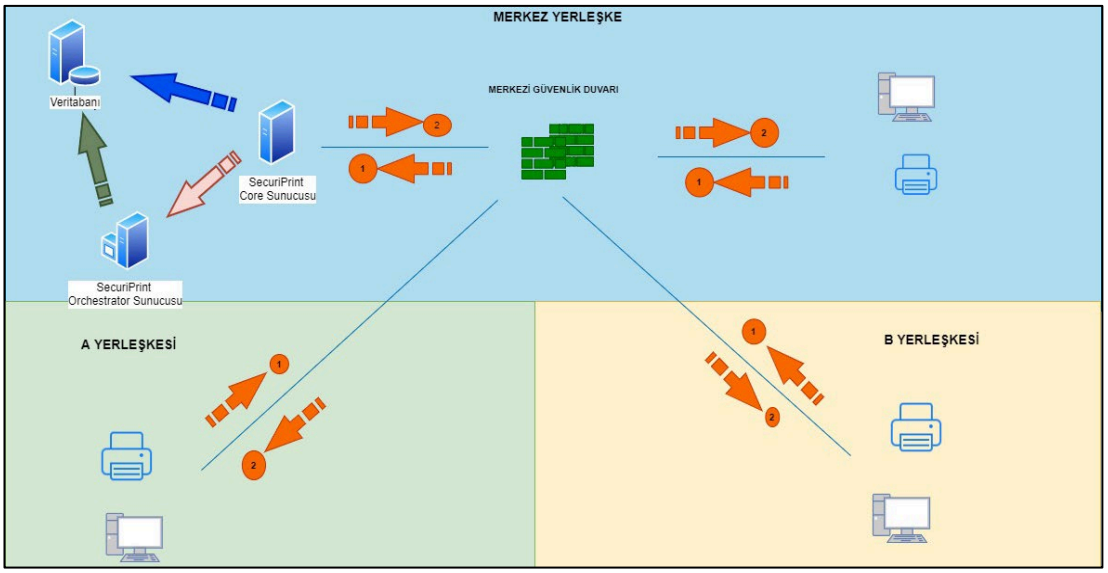
Yazıcı üzerine kurulması gereken iki uygulama bulunmaktadır. Yazıcı ekranında uygulamaların görünebilmesi için yazıcıda kart okuyucu takılı olması ve kart okuyucu tanımlanabilmesi için ise keyboard reader yüklü olması gerekmektedir

SecuriPrint: Çıktı Al uygulamasıdır. Kullanıcılar kartları ile veya kullanıcı adı/şifre bilgileri ile oturum açarak bekleyen işlerini listeleyebilirler. İstedikleri işlerin çıktısını alabilirler.

SecuriRoll: Kullanıcıları kart kaydetmek için kullandıkları uygulamadır. Sırasıyla aşağıdaki adımlar takip edilerek uygulama yazıcı üzerine kurulur.

4.5. Güvenli Baskı Yönetim Sisteminin Son Durumu

Güvenli Baskı Merkezi Yönetim Sistemi çalışmaları kapsamda şirketin ihtiyaçlarının tespiti, mevcut yazıcı durumu, maliyet analizi ve SecuriPrint uygulamasının testleri tamamlandıktan sonra SCCM (Microsoft System Center Configuration Manager) ile agent uygulaması merkezi olarak dağıtılmış ve şirketin baskı topolojisi üç lokasyonu kapsayacak şekilde aşağıdaki gibi oluşturulmuştur.



Şekil 4.16. Güvenli merkezi baskı sisteminin şirket topolojisi

Yeni durumda Merkez Yerleşke, A Yerleşke ve B Yerleşkede kartlı ve kartsız yazıcılardan çıktı alma işlemi Merkez Yerleşkede bulunan SecuriPrint Core yazıcı sunucusu üzerinden, Core sunucusu üzerinde bulunan log bilgilerinin toplanması ve merkezi lisans dağıtımı Orchestrator sunucusu tarafından yapılmaktadır. Core sunucusunun kullanıcı ve yazıcı bilgileri ile Orchestrator sunucusu üzerinde bulunan log bilgileri merkezi veritabanında tutulmaktadır.

SecuriPrint yazılımının Aktif Directory ile entegrasyonu sağlanmış, Aktif Directory senkronizasyonu her gün saat 06:00'da çalışacak olup yeni oluşturulan kullanıcılar senkronizasyon işleminin bitimini müteakip yazılım üzerinde kendilerini tanımlayabileceklerdir.

Gün içerisinde kartlı yazıcı sistemine gönderilen ve çıktısı alınmayan yazıcı çıktı istekleri, sistem tarafından her gün saat 02:00'de bir defaya mahsus olmak üzere otomatik olarak silinecek şekilde ayarlanmıştır. Bu durum çıktı alınmak istenmeyen dokümanların kuyruktan silinmesini sağlayarak, sisteme maliyet açısında tasarruf sağlamaktadır.

Çıktı alınan dokümanın dört köşesine filigran bilgisini içeren kare kod (QR) uygulanacak şekilde ayarlanmıştır. QR kod, çıktı gönderen personelin kullanıcı adı,

çıktı gönderilen istemci bilgisayar IP bilgisi, çıktı alınan doküman üzerindeki filigran bilgisi, çıktı gönderme ve alma işlemlerinin tarih saat bilgisi gibi çıktı alma işlemlerinin iz bilgilerini tutmaktadır.

Çıktı alınan dokümanın üzerine okunurluğu bozulmayacak şekilde dört adet çapraz şekilde filigran %35 saydamlık seviyesinde uygulanacak şekilde ayarlanmış, her dokümana ayrı üretilen kod filigran olarak kullanılmaktadır. Üretilen kod numarasının SecuriPrint sunucusundan sorgulanması ile çıktı alma işlemine ait iz bilgilerine ulaşılabilmektedir.

Yazıcılar şirket çalışanları dışında yabancı ve yetkisiz kişilerin erişimine karşı korunmuştur. Kişisel hesabı ve giriş kodu atanmamış yabancı kişi veya çalışanlar, yazıcı üzerinde herhangi bir işlem yapma olanağına sahip değildir. MFP'larda çıktı alma işlemi iki farklı güvenlik şifresi ile korunmaktadır. Birincisi kullanıcı istemci bilgisayardan yazıcıya doküman gönderdikten sonra şirkete kayıtlı tüm çalışanlara atanan kurumsal kullanıcı adı ve şifresi ile yazıcıya giriş baskı işlemini yapabilmektedir. Giriş yaparken ikinci güvenlik şekli ise bir çip kartı kaydetme seçeneğidir. Bu kartlar hem şirkete girişlerde hem de turnikelerde kullanıldığı için şirkette çalışan herkesin böyle bir kartı vardır. Her çalışan bu kartı veya çipi her zaman yanında taşımakla yükümlüdür. Bu kart bir kereliğine mahsus yazıcı ekranı üzerinde "beni kaydet" butonu seçilerek şirket kartını tanımlaması gerekmektedir. Müteakip SecuriPrint yazılımı üzerinden şirket kimlik kartı ile çıktı alınabilecektir. Kartın unutulması veya okuma cihazının arızalanması durumunda yine kullanıcı ve şifre ile yazdırma işlemi başlatılabilmektedir.

4.6. Güvenli Baskı Yönetim Sisteminin İzlenmesi ve Yönetimi

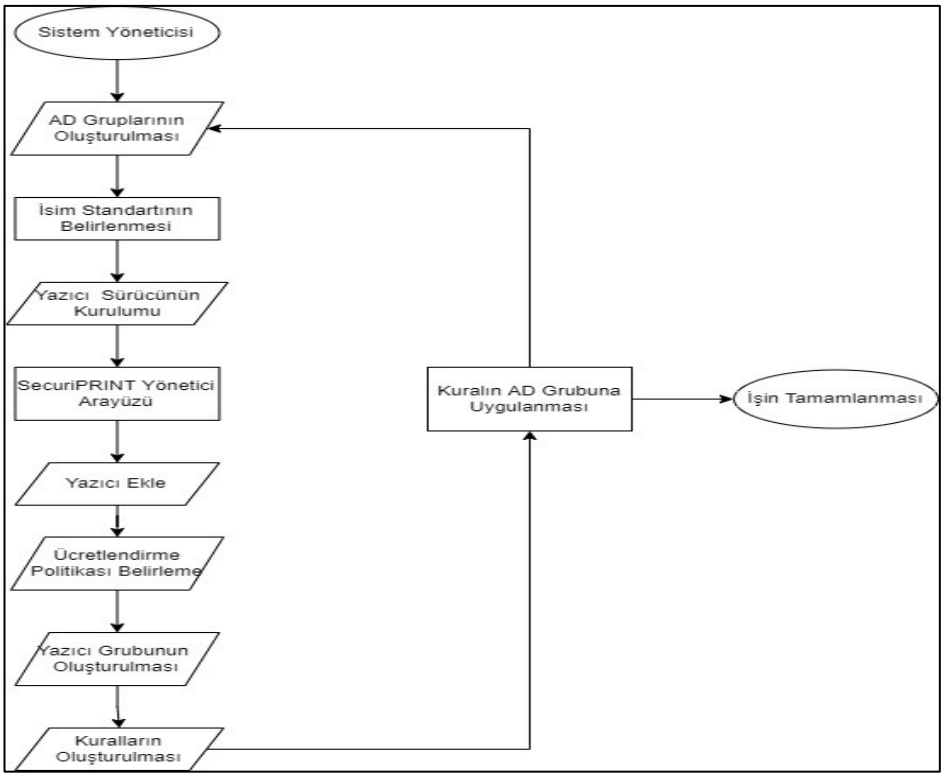
Mevcut durumda teknik personel, çalışanlardan gelen talepleri destek masası üzerinden almaktadır. Bu talepler sorunu çözebilecek ilgili destek personeline atanmaktadır. Teknisyenler müsait olmadığı durumlarda iş sürecini hızlandırmak için çalışanlar kendi başlarına hareket edip sorunu kendileri çözmeye çalışmaktaydılar. Bu gibi durumlar yazıcılarda daha fazla hasar meydana gelmesine ve bazı yazıcıların

kullanım dışı kalmasına sebep olmaktaydı. Örneğin, kağıt sıkışması gibi bir durumlarda kullanıcılar gelişi güzel kağıdı çıkarmaya çalışırken yazıcının bir çok hareketli parçasını kırmaya yol açmaktaydılar.

Yeni sistem, sarf malzemeleri ve kullanıcı hataları ilgili bir geri bildirim sistemi kullanılmaktadır. Yeni sistemin devreye alınmasıyla, bir - iki teknisyen şirketin tüm yazıcı desteğini sağlayabilmektedir. Ağ yazıcılarının zorunlu kullanımı ve küçük yerel yazıcılarının kullanımının sonlandırılması, sık sık yapılan yazdırma hataları azaltılmıştır. Küçük tonerlerden birkaç kat daha fazla dayanıklılık gösteren yüksek kapasiteli yazıcı tonerleri kullanan ağ yazıcılarının kullanılması şirketin yazıcı kaynaklı arızalarını % 50 'den fazla azaldığı görülmüştür. Bildirim sistemi sayesinde toner durumunu %20 kalması durumunda teknisyen ertesi gün, acil durumlarda aynı gün yeniden doldurur ve toner dengesi durumu raporlanır. Teknisyen bir yanlış besleme veya başka bir arıza bildirildiğinde bunu bilir ve neredeyse anında müdahale eder. Kağıt sıkışması veya başka bir sorunun tespit edilmesi durumunda, kullanıcı hatayı bildirmeden önce sorun çözülür. Kullanıcı hatalarının neden olduğu en yaygın sorun, tepsilere yanlış yerleştirilmiş kağıtlardır. Bu da yazıcının arızalanmasına veya besleyicide anında kağıt sıkışmasına neden olmaktadır. Yeni sistem sayesinde bu gibi durumların tespiti oldukça kolay tespit edilmektedir.

Yeni sistem çıktı alma işlemlerinin raporlaması sağlamkta ve bir kullanıcının, kaç sayfa siyah/beyaz veya renkli çıktı aldığı, kaç sayfa tek yüz veya çift yüz çıktı aldığı, hangi boyutta (a3/a4/a5) çıktı aldığı, hangi yazıcıdan çıktı aldığı bilgileri bulunmaktadır. Ayrıca yazıcıların durumu, toplam maliyet hesabı, en çok çıktı alan kullanıcıların tespiti, gibi durumlarda raporlanmaktadır.

Uygulamanın son aşaması ise sistemin yönetilmesi ve personelin eğitilmesidir. Sistem Yönetimi Teknik Departmanı için gelen sorunların tespiti dışında en önemli iş sistemin yönetimidir. Bu sorunun çözümü her zaman olmamakla birlikte şirkete yeni bir birim veya departmanın açılması durumunda yapılacak işlemleri adım adım aşağıdaki iş akış şemasındaki gibi yapması gerekmektedir.



Şekil 4.17. İş akış şeması

Şirkette yeni bir birim açıldığında bu talep destek masasına yazılır ve ilgili teknik personele iletilir. Teknik personel ilk olarak AD yapısı üzerinde ilgili yönetimsel birimin altına şirketin isim standartlarına uyumlu bir yazıcı grubu oluşur. Örneğin; İnsan Kaynakları departmanı için oluşturulacaksa ygIK adında yazıcı grubu oluşturulur. Burada "yg" yazıcı grubunu, IK departmanın adını temsil etmektedir. Ardından yazıcı sunucusuna bağlanılır ve "print managment" servisi açılarak yazıcı sürücüsü yine isim standartlarına uygun bir şekilde eklenir. Biz isim standartını IKYZC001 olarak belirliyoruz. IK departman ismi, YZC isimin bir yazıcı aygıtına ait olduğunu, 001 IK departmanının ilk yazıcısını ifade etmektedir.

Yazıcı sürücüsü yüklendikten sonra SecuriPrint yönetici ara-yüzü açılır. IKYZC001 isimli yazıcıyla aynı olacak şekilde yazıcının IP bilgisi, seri numarası ve yazıcının şirketteki konumu uygulamaya kaydedilir. Müteakip yazıcı grubu oluşturulur ve yazıcı bu gruba dahil edilir. Örneğin İnsan Kaynaklarına hizmet verecek yazıcı grubunun adını temsil eden "IK" adında bir yazıcı grubu oluşturup, IKYZC001 yazıcısını bu gruba dahil ediyoruz. IK yazıcı grubu sadece bu departmanda çalışan kullanıcılara

hizmet verebilmesi için bir politikanın belirlenmesine ihtiyaç duyulmaktadır. Yazıcıların çeşitli ayarlamaları ve hangi yazıcının hangi departmana hizmet vereceği kurallar ile belirlenir. IK departmanına tanımlanacağı için IK adında bir kural oluşturulup gerekli düzenlemeler yapıldıktan sonra kural AD üzerinde oluşturmuş olduğumuz ygIK grubuna uygulanır. Böylece IK departmanına kayıtlı tüm çalışanlar bu yazıcı üzerinde çıktı alabileceklerdir. Teknik personel bu süreci takip ederek sistemi yönetebilmektedir.

BÖLÜM 5. TARTIŞMA VE SONUÇ

Bu tezde çok sayıda yazıcı ve kötü tasarlanmış bir baskı sistemine sahip bir şirket ele alınmıştır. Tezin ana hedefi, dağıtık yapıda bulunan şirketin üç ana yerleşkesi için tek bir güvenli baskı sistemine sahip bir yapı oluşturmak bu şekilde belgelerin güvende kalmasını ve kullanıcı dostu bir baskı sistemini şirkete kazandırmaktır. Bu amaç ile uygulanacak baskı çözümünün seçimi, şirketin mevcut altyapısının analizi ve yeni sistemin uygulanma süreci ayrıntılı olarak tartışılmıştır. Şirketin baskı sürecinin güçlü ve zayıf yönleri belirlenmiştir. Analiz sonrasında alternatif bir merkezi baskı modeli tasarlanmış ve mevcut sistemin yerine yeni bu model oluşturulmuştur.

MBYS oluşturulurken SecuriPrint yazılımı kullanılmış ve şirketin mevcut yapısına entegre edilmiştir. SecuriPrint, çalışanların kendi birimlerinde veya farklı bir birimde olmaları fark etmeksizin aynı yazdırma kuyruğunda çıktı almalarına olanak sağlamaktadır. SecuriPrint, kullanıcıların yazıcılarda kimlik doğrulaması yapmasını zorunlu kıldığı için çıktıların otomatik olarak yazdırılmasını engellemekte ve gizli belgelerin güvende kalmasını sağlamaktadır. Belge ve dokümanların güvenliğini daha da artırmak için çıktılara filigran ve QR kod özelliği eklenmiş ve bu sayede baskı güvenliği ve takibi sağlanmıştır.

Şirkete çalışan yerel yazıcılar devre dışı bırakılmış ağ yazıcıların bakımı yapıldıktan sonra ilgili yerlere planlanmsı yapılmıştır. Yazıcı sayısı yeterli olduğundan yeni yazıcı alımı yapılmamış mevcut yazıcılar kurumun ihtiyaçlarını karşılayacak şekilde planlanmıştır. Yerel yazıcıların sistemden çıkarılması yazıcı sayısını türünü ve sayısını azaltmış bu durum sarf malzemelerinin türünü ve maliyetini önemli ölçüde azaltmıştır.

Eski sistemin kaldırılması yeni sistemin devreye alınması sırasında çalışanların olası tepkileri değerlendirilmiş ve teknik destek personelinin bu tepkilere karşı göserdiği tutum ele alınmıştır. Proje uygulaması sırasında çalışanlardan gelen geri dönüşler birer

fırsat olarak değerlendirilmiş ve yeterli analizler neticesinde uygulamasa iyeleştirmeler yapılmıştır.

Çalışmanın temel faydaları, yalnızca yeni bir baskı modeli tasarlamak ya da baskı sistemi olan bir organizasyonun durumunun analizini değil, aynı zamanda benzer baskı sorunları olan kurumların bu durumu iyileştirmek için uygulaması gereken adımlar birer birer anlatılmıştır. Çalışma, kurumsal belge güvenliğine karşı yapılacak olan fiziksel ve ağ ataklarını en aza indirecek bir çözüm getirilmiştir. Bu baskı çözümü sadece basılı dokümanların güvenliği açısından değil, aynı zamanda şirketin ulusal ve uluslararasında büyük bir nitelik kazanması açısından da büyük fayda sağlayan bir sistem getirmiştir. Bu durum aynı sorunları olan kurum ve şirketler için yeni projeler geliştirmeye temel teşkil edebilecektir.

KAYNAKLAR

[1] Erdem, E. S., Siber Güvenlik Farkındalığı İçin Yetenek Tabanlı Dinamik Model. Gazi Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 2016.

[2] Yılmaz, H., TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı kapsamında bilgi güvenliği yönetim sisteminin kurulması ve bilgi güvenliği risk analizi. Denetişim, 15, 45-49, 2016.

[3] Kaçar, M.S., Ağ Güvenliği Skorlama Sistemi, KTO Karatay Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 2017.

[4] Çakır, H., Tuğ, E., Adak, Ş.F., Bilişim güvenliği tedbirleri ve TKDK kurumunda uygulama örneği. Bilişim Teknolojileri Dergisi, 7(1), 11-18, 2014.

[5] Quocirca, Global Print Security Landscape, A global market perspective on print security, 2019.

[6] Quocirca, Global Print Security Landscape, Print security trends in the US and Europe, 2020.

[7] Ankita, J., Print document using password authentication on network printer. Journal of Information Technology ve Software Engineering, 5(2), 1, 2015.

[8] Kaczor, S., Kryvinska, N., It is all about services-fundamentals, drivers, and business models. Journal of Service Science Research, 5(2), 125-154. 2013.

[9] Çınar, S.M., Yıldırım, A., Bir kurumsal geniş alan ağının ağ yönetim sistemiyle etkili yönetimi. Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi, 9(1), 9-22, 2020.

[10] Datta, P.K., Empirical Study on Network Configuration Using Mikrotik Router. Daffodil International University, Doctoral Dissertation, 2021.

[11] Troia, S., Zorello, L.M.M., Maralit, A.J., Maier, G., SD-WAN: An open-source implementation for enterprise networking services. 22nd International Conference on Transparent Optical Networks (ICTON), July 19-23, Bari, Italy, 2020.

[12] Karovič, V., Kováč, F., Veselý, P., Print management system model in a large organization. Applied Sciences, 10(12), 4193, 2020.

[13] Durdu A., Eren A., ISO 27001 bilgi güvenliği yönetim sistemi yazılım tasarımı. Bilişim Teknolojileri Dergisi, 14(3), 255-266, 2021.

[14] Akçay, M., Mercanlı, M., Merkezi kimlik doğrulama sistemi. 4th International Symposium on Innovative Technologies in Engineering and Science (ISITES 2016), Novermber 3-5, Antalya, Turkey, 2016.

[15] Yılmaz, H., TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı kapsamında bilgi güvenliği yönetim sisteminin kurulması ve bilgi güvenliği risk analizi. KİDDER Kamu İç Denetçileri Derneği, 15(1), 45-59, 2014.

[16] Ylikangas, H., Print Management in Finnish Companies: Opportunities for Companies to Achieve Financial and Environmental Savings. Turku University of Applied Sciences, Bachelor's Thesis, 2016.

[17] Guo, Z., Zheng, H., You, C., Xu, X., Wu, X., Zheng, Z., Ju, J., Digital forensics of scanned QR code images for printer source identification using bottleneck residual block. Sensors, 20(21), 6305, 2020.

[18] Şeref, B. Öneri Sistemlerinde Başarımı Arttırmak için Yapay Zeka Tabanlı Yaklaşımlar. Ankara Üniversitesi Fen Bilimleri Enstitüsü, Doktora Tezi, 2021.

[19] Yüksel, Y., Kurumsal değişime direnme ve kabullenme: Compstat örnek olayı. Uluslararası Beşeri ve Sosyal Bilimler İnceleme Dergisi, 4(1), 4-24, 2020.

[20] Tuominen, T., Implementing a New Printing Solution: FollowPrint. Tampere University of Applied Sciences, Bachelor's Thesis, 2016.

[21] Serdar, Ö., Yücedağ, D. İ., Web API Tasarımı. Düzce Üniversitesi Teknoloji Fakültesi, Lisans Bitirme Tezi, 2020.

[22] Rasaq, M.O., Central Printing Management System: A Case Study of Contact Resolution Limited. Laurea University of Applied Sciences, Bachelor's Thesis, 2016.

[23] Biroğul, S., Koçer, K., Web ve mobil tabanlı bakım onarım ve varlık yönetim sisteminde önbellekleme yaklaşımları. Mühendislik Bilimleri ve Tasarım Dergisi, 6(4), 579-589, 2018.

[24] Yıldırım, S., Kenan, İ., Kampüs ağlarında internet erişimi için bağlantı katmanı kimlik doğrulama uygulaması. Computer Science, (Special), 82-92, 2021.

ÖZGEÇMİŞ

Adı Soyadı **:** Deniz GÖKÇEK

ÖĞRENİM DURUMU

Derece	**Eğitim Birimi**	**Mezuniyet Yılı**
Yüksek Lisans	Sakarya Üniversitesi / Fen Bilimleri Enstitüsü / Elektrik- Elektronik Mühendisliği	Devam ediyor
Akademi	Jandarma ve Sahil Güvenlik Akademisi / Subay Eğitim Merkezi	2019
Lisans	Kırklareli Üniversitesi / Mühendislik Fakültesi / Elektrik- Elektronik Mühendisliği	2016
Lise	Ağrı Anadolu Lisesi	2012

İŞ DENEYİMİ

Yıl	**Yer**	**Görev**
2019-Halen	Jandarma Genel Komutanlığı	Bilgi Sistem Subayı

YABANCI DİL

İngilizce